Ejercicios del Capítulo 1

LEYENDA: ♡ fácil, ♢ difícil, ♢♢ muy difícil, ∘ opcional.

Sección 1.1

1. Demostrar que:
i) $\{n + m\sqrt{3} \ : \ n, m \in \mathbb{Z}\}$ es un anillo.
ii) $\{a + b\sqrt{3} \ : \ a, b \in \mathbb{Q}\}$ es un anillo tal que todos sus elementos no nulos son unidades.
iii) $\{a + b\sqrt[4]{3} \ : \ a, b \in \mathbb{Q}\}$ no es un anillo.
♢iv) $\{a + b\sqrt[3]{3} + c\sqrt[3]{9} \ : \ a, b, c \in \mathbb{Q}\}$ es un anillo tal que todos sus elementos no nulos son unidades.

♡**2.** Sean $R_1, \ldots, R_n$ anillos. Demostrar que $R_1 \oplus \ldots \oplus R_n$ es un anillo con las operaciones de suma y producto obvias (las dadas por las de cada R_i coordenada a coordenada).

♡**3.** Escribir la tabla de multiplicación del anillo $\mathbb{Z}_3[i] = \{a + bi : a, b \in \mathbb{Z}_3\}$.

4. El conjunto $\{0, 2, 4, 6, 8\}$ es un anillo conmutativo con unidad, con la suma y el producto módulo 10. ¿Cuál es la unidad multiplicativa? ¿Y los elementos invertibles?

5. Probar que los elementos neutros de las operaciones de un anillo con unidad son únicos.

6. Comprobar que las unidades de $\mathbb{Z}_{17}$ forman un grupo cíclico.

7. ¿Cuántas unidades hay en $\mathbb{Z}_{10^6}$?

8. Hallar todas las unidades en $\mathbb{Z}[\sqrt{-5}]$, $\mathbb{Z}[(1 + \sqrt{-3})/2]$ y en el anillo de matrices enteras 2×2.

9. Probar que $2x + 1$ tiene inverso multiplicativo en $\mathbb{Z}_4[x]$.

10. Hallar las unidades del anillo de matrices 2×2 con elementos en $\mathbb{Z}_4$.

11. Hallar el inverso multiplicativo de 5 en $\mathbb{Z}_{21}$ usando el algoritmo de Euclides.

12. Probar que en el anillo de matrices reales $n \times n$, para todo elemento, m, que no es una unidad, existe $m' \neq 0$ tal que $m'm = 0$.

13. Encontrar un anillo R en el que no se verifiquen ninguna de las siguientes propiedades:

i) Si $a^2 = a$, entonces $a = 1$ ó $a = 0$.

ii) Si $ab = ac$ para $a \neq 0$ entonces $b = c$.

14. Si R no es un dominio de integridad la intuición que tenemos sobre ecuaciones algebraicas puede ser completamente errónea. Meditemos sobre este hecho:

i) Buscar un anillo R en el que la ecuación $ax = b$ con $a, b \in R$ tenga más de una solución.

ii) Encontrar todas las soluciones de la ecuación $x^2 - 5x + 6 = 0$ en $\mathbb{Z}_{12}$.

♡**15.** Sea $f : R \to S$ un homomorfismo de anillos. Demostrar que:

i) Para todo $r \in R$, y para todo entero positivo n, se tiene que $f(r^n) = f(r)^n$.

ii) La imagen de R por f, $\{s \in S : s = f(r), \text{ para algún } r \in R\}$, es un subanillo de S.

♡**16.** Sea $\phi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}$ dada por $\phi(P) = 2^{\partial P}$. Estudiar si es un homomorfismo.

17. Probar que el anillo $\mathbb{Z}_6$ es isomorfo al anillo $\mathbb{Z}_2 \oplus \mathbb{Z}_3$.

18. Demostrar que los anillos $\mathbb{Z}[\sqrt{7}] = \{a + b\sqrt{7} : a, b \in \mathbb{Z}\}$ y

$$R = \left\{ \begin{pmatrix} c & 7d \\ d & c \end{pmatrix} : c, d \in \mathbb{Z} \right\}$$

son isomorfos.

19. Demostrar que la aplicación $f : \mathbb{Z}_n \to \mathbb{Z}_n$ dada por $f(x) = x^n$ es un homomorfismo de anillos si n es primo. ¿Es el resultado cierto si n no es primo?

∘**20.** Escribir $x_1^2 + x_2^2 + x_3^2$ y $x_1^3 + x_2^3 + x_3^3$ en términos de los polinomios simétricos elementales.

∘**21.** Sea $s_k = x_1^k + x_2^k + \cdots + x_n^k$ para $0 < k$ y $s_0 = k$. Demostrar las "identidades de Newton"

$$\begin{aligned} (-1)^{k+1} s_k &= \sum_{i=0}^{k-1} (-1)^i s_i \sigma_{k-i} \qquad \text{para } 0 < k \leq n \\ (-1)^{k+1} s_k &= \sum_{i=k-n}^{k-1} (-1)^i s_i \sigma_{k-i} \qquad \text{para } k > n \end{aligned}$$

donde σ_i son los polinomios simétricos elementales. *Indicación*: Defínase $\sigma_i = 0$ para $i > n$ y aplíquese inducción para demostrar simultáneamente ambas identidades.

Sección 1.2

♡**22.** Probar que a y b están asociados si y sólo si $\langle a\rangle = \langle b\rangle$.

23. ¿Cuándo tiene sentido $n\mathbb{Z}/m\mathbb{Z}$?

24. Hallar el generador mónico del ideal $I = \langle x^3+1, x^2+1\rangle$ en $\mathbb{Z}_2[x]$.

♡**25.** Demostrar que $\mathbb{Q}[x]/\langle x^2-5x+6\rangle$ no es un dominio de integridad.

26. En $\mathbb{Z}[x]$ sea I el subconjunto formado por los polinomios tales que la suma de sus coeficientes es cero. Probar que I es un ideal y que $\mathbb{Z}[x]/I$ es isomorfo a $\mathbb{Z}$.

27. Hallar un subanillo de $A = \mathbb{Z}[\sqrt{2}]$ que no sea ideal.

28. Probar que todos los subanillos de $\mathbb{Z}$ son ideales. Dar un contraejemplo si $\mathbb{Z}$ se reemplaza por $\mathbb{Z}\oplus\mathbb{Z}$.

29. Demostrar que el grupo multiplicativo de $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ es cíclico y dar un generador.

30. Hallar los ideales de $\mathbb{Z}_{24}$.

31. Sea $f : R \to S$ un homomorfismo de anillos. Demostrar que:
i) Si $J \subset S$ es un ideal, entonces $f^{-1}(J) = \{r \in R : f(r) \in J\}$ es un ideal en R.
ii) El núcleo de f es un ideal.
iii) Un homomorfismo de anillos es inyectivo si y sólo si su núcleo es $\{0\}$.

32. Dado un anillo R y un ideal $I \subset R$, demostrar que hay una correspondencia biyectiva entre los ideales de R/I y los ideales de R que contienen a I. *Indicación*: usar el homomorfismo natural $\pi : R \to R/I$, que a cada elemento $a \in R$ le asocia su clase módulo I, y observar que la imagen inversa de un ideal por un homomorfismo de anillos es también un ideal.

33. Sea $A = \mathbb{Z}[\sqrt{2}]$. Hallar todos los ideales del anillo $A/2A$.

34. Hallar los ideales de $\mathbb{Q}[x]/\langle x^3-1\rangle$.

35. Decidir si el ideal $\langle 29, 13+\sqrt{-5}\rangle$ es principal en $\mathbb{Z}[\sqrt{-5}]$

36. Probar que el anillo de matrices cuadradas reales $n \times n$ no tiene ideales no triviales.

37. Encontrar todos los ideales maximales de los anillos $\mathbb{Z}_8,\ \mathbb{Z}_{10},\ \mathbb{Z}_{12}$ y $\mathbb{Z}_n$.

38. Probar que $I = \{(3n, m) : n, m \in \mathbb{Z}\}$ es un ideal maximal en $\mathbb{Z}\oplus\mathbb{Z}$.

39. Sea $I \subset \mathbb{Z}[\sqrt{-5}]$ dado por $I = \{a + b\sqrt{-5} \ : \ \ a + b \text{ es par}\}$. Demostrar que es un ideal maximal de $\mathbb{Z}[\sqrt{-5}]$.

$\diamondsuit$**40.** Sean I y J, con $J \subset I$, ideales de un anillos A. Probar que A/I es isomorfo a $(A/J)/(I/J)$. (Esto requiere en particular probar que este último cociente tiene sentido).

$\diamondsuit$**41.** Sea p primo y sea $A \subset \mathbb{Q}$ el anillo formado por todas las fracciones cuya forma irreducible tiene denominador no divisible por p. Hallar un anillo sencillo que sea isomorfo a $A/\langle p \rangle$.

Sección 1.3

42. Sea el conjunto $H = \{1, 5, 9, 13, 17, 21, 25 \dots\}$. Decimos que $p \in H$ es un H-primo si $p \neq 1$ y no es divisible por ningún elemento de H salvo por sí mismo y por uno. Por ejemplo, 5 y 9 son H-primos, pero $25 = 5 \cdot 5$ no. Comprobar que 693 tiene varias posibles descomposiciones en factores H-primos. (Nota: Hilbert (1862-1943) propuso H como un conjunto sencillo en el que no se cumple el análogo del teorema fundamental de la aritmética).

43. Hallar todos los polinomios irreducibles en $\mathbb{Z}_2[x]$ de grados 2, 3 y 4.

44. Decir si son irreducibles en $\mathbb{Q}[x]$ los polinomios $3x^2 - 7x - 5$, $6x^3 - 3x - 18$ y $x^3 - 7x + 1$.

45. Demostrar que $x^3 - x + 1$ es irreducible en $\mathbb{Z}_3[x]$.

46. Demostrar que $x^5 - x^2 + 1$ es irreducible en $\mathbb{Z}_2[x]$.

47. Probar la irreducibilidad en $\mathbb{Q}[x]$ de los polinomios: $x^5 - 3x + 3$, $x^6 - 6x + 2$, $x^2 + 1$, $x^4 + 1$ y $x^6 + x^3 + 1$.

48. Probar que $P \in \mathbb{Q}[x]$ es irreducible si y sólo si Q dado por $Q(x) = P(x + 1)$, lo es.

49. Probar que el criterio de Eisenstein es aplicable al polinomio

$$x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \cdots + \binom{p}{p-2} x + \binom{p}{p-1}.$$

50. Decidir si los siguientes polinomios son irreducible en $\mathbb{Q}[x]$: $x^4 + 3x + 6$, $x^3 + 11^{11}x + 13^{13}$, $\frac{1}{3}x^5 + \frac{5}{2}x^4 + \frac{3}{2}x^3 + \frac{1}{2}$, $x^5 - 9x^2 + 1$ y $x^4 - x^3 - x - 1$.

51. Probar que $x^2 + bx + c$ es irreducible en $\mathbb{Z}_7[x]$ si y sólo si $b^2 - 4c = 3, 5, 6$.

52. Estudiar la irreducibilidad de $P = x^2 + 1$ en $\mathbb{Z}_3[x]$, $\mathbb{Z}_5[x]$, $\mathbb{Z}_7[x]$, $\mathbb{Z}_{11}[x]$, $\mathbb{Z}_{13}[x]$ y $\mathbb{Z}_{17}[x]$.

∘**53.** Intentar inducir (sin demostración) una regla general sencilla que permita decidir la irreducibilidad de $P = x^2 + 1$ en $\mathbb{Z}_p[x]$ sin calcular sus raíces.

54. Hallar un contraejemplo a la Proposición 1.3.8 si se omite la condición $\partial P = \partial \overline{P}$.

55. Estudiar si $\mathbb{Z}[\sqrt{-2}]$ es un dominio de factorización única.

56. Demostrar que $\mathbb{Z}[\sqrt{2}]$ es un dominio de factorización única y encontrar la factorización de 20. *Indicación*: La ecuación en enteros $a^2 - 2b^2 = 5$ no tiene solución (lleva a contradicción módulo 5).

57. Estudiar si $\mathbb{Z}[\sqrt{-6}]$ es un dominio de factorización única.

♢**58.** Estudiar si $\mathbb{Z}[\sqrt{6}]$ es un dominio de factorización única.

♢**59.** Demostrar que un polinomio de la forma $P = x^n + px + p^2$ es irreducible en $\mathbb{Z}[x]$.

♢**60.** Sea $p > 2$ primo. Demostrar que existen $n, m \in \mathbb{Z}$ tales que $p = n^2 + mn + m^2$ si y sólo si $P = x^2 + x + 1$ factoriza en $\mathbb{Z}_p[x]$.

Ejercicios del Capítulo 2

LEYENDA: ♡ fácil, ♢ difícil, ♢♢ muy difícil, ∘ opcional.

Sección 2.1

♡**61.** Demostrar que $\mathbb{Z}/6\mathbb{Z}$ no es un cuerpo. Hallar las unidades.

62. Hallar el máximo común divisor de $P = x^4 + 6x^3 + 13x^2 + 12x + 3$ y $Q = x^4 + 5x^3 + 9x^2 + 8x + 2$, y escribirlo en la forma $AP + BQ$.

63. Demostrar que si la característica de un cuerpo no es cero, entonces es un número primo.

64. Demostrar que un dominio de integridad finito es un cuerpo.

65. Sea F un cuerpo y $f(x) \in F[x]$ un polinomio. Se dice que $a \in F$ es un cero de $f(x)$ si $f(a) = 0$. Demostrar que a es un cero de $f(x)$ si y sólo si $x - a$ divide a $f(x)$. *Indicación*: Estudiar el resto al dividir $f(x)$ por $x - a$.

66. El polinomio $f = x^3 - 3x + 1$ es irreducible en $\mathbb{Q}[x]$. Sea $\beta = \overline{x^4 - 3x^2 + 2x + 3} \in \mathbb{Q}[x]/\langle f \rangle$. Hallar β^{-1} y β^2 expresándolos como combinación lineal de $\{1, \overline{x}, \overline{x}^2\}$.

67. Probar que si P es un polinomio no nulo sobre un cuerpo, su número de raíces es menor que el grado. Dar un contraejemplo si el cuerpo se reemplaza por un anillo.

68. Si K es un cuerpo y R es un anillo, probar que cualquier homomorfismo no nulo $f : K \longrightarrow R$ es necesariamente un monomorfismo.

69. Dado un cuerpo L, sea K la intersección de todos sus subcuerpos (K recibe el nombre de *subcuerpo primo* de L). Demostrar que la característica de L es positiva si y sólo si K es isomorfo a $\mathbb{F}_p$, y es cero si y sólo si K es isomorfo a $\mathbb{Q}$.

70. Sea $f : L \to M$ un homomorfismo no trivial de cuerpos. Probar que la característica de L es igual a la de M, y que si K es el subcuerpo primo de L entonces $f(s) = s$ para todo $s \in K$.

71. Encontrar todos los automorfismos de $\mathbb{Q}(\sqrt[3]{5})$. *Indicación*: Hallar la imagen de 5 y emplear $(\sqrt[3]{5})^3 = 5$ para determinar la de $\sqrt[3]{5}$.

72. Calcular todos los automorfismos de $\mathbb{Q}(\sqrt{7})$.

73. Demostrar que $\mathbb{Q}(\sqrt{2})$ no es isomorfo a $\mathbb{Q}(\sqrt{5})$.

74. Demostrar que en $\mathbb{Z}$ y en $K[x]$ (K un cuerpo) hay infinitos irreducibles no asociados.

75. Se dice que un cuerpo K es algebraicamente cerrado si todo polinomio $P \in K[x]$ con $\partial P \geq 2$ se descompone en factores lineales. Probar que ningún cuerpo finito es algebraicamente cerrado

76. Establecer las relaciones de inclusión que hay entre los cuerpos $\mathbb{Q}(i, \sqrt{3})$, $\mathbb{Q}(\sqrt{-3})$ y $\mathbb{Q}(i + \sqrt{3})$.

77. Demostrar que $\mathbb{F}_2[x]/\langle x^2 + x + 1 \rangle$ es un cuerpo y calcular su cardinal. Dar la tabla de su producto.

78. Construir un cuerpo con 25 elementos y otro con 27. *Indicación*: No es necesario escribir la tabla de las operaciones en estos cuerpos.

79. Probar que sólo hay un cuerpo de cuatro elementos salvo isomorfismos.

80. Probar que no hay dominios de integridad de seis elementos (por lo tanto no hay cuerpos de seis elementos).

81. Probar que para todo primo p, en $\mathbb{F}_p[x]$ se cumple

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1)).$$

82. Si K tiene característica p, probar que $\phi : K \longrightarrow K$ dado por $\phi(k) = k^p$ es un homomorfismo.

83. Sea $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ en $K[x]$ con $a_0, a_n \neq 0$. f es irreducible si y sólo si $a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$ es irreducible.

♢**84.** Sea A un dominio de integridad y supongamos que existe un cuerpo $K \subset A$ tal que A es un espacio vectorial de dimensión finita sobre K. Demostrar que A es también un cuerpo.

♢**85.** Demostrar que si un primo p es de la forma $p = n^2 + 2m^2$ con $n, m \in \mathbb{Z}$, entonces $\mathbb{Z}[\sqrt{-2}]/(n + m\sqrt{-2})$ es isomorfo a $\mathbb{F}_p$.

Sección 2.2

86. Hallar el grado de las siguientes extensiones y decir de qué tipo son:

i) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ ii) $\mathbb{Q}(e^{2\pi i/5})/\mathbb{Q}$ iii) $\mathbb{R}(\sqrt{3})/\mathbb{R}$ iv) $\mathbb{R}(\sqrt[4]{-3})/\mathbb{R}$
v) $\mathbb{F}_7(t)/\mathbb{F}_7(t^2)$ vi) $\mathbb{F}_7(t)/\mathbb{F}_7$ vii) $\mathbb{Q}(\sqrt{5}, \sqrt[6]{5})/\mathbb{Q}$ viii) $\mathbb{Q}(\sqrt{5}, \sqrt[6]{5})/\mathbb{Q}(\sqrt{5})$

87. Probar que $\mathbb{Q}(\sqrt{7}, \sqrt[3]{7}, \ldots, \sqrt[n]{7}, \ldots)$ no es una extensión finita de $\mathbb{Q}$.

♡**88.** Probar que $A/\mathbb{Q}$ es una extensión infinita, donde $A \subset \mathbb{C}$ son los números algebraicos sobre $\mathbb{Q}$.

89. Demostrar que una extensión de grado primo es simple.

90. Si L/K es finita y P es un polinomio irreducible en $K[x]$, demostrar que si P tiene alguna raíz en L, entonces ∂P divide a $[L : K]$.

91. Si L/K es finita y $K \subset M \subset L$, probar que para cualquier $\alpha \in L$ se cumple $[M(\alpha) : M] \leq [K(\alpha) : K]$.

92. Sea $K(\alpha, \beta)$ una extensión algebraica de K, $n_\alpha = [K(\alpha) : K]$, $n_\beta = [K(\beta) : K]$ y $n = [K(\alpha, \beta) : K]$.

i) Demostrar que $\text{mcm}(n_\alpha, n_\beta) | n$ y $n \leq n_\alpha \cdot n_\beta$. ¿Qué se puede decir si n_α y n_β son coprimos?

ii) Mostrar un ejemplo con $n_\alpha \neq n_\beta$ en el que se cumpla $n < n_\alpha \cdot n_\beta$.

93. Probar que L/K y M/L algebraicas, implica M/K algebraica.

94. Sea $a < 0$ un número real algebraico sobre $\mathbb{Q}$, y sea $p(x) \in \mathbb{Q}[x]$ el polinomio mínimo de a sobre $\mathbb{Q}$. Demostrar que $\sqrt{a}$ es también algebraico sobre $\mathbb{Q}$, y determinar su polinomio mínimo sobre $\mathbb{Q}$.

♡**95.** Sea F un cuerpo y sea $f(x) \in F[x]$ un polinomio no nulo. Probar que si a está en alguna extensión de F, y $f(a)$ es algebraico sobre F, entonces a es algebraico sobre F.

♡**96.** Sea β un cero de $f(x) = x^5 + 2x + 6$. Probar que ninguno de los números $\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}$ pertenece a $\mathbb{Q}(\beta)$.

♡**97.** Si α es trascendente sobre K, ¿cuál es el grado de $K(\alpha)/K$?

98. Probar que un polinomio mónico P (no constante) es el polinomio mínimo de α sobre $K[x]$ si y sólo si es irreducible y cualquier $Q \in K[x]$ con $Q(\alpha) = 0$ es divisible por P.

99. Hallar $[\mathbb{Q}(\sqrt[7]{2}, \sqrt[5]{3}) : \mathbb{Q}]$.

100. Si $[K(\alpha) : K] = n$ y $P \in K[x]$ es el polinomio mínimo de α, indicar alguna base de $K[x]/\langle P\rangle$ sobre K.

101. Sean α y β en L/K tales que $[K(\alpha) : K] = m$ y $[K(\beta) : K] = n$. Demostrar que el grado del polinomio mínimo de β en $K(\alpha)$ es n si y sólo si el grado del polinomio mínimo de α en $K(\beta)$ es m.

102. Calcular el polinomio mínimo de $\sqrt{3} + \sqrt{5}$ en $\mathbb{Q}(\sqrt{15})$.

103. Sea α una raíz de $P = x^3 - x - 2 \in \mathbb{Q}[x]$. Escribir $(\alpha + 1)/(\alpha - 1)$ como una combinación lineal de 1, α y α^2.

104. Si $K(\alpha)/K$ es una extensión de grado tres, calcular $[K(\alpha^2) : K]$. Suponiendo que el polinomio mínimo de α es $x^3 + x - 1$, hallar el polinomio mínimo de α^2.

♢**105.** Calcular el polinomio mínimo de $\sqrt[3]{9} + \sqrt[3]{3} - 1$.

106. Probar que $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

107. Calcular el grado del polinomio mínimo de $\cos(2\pi/p)$ sobre $\mathbb{Q}$ donde p es un primo. *Indicación*: Compárese la extensión correspondiente con $\mathbb{Q}\big(e^{2\pi i/p}\big)/\mathbb{Q}$.

108. Si n y m son enteros positivos libres de cuadrados (no divisibles por cuadrados distintos de 1^2), comparar los cuerpos $\mathbb{Q}(\sqrt{n}, \sqrt{m})$, $\mathbb{Q}(\sqrt{n} + \sqrt{m})$ y $\mathbb{Q}(\sqrt{nm})$.

109. Hallar el grado de la extensión $\mathbb{Q}\big(\sqrt{1 + \sqrt{3}}\big)/\mathbb{Q}$.

110. Probar que $\mathbb{Q}(\alpha)/\mathbb{Q}$ es trascendente si y sólo si $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}$ lo es.

111. Sea $A \subset \mathbb{C}$ el cuerpo formado por todos los números algebraicos sobre $\mathbb{Q}$. Demostrar que todo polinomio no constante de $A[x]$ se descompone en factores lineales en este anillo.

112. Si α es trascendente sobre K, hallar $[K(\alpha) : K\big(\alpha^3/(\alpha+1)\big)]$.

♢**113.** Probar que $\mathbb{R}$ no es una extensión simple de $\mathbb{Q}$.

♢**114.** Sea α raíz de un polinomio irreducible $P = x^n - a_{n-1}x^{n-1} + \cdots + (-1)^{n-1}a_1x + (-1)^n a_0$ de grado n primo. Probar que si $\beta = Q(\alpha) \notin \mathbb{Q}$, entonces el polinomio mínimo sobre $\mathbb{Q}$ de β viene dado por el determinante

$$\det(xI - Q(A)) \qquad \text{donde} \qquad A = \begin{pmatrix} 0 & -1 & 0 & 0 & \dots & 0 \\ 0 & 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & 0 & -1 & \dots & 0 \\ \dots & & \dots & & \dots & \\ 0 & 0 & 0 & 0 & \dots & -1 \\ a_0 & a_1 & a_2 & a_3 & \dots & a_{n-1} \end{pmatrix}$$

Sección 2.3

115. Decir cuáles de las siguientes longitudes son construibles con regla y compás

$$\sqrt{\sqrt{2}+\sqrt{3}}, \qquad \sqrt[3]{7+5\sqrt{2}}, \qquad \sqrt{1+\sqrt{\sqrt{2}+\sqrt[3]{3}}}, \qquad e^{i\pi/8} + e^{-i\pi/8}.$$

116. Diseñar un método sencillo para construir la longitud $\sqrt{1+\sqrt{3}}/\sqrt{2}$ con regla y compás.

117. Probar que la distancia al origen de un punto construible, es construible.

118. Demostrar que los polígonos regulares inscritos en el círculo unidad de 7, 11, 13 y 19 lados no son construibles con regla y compás. *Indicación*: Considérese la extensión $\mathbb{Q}\big(e^{2\pi i/p}\big)/\mathbb{Q}$ con p primo.

119. ¿Algún cubo es duplicable? ¿Algún ángulo es trisecable?

120. ¿Es el pentágono regular construible con regla y compás? *Indicación*: Hallar $\cos(2\pi/5) + \cos(4\pi/5)$ y $\cos(2\pi/5) \cdot \cos(4\pi/5)$.

♢**121.** Crear un método para construir el pentágono regular.

122. Usando los principios de lo que más tarde sería la teoría de Galois, Gauss demostró (a los 19 años) que el valor de $\cos(2\pi/17)$ es

$$-\frac{1}{16}+\frac{1}{16}\sqrt{17}+\frac{1}{16}\sqrt{34-2\sqrt{17}}+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}$$

Explicar por qué de esta fórmula se deduce que el polígono regular de 17 lados se puede construir con regla y compás. (Nota: Esta construcción geométrica es una de las pocas que había escapado al ingenio de los antiguos geómetras griegos. Según se dice, Gauss mandó que fuera inscrita en su tumba).

123. Demostrar que si los polígonos regulares de n y m lados son construibles con regla y compás, también lo es el de $\mathrm{mcm}(n,m)$ lados. Concluir del ejercicio anterior que el polígono regular de 204 lados es construible con regla y compás.

124. Sea α la única raíz real positiva de $P=x^4-10x^3+26x^2+16x-14$. Sabiendo que no existe $\mathbb{Q}\subsetneqq M\subsetneqq\mathbb{Q}(\alpha)$ tal que $M/\mathbb{Q}$ sea de grado 2, probar que $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$ pero α no es construible.

125. ¿Se puede triplicar el cubo?

126. ¿Se puede trisecar el ángulo de $\pi/2^n$ radianes?

127. Decir si las siguientes extensiones son algebraicas o trascendentes.

$$\mathbb{Q}(\pi,\sqrt{3})/\mathbb{Q}(\sqrt{3}),\qquad \mathbb{Q}(\sqrt{\pi})/\mathbb{Q}(\pi),\qquad \mathbb{Q}(e)/\mathbb{Q}(e^5-e^3+7e^2+100e-1).$$

128. Demostrar que si α y β son trascendentes sobre $\mathbb{Q}$, entonces $\alpha+\beta$ ó $\alpha\cdot\beta$ son trascendentes sobre $\mathbb{Q}$. Dar un contraejemplo a la implicación: α, β trascendentes $\Rightarrow$ $\alpha+\beta$ trascendente.

129. Responder a la siguiente crítica: El argumento para probar que el ángulo de 60° no se puede trisecar no es concluyente, porque sólo se demuestra que $(\cos 20°,\sin 20°)$ no es construible, y quizá haya algún otro punto distinto del origen) en la recta $u=x\tan 20°$ que sí sea construible, lo que permitiría la trisección.

130. Supongamos que disponemos de una regla curva cuyo borde tiene la forma de la gráfica de $y=x^3$ para $x\geq 0$. Esta regla está sin graduar (aunque tiene marcado el cero) y sólo puede ser usada para trazar la curva que une dos puntos construibles, uno de ellos situado en el origen de la regla. Demostrar que con regla, compás y regla curva se puede duplicar el cubo. ¿Se puede cuadrar el círculo? ¿Y trisecar el ángulo?

♢**131.** Sea $P(x)=x^n(1-x)^n/n!$. Probar que si π^2 fuera una fracción con numerador a, entonces $E_n=a^n\pi\int_0^1 P(x)\,\mathrm{sen}(\pi x)\,dx$ sería un entero no nulo para todo n. Demostrar que $\lim E_n=0$, llegando a una contradicción con que $\pi^2\in\mathbb{Q}$.

Ejercicios del Capítulo 3

LEYENDA: ♡ fácil, ♢ difícil, ♢♢ muy difícil, ∘ opcional.

Sección 3.1

132. Hallar el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $x^6 - 8$, y calcular el grado de la extensión correspondiente.

133. Hallar el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio x^4+5x^2+5 y calcular su grado.

134. Probar que $P = x^4 - 2x^3 - x^2 - 2x - 2$ y $Q = x^5 - 3x^3 + x^2 - 3$ tienen el mismo cuerpo de descomposición sobre $\mathbb{Q}$. *Indicación*: Nótese que i es raíz del primero y que $\sqrt{3}$ es raíz del segundo.

135. Sean cuerpos $K \subset M \subset L$ y sea $P \in K[x]$ no constante. Si L es cuerpo de descomposición de P sobre K, probar que L es cuerpo de descomposición de P sobre M.

136. Si L es el cuerpo de descomposición de $P \in K[x]$, demostrar que $[L : K] \big| (\partial P)!$. *Indicación*: Procédase por inducción en el grado del polinomio, distinguiendo dos casos al aplicar la hipótesis de inducción dependiendo de la irreducibilidad de P. Recuérdese que $r!s!$ divide a $(r + s)!$ por la fórmula para los números combinatorios.

137. Sea L/K una extensión de grado 4. Demostrar que si L es el cuerpo de descomposición de un polinomio irreducible de la forma $x^4 + ax^2 + b \in K[x]$, existe un cuerpo intermedio $K \subset E \subset L$ tal que $[E : K] = 2$.

138. Si $K \subset M \subset L$, demostrar que L/K normal $\Rightarrow L/M$ normal, pero L/K normal $\not\Rightarrow M/K$ normal, y L/M, M/K normales $\not\Rightarrow L/K$ normal.

139. Estudiar si las extensiones $\mathbb{Q}(\sqrt[3]{-2}, \sqrt{-2})/\mathbb{Q}$ y $\mathbb{Q}(\sqrt[3]{-3}, \sqrt{-3})/\mathbb{Q}$, son normales.

140. Probar que $P = x^6 + x^3 + 1$ es irreducible en $\mathbb{Q}[x]$ y utilizarlo para demostrar que la extensión $\mathbb{Q}(e^{2\pi i/9})/\mathbb{Q}$, es normal y de grado 6.

141. Demostrar que toda extensión de grado dos es normal.

142. Dar un ejemplo de una extensión normal que no sea finita.

143. Estudiar si $\mathbb{Q}(x)/\mathbb{Q}(x^3)$ es normal.

144. Dar un ejemplo de una extensión normal de grado 3.

♢**145.** Dar un ejemplo de extensión normal de grado 3 sobre $\mathbb{Q}$. *Indicación*: Buscar un polinomio cuyas raíces sean $\cos(2\pi/7)$, $\cos(4\pi/7)$ y $\cos(6\pi/7)$.

146. Demostrar que dada una extensión finita M/K siempre existe un L, $L \supset M \supset K$ tal que L/K es normal y finita. A un cuerpo con estas características y $[L : K]$ mínimo se le llama *clausura normal* (o cierre normal) de M/K. Probar que sólo hay una clausura normal salvo isomorfismos y hallar la de $\mathbb{Q}(\sqrt[5]{5})/\mathbb{Q}$.

147. Demostrar que $K_1 = \mathbb{F}_2[x]/\langle x^3 + x + 1\rangle$ y $K_2 = \mathbb{F}_2[x]/\langle x^3 + x^2 + 1\rangle$ son cuerpos de descomposición de $x^8 - x \in \mathbb{F}_2[x]$. Concluir que K_1 y K_2 son isomorfos.

148. Probar que $\mathbb{F}_8$ es el cuerpo de descomposición de $x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ y que $\mathbb{F}_8/\mathbb{F}_2$ es simple.

149. ¿Cuál es el grupo aditivo de $\mathbb{F}_8$?

150. Si $P \in \mathbb{F}_p[x]$ es irreducible y gr $P = n$, ¿es su cuerpo de descomposición isomorfo a $\mathbb{F}_{p^n}$?

151. Estudiar si $\mathbb{F}_{64}$ es una extensión de $\mathbb{F}_{16}$ y de $\mathbb{F}_8$ y en su caso hallar el grado.

152. Sea $P = x^q - x$ con $q = p^n$. Demostrar que cualquier polinomio irreducible en $\mathbb{F}_p[x]$ de grado n divide a P.

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

154. Demostrar que si α es una raíz de $x^3 - 2$ en $\mathbb{F}_{7^3}$, entonces -1, α y $-1 + \alpha$ tienen orden (multiplicativo) 2, 9 y 19 respectivamente en el grupo multiplicativo de $\mathbb{F}_{7^3}$. Galois utilizó este hecho para deducir que una raíz de $x^3 - x + 1 \in \mathbb{F}_7[x]$ genera este grupo multiplicativo. Tratar de reconstruir su argumento. *Indicación*: $7^3 - 1 = 2 \cdot 9 \cdot 19$ y en un grupo abeliano $|\langle g\rangle| = n$, $|\langle h\rangle| = m \Rightarrow |\langle gh\rangle| = \text{mcm}(n, m)$.

♢**155.** Probar que el grupo multiplicativo de un cuerpo finito es cíclico. *Indicación*: Estudiar el número de raíces de $x^n - 1$.

∘**156.** Se dice que un cuerpo de característica p es un *cuerpo perfecto* si el morfismo de Frobenius $x \mapsto x^p$ es un isomorfismo. Probar que si K es perfecto todo polinomio irreducible en $K[x]$ es separable. *Indicación*: Tratar de ajustar la prueba vista en el caso $K = \mathbb{F}_p$.

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

♢**158.** Sea K un cuerpo de característica $p > 0$ y supongamos que $P = x^p - x - a$ es irreducible en $K[x]$. Probar que si $\alpha \in L \supset K$ es raíz de P entonces $K(\alpha)/K$ es normal.

159. Sea K un cuerpo de característica $p \neq 0$, y sea $f(x) = x^p - a \in K[x]$. Demostrar que $f(x)$ es irreducible sobre K, o que descompone como producto de factores de grado 1 sobre K.

160. Si $K \subset M \subset L$ con L/K finita, demostrar que L/K separable$\Rightarrow L/M$ separable, pero M/K separable $\not\Rightarrow L/K$ separable.

161. Hallar una extensión separable y normal que no sea finita.

162. Dar un ejemplo de una extensión de grado 3 no separable.

163. Sea K un cuerpo de característica $p \neq 0$. Probar que $x^{p^n} - x$ no tiene raíces repetidas.

164. Sea L/K una extensión algebraica con K un cuerpo de característica $p > 0$. Demostrar que si $\alpha \in L$ es separable sobre K y $\alpha^n \in K$ con n una potencia de la característica, entonces $\alpha \in K$.

165. Sea L/K una extensión algebraica con K un cuerpo de característica $p > 0$. Probar que $\alpha \in L$ es separable sobre K si y sólo si $K(\alpha) = K(\alpha^p)$.

166. Sabiendo que el cuerpo de descomposición de un polinomio sin raíces múltiples da lugar siempre a una extensión separable (lo cual es el contenido de un ejercicio de la próxima sección), probar que los elementos separables sobre un cuerpo siempre forman un cuerpo.

♢♢**167.** Sea L/K finita, a partir de la conclusión del ejercicio anterior, probar que si L/M y M/K son separables, L/K también lo es. *Indicación*: Comenzar probando que para todo $\alpha \in L$ existe n igual a una potencia de $\mathrm{char}(K)$ tal que α^n es separable.

168. ¿Es cierto el recíproco del teorema del elemento primitivo?

♢♢**169.** Demostrar que si $K \subset L$ y $[L : K] < \infty$, la extensión L/K no es simple si y sólo si existen infinitos cuerpos intermedios $K \subset M \subset L$. *Indicación*: Si $L = K(\alpha)$, probar que M debe estar generado sobre K por los coeficientes de algún factor del polinomio mínimo de α.

Sección 3.2

♡**170.** Si $L = K(a_1, \ldots, a_n)$ y σ es un K-automorfismo de L tal que $\sigma(a_i) = a_i$ para todo i, probar que σ es la identidad.

171. Sea L un cuerpo. Demostrar que cualquier automorfismo es un K-automorfismo donde K es la intersección de todos los subcuerpos de L (el llamado *subcuerpo primo*).

172. Demostrar que los conjuntos:

$$A = \{\lambda_1 + \lambda_2\sqrt{7} \ : \ \lambda_1, \lambda_2 \in \mathbb{Q}\} \quad \text{y} \quad B = \left\{\lambda_1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \ : \ \lambda_1, \lambda_2 \in \mathbb{Q}\right\}$$

son espacios vectoriales sobre $\mathbb{Q}$ isomorfos, pero no son cuerpos isomorfos. *Indicación*: Sólo en uno de ellos la ecuación $x^2 + 1 = 0$ tiene solución.

173. ¿Cuáles son los automorfismos de $\mathbb{Q}$? ¿y los $\mathbb{R}$-homomorfismos (homomorfismos que dejan fijo $\mathbb{R}$) de $\mathbb{C}$ en $\mathbb{C}$?

174. Este ejercicio determina $\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$.

i) Probar que cada $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ lleva cuadrados a cuadrados y reales positivos a reales positivos. Concluir que $a < b \Rightarrow \sigma(a) < \sigma(b)$.

ii) Probar que $|a - b| < 1/m \ \Rightarrow \ |\sigma(a) - \sigma(b)| < 1/m$. Concluir que σ es una aplicación continua de $\mathbb{R}$.

iii) Comprobar que una aplicación continua de $\mathbb{R}$ que es la identidad sobre $\mathbb{Q}$ debe ser la identidad en todo $\mathbb{R}$, y por tanto $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = \{\mathrm{Id}\}$.

175. Probar con todo rigor que en $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ la aplicación $\sigma(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$ con $a, b, c, d \in \mathbb{Q}$ es un $\mathbb{Q}$-automorfismo.

176. Hallar el grupo de Galois del cuerpo de descomposición de $x^4 + x^2 - 6$ sobre $\mathbb{Q}$.

177. Encontrar el grupo de Galois de una extensión normal de $\mathbb{Q}$ de grado mínimo conteniendo a $\sqrt{2} + \sqrt[3]{2}$.

178. Calcular el grupo de Galois de la extensión $\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}$.

179. Hallar el grupo de Galois del polinomio $x^4 - 9$ sobre $\mathbb{Q}$.

180. Hallar el grupo de Galois del polinomio $x^4 + 9$ sobre $\mathbb{Q}$.

181. Calcular $\mathcal{G}(L/K)$ donde $K = \mathbb{Q}(e^{2\pi i/5})$ y L es el cuerpo de descomposición de $P = x^5 - 7$ sobre K.

182. Sea $K \subset \mathbb{C}$ el cuerpo de descomposición de $x^2 - x + 1 \in \mathbb{Q}[x]$ y L el de $x^3 - 2$. Hallar $\mathcal{G}(L/K)$.

183. Hallar el grupo de Galois del cuerpo de descomposición de $x^3 - 5 \in \mathbb{Q}[x]$.

184. Recuérdese que el cuerpo de descomposición, L, de $P = x^2 + x + 1 \in \mathbb{F}_2[x]$ es un cuerpo de cuatro elementos. Hallar sus automorfismos y sus $\mathbb{F}_2$-automorfismos.

185. Sea $P \in K[x]$ irreducible de grado tres con $\mathrm{char}(K) = 0$, y sea L su cuerpo de descomposición. Demostrar que o bien $[L : K] = 3$ o bien $[L : K] = 6$.

186. Hallar $\mathcal{G}\big(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})\big)$, $\mathcal{G}\big(\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}(\sqrt{6})\big)$, $\mathcal{G}\big(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}\big)$.

187. Hallar $\mathcal{G}\big(\mathbb{Q}(\sqrt{3}+\sqrt[4]{3})/\mathbb{Q}(\sqrt{3})\big)$.

188. Hallar $\mathcal{G}\big(\mathbb{Q}(\sqrt{5}+\sqrt{7})/\mathbb{Q}\big)$.

189. Sea $P = x^4 - 3x^2 + 4 \in \mathbb{Q}[x]$. Calcular el grupo de Galois de su cuerpo de descomposición sobre $\mathbb{Q}$.

190. Sea $\alpha = \sqrt{2} + i$ y sea P el polinomio mínimo de α sobre $\mathbb{Q}$. Hallar el grupo de Galois del cuerpo de descomposición de P sobre $\mathbb{Q}$.

191. Calcular $\mathcal{G}(\mathbb{Q}(x,y)/\mathbb{Q}(x+y,xy))$ y $\mathcal{G}(\mathbb{Q}(x,y,z)/\mathbb{Q}(x+y+z,xy+xz+yz,xyz))$ donde $\mathbb{Q}(x,y)$ y $\mathbb{Q}(x,y,z)$ denotan los cuerpos de funciones racionales en dos y tres variables respectivamente. *Indicación*: En el primer caso, x e y son raíces del polinomio $X^2 - (x+y)X + xy \in \mathbb{Q}(x+y,xy)[X]$.

♢**192.** Calcular $\mathcal{G}(\mathbb{Q}(x)/\mathbb{Q})$.

193. Hallar un grupo sencillo que sea isomorfo a $\mathcal{G}\big(\mathbb{Q}(e^{2\pi i/13})/\mathbb{Q}\big)$.

♡**194.** ¿Por qué $\mathcal{G}(L/H') \supset H$ es trivial?

195. Probar que si $L = \mathbb{Q}(\cos\frac{2\pi}{17})$, $\mathcal{G}(L/\mathbb{Q}) = \{\mathrm{Id}, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \sigma^6, \sigma^7\} \cong \mathbb{Z}_8$ donde $\sigma\big(2\cos(2\pi/17)\big) = \sigma\big(\zeta + \zeta^{-1}\big) = \zeta^3 + \zeta^{-3}$ con $\zeta = e^{2\pi i/17}$. Demostrar que $\cos(2\pi k/17) \in L$ y que $\sigma(\cos(2\pi k/17)) = \cos(6\pi k/17)$. Si $H = \{\mathrm{Id}, \sigma^4\}$, probar que $H' = \mathbb{Q}(x_1, x_2)$ donde $x_1 = \cos\frac{2\pi}{17} + \cos\frac{26\pi}{17}$ y $x_2 = \cos\frac{2\pi}{17} \cdot \cos\frac{26\pi}{17}$.

196. Encontrar todos los elementos de $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ con $\zeta = e^{2\pi i/7}$ que dejan fijo a $\zeta + \zeta^2 + 3\zeta^3 + \zeta^4 + 3\zeta^5 + 3\zeta^6$.

197. Hallar $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta + \zeta^3 + \zeta^9))$ con $\zeta = e^{2\pi i/13}$.

198. Sean L_1 y L_2 los cuerpos de descomposición de dos polinomios P_1 y P_2 sobre $\mathbb{Q}$. Demostrar que si $L_1 \cap L_2 = \mathbb{Q}$, entonces $\mathcal{G}(L_1/\mathbb{Q}) \times \mathcal{G}(L_2/\mathbb{Q}) \cong \mathcal{G}(L/\mathbb{Q})$ donde L es el cuerpo de descomposición de P_1P_2.

199. Hallar una extensión cuyo grupo de Galois sea isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

200. Si H y N son subgrupos de $\mathcal{G}(L/K)$ cuyos subcuerpos fijos son $H' = L_1$ y $N' = L_2$, indicar qué subcuerpo es $\langle \sigma, \tau \,:\, \sigma \in H,\ \tau \in N\rangle'$.

201. Si $L = \mathbb{Q}(x, y, z)$ y $K = \mathbb{Q}(x + y + z, xy + xz + yz, xyz)$, probar que $\mathbb{Q}\big((x - y)(x - z)(y - z)\big) = \langle \sigma \rangle'$ con σ un elemento de orden 3 de $\mathcal{G}(L/K)$.

♢**202.** Sea L el cuerpo de descomposición de un polinomio sin raíces múltiples. Digamos $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ con $P = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) \in K[x]$, $\alpha_i \neq \alpha_j$. Sea $L_j = K(\alpha_1, \alpha_2, \ldots, \alpha_j)$ y $L_0 = K$. Probar que cada monomorfismo $L_j \longrightarrow L$ se extiende a $[L_{j+1} : L_j]$ monomorfismos $L_{j+1} \longrightarrow L$. Deducir de ello que $|\mathcal{G}(L/K)| = [L : K]$. Concluir finalmente que todos los elementos de L son separables sobre K.

203. Hallar $\mathcal{G}(\mathbb{Q}(x)/\mathbb{Q}(x^n))$, $\mathcal{G}(\mathbb{C}(x)/\mathbb{C}(x^n))$ y $\mathcal{G}(K(x)/K(x^{15}))$ con $K = \mathbb{Q}(e^{2\pi i/3})$, calculando en cada caso los cuerpos que quedan fijos por todos los automorfismos.

204. Hallar $\mathcal{G}(\mathbb{F}_2(x)/\mathbb{F}_2(x^2))$.

205. Consideremos $\zeta = e^{2\pi i/5}$ y sea σ el $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\zeta)$ dado por $\sigma(\zeta) = \zeta^4$. Demostrar que el cuerpo fijo de σ es $\mathbb{Q}(\sqrt{5})$. *Indicación*: Elevar al cuadrado $\frac{1}{2} + \zeta^2 + \zeta^3$.

206. Sea $L = \mathbb{F}_2[x]/\langle x^4 + x^3 + 1\rangle$ y $K = \mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$. Hallar $\mathcal{G}(L/K)$ y comprobar que el orden del morfismo de Frobenius en L es 4.

♡**207.** Si σ tiene orden 4 y $\tau \neq \sigma^2$ tiene orden 2, ¿por qué sabemos que los automorfismos en $\{\mathrm{Id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$ son distintos?

208. Sea L el cuerpo de descomposición en $\mathbb{C}$ del polinomio x^4+1 sobre $\mathbb{Q}$. Encontrar los automorfismos de L con cuerpos fijos $\mathbb{Q}(\sqrt{-2})$ y $\mathbb{Q}(\sqrt{2})$.

209. Sea σ un elemento de $\mathcal{G}(L/K)$ de orden $2n$. Demostrar que para cualquier $\alpha \in L$, $\alpha + \sigma^2(\alpha) + \sigma^4(\alpha) + \cdots + \sigma^{2n-2}(\alpha) \in \langle \sigma^2 \rangle'$.

Sección 3.3

210. Sea $L = \mathbb{Q}(\zeta)$ donde $\zeta = e^{2\pi i/11}$. Demostrar que L es una extensión normal de $\mathbb{Q}$ y determinar su grupo de Galois. Encontrar todos los cuerpos intermedios de la extensión $L/\mathbb{Q}$ y los subgrupos de $\mathcal{G}(L/\mathbb{Q})$ que les corresponden indicando cuáles dan lugar a extensiones normales de $\mathbb{Q}$.

211. Si L/K es una extensión de Galois con grupo de Galois cíclico, probar que dos cuerpos intermedios M_1, M_2 (conteniendo a K) satisfacen $M_1 \subset M_2$ si y sólo si $[L : M_1]$ es un múltiplo de $[L : M_2]$.

212. Sean $K \subset M \subset L$ con L/K de Galois. Probar que $M = K(a)$ con $a \in M$ si y sólo si los únicos elementos de $\mathcal{G}(L/K)$ que fijan a están en $\mathcal{G}(L/M)$. Emplear este resultado para dar una nueva prueba de $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Demostrar de igual manera que $\mathbb{Q}(\sqrt[3]{17}, \sqrt{17}) = \mathbb{Q}(\sqrt[3]{17} + \sqrt{17})$.

♡**213.** Si $K \subset M \subset L$ y L/K es de Galois, ¿deben ser necesariamente L/M y M/K de Galois?

214. Si en una extensión de Galois L/K, con $\text{char}(K) \neq 2$, el grupo de Galois es $\mathbb{Z}_2 \times \mathbb{Z}_2$, demostrar que $L = K(\alpha, \beta)$ con $\alpha^2, \beta^2 \in K$.

215. Sea $\alpha = \sqrt{2} + i$ y sea P el polinomio mínimo de α sobre $\mathbb{Q}$. Hallar todos los subcuerpos de su cuerpo de descomposición sobre $\mathbb{Q}$.

♡**216.** Demostrar que si L es un cuerpo de descomposición de un polinomio sobre $\mathbb{Q}$ y $\mathcal{G}(L/\mathbb{Q})$ es abeliano, entonces $M/\mathbb{Q}$ es normal para todo subcuerpo M, $\mathbb{Q} \subset M \subset L$.

217. Supongamos que $f(x) \in \mathbb{Q}[x]$ es irreducible con $\partial f = 4$ y su cuerpo de descomposición sobre $\mathbb{Q}$ tiene grupo de Galois A_4. Sea θ una raíz de $f(x)$ y sea $L = \mathbb{Q}(\theta)$. Probar que L es una extensión de grado 4 de $\mathbb{Q}$ que no tiene subcuerpos propios. ¿Hay alguna extensión de Galois de $\mathbb{Q}$ de grado cuatro sin subcuerpos propios?

218. Probar que si el grupo de Galois del cuerpo de descomposición de una cúbica sobre $\mathbb{Q}$ es $\mathbb{Z}_3$, entonces todas las raíces de la cúbica son reales.

219. Hallar el grupo de Galois del cuerpo de descomposición de $P = (x^2 - 3)(x^2 + 3)$ sobre $\mathbb{Q}$, calculando los subcuerpos intermedios.

220. Calcular cuántos subcuerpos tiene el cuerpo de descomposición de $P = x^5 + 3x^3 - 3x^2 - 9$ sobre $\mathbb{Q}$.

221. Calcular cuántos subcuerpos tiene el cuerpo de descomposición de $P = x^7 + 4x^5 - x^2 - 4$ sobre $\mathbb{Q}$.

222. Hallar todos los subcuerpos del cuerpo de descomposición sobre $\mathbb{Q}$ de $P = x^4 + 1$.

223. Hallar todos los subcuerpos propios del cuerpo de descomposición de $P = x^4 - 2$ sobre $\mathbb{Q}$.

224. Calcular cuántos subcuerpos tiene $\mathbb{Q}\big(\cos(2\pi/13)\big)$.

225. Estudiar qué automorfismos de $\mathcal{G}\big(\mathbb{Q}(e^{2\pi i/7})/\mathbb{Q}\big)$ dejan invariante $i\,\text{sen}(2\pi/7)$ y utilizar el resultado para hallar $[\mathbb{Q}\big(i\,\text{sen}(2\pi/7)\big) : \mathbb{Q}]$ y $[\mathbb{Q}(e^{2\pi i/7}) : \mathbb{Q}\big(i\,\text{sen}(2\pi/7)\big)]$.

♡**226.** Sabiendo que $L/\mathbb{Q}$ es normal y $[L : \mathbb{Q}] = p$, hallar un grupo isomorfo a $\mathcal{G}(L/\mathbb{Q})$.

227. Si $\mathcal{G}(L/K) \cong \mathbb{Z}_{pq}$ (donde p y q son primos distintos) con L/K normal, finita y separable, ¿cuántos subcuerpos, M, hay con $K \subset M \subset L$?

228. Si $\mathcal{G}(L/\mathbb{Q}) \cong \mathbb{Z}_{p^2q}$ (donde p y q son primos distintos) con $L/\mathbb{Q}$ de Galois, probar que L tiene subcuerpos L_1, L_2, L_3 tales que $[L_1 : \mathbb{Q}] = p$, $[L_2 : \mathbb{Q}] = p^2$ y $[L_3 : \mathbb{Q}] = q$.

229. Sea K un cuerpo de característica cero, y sea E el cuerpo de descomposición de algún polinomio sobre K. Si $\mathcal{G}(E/K)$ es isomorfo a A_4, probar que E no tiene ningún subcuerpo L tal que $[E : L] = 2$.

230. Sea α una raíz de $x^4 + x^3 + 1 \in \mathbb{F}_2[x]$. Hallar β en función de α de tal forma que $\mathbb{F}_2 \subsetneqq \mathbb{F}(\beta) \subsetneqq \mathbb{F}_2(\alpha)$ y dar un polinomio en $\mathbb{F}_2[x]$ cuyo cuerpo de descomposición sea $\mathbb{F}_2(\beta)$.

231. Demostrar que si $\mathbb{Q} \subset M \subset \mathbb{Q}(e^{2\pi i/k})$, entonces $\mathcal{G}(M/\mathbb{Q})$ es abeliano. (Nota: El recíproco, para $M/\mathbb{Q}$ de Galois, es un profundo resultado llamado *teorema de Kronecker-Weber*).

232. Para cada n par hallar un polinomio $P \in \mathbb{Q}[x]$ con $\partial P = n$ y raíces distintas no racionales, tal que el grupo de Galois de su cuerpo de descomposición sea isomorfo a $\mathbb{Z}_2$.

233. Hallar una extensión normal de $\mathbb{Q}$ cuyo grupo de Galois sea $\mathbb{Z}_9$. *Indicación*: $9 = (19 - 1)/2$.

234. Sea L/K una extensión de Galois y sean M_1/K y M_2/K subextensiones de Galois. Demostrar que si M_3 es el menor subcuerpo de L que contiene a M_1 y M_2, entonces $\mathcal{G}(M_3/M_1)$ es isomorfo a $\mathcal{G}(M_2/(M_1 \cap M_2))$.

235. Sea $p = 2q + 1$ con p y q primos, hallar cuántos subcuerpos tiene $\mathbb{Q}(e^{2\pi i/p})$.

236. Sea L un cuerpo y sea G un subgrupo finito del grupo de automorfismos $\phi : L \longrightarrow L$. Sea $K = \{a \in L \ : \ \phi(a) = a, \ \forall \ \phi \in G\}$. *i*) Probar que K es un subcuerpo de L con $[L : K] = |G|$. *ii*) Probar que si L/K es simple, es de Galois. $\diamondsuit$*iii*) Probar incondicionalmente que L/K es de Galois.

237. Demostrar que $\sqrt[3]{n} \in \mathbb{Q}(e^{2\pi i/p})$ con $n \in \mathbb{Z}$ y p primo si y sólo si n es un cubo perfecto.

$\diamondsuit\diamondsuit$**238.** Sea p un primo con $p - 1$ divisible por 4. Demostrar que $\sqrt{n} \in \mathbb{Q}(e^{2\pi i/p})$ con $n \in \mathbb{Z}$ si y sólo si n o n/p son cuadrados perfectos. *Indicación*: Probar que $\sum_{n=1}^{p} e^{2\pi i n^2/p}$ genera la única subextensión de grado 2 de $\mathbb{Q}(e^{2\pi i/p})$.

239. Sea $L = \mathbb{F}_3(\sqrt[3]{x}, \sqrt[3]{y})$ y $K = \mathbb{F}_3(x, y)$. Demostrar que L/K es normal y finita, pero existen infinitos subcuerpos intermedios $K \subset M \subset L$. ¿Por qué esto no contradice el teorema fundamental de la teoría de Galois?

∘**240.** Galois enunció el siguiente lema sin demostración *"Sea una ecuación cualquiera sin raíces iguales, digamos* $a, b, c, \ldots$ *Siempre se puede formar una función* V *de las raíces tal que los valores que se obtienen permutando dichas raíces de todas las formas posibles son todos desiguales. Por ejemplo se puede tomar* $V = Aa + Bb + Cc + \ldots$, *siendo* $A, B, C, \ldots$ *números enteros* [no nulos] *convenientemente elegidos"*. Y después dedujo otro lema: *"La función tomada anteriormente tienen la propiedad de que todas las raíces de la ecuación propuesta se expresan racionalmente en función de* V*"*. En notación moderna esto es $a, b, c, \cdots \in K(V)$ donde K es el cuerpo generado por los coeficientes de la ecuación. Probar estos resultados (para $K \subset \mathbb{C}$). *Indicación*: El primero se cumple para números complejos arbitrarios. Para el segundo, Galois aplicó el teorema de los polinomios simétricos al producto de factores $(Ax + Bb + Cc + \cdots - V)$ permutando de todas las formas posibles $b, c, \ldots$ pero sin cambiar V.

Ejercicios del Capítulo 4

LEYENDA: ♡ fácil, ♢ difícil, ♢♢ muy difícil, ∘ opcional.

Sección 4.1

♡**241.** Probar que si un grupo finito no trivial G no tiene subgrupos propios, $G \cong \mathbb{Z}_p$.

242. Si un grupo soluble tiene como cocientes $\mathbb{Z}_2$ y $\mathbb{Z}_3$, apareciendo en ese orden, ¿puede encontrarse siempre otra serie de composición de manera que aparezcan en orden inverso?

♡**243.** Dar una serie de composición para $\mathbb{Z}_{p^k}$.

244. Deducir del ejercicio anterior y del teorema de clasificación de grupos abelianos finitos que todo grupo abeliano finito es soluble.

245. Hallar tres series de composición distintas para $\mathbb{Z}_{15} \times S_3$.

246. Hallar una serie de composición para D_{10}.

♡**247.** Hallar $H_1 \subset H_2 \subset G$ tales que $H_1 \lhd H_2$, $H_2 \lhd G$ pero de modo que H_1 no sea normal en G.

♡**248.** Demostrar que todo subgrupo de índice dos es normal.

249. Sean $K \subset M \subset L$ con M/K y L/K extensiones de Galois, demostrar que si $\mathcal{G}(L/K)$ es soluble, entonces $\mathcal{G}(M/K)$ también lo es.

250. Demostrar que si G y H son solubles entonces su producto directo $G \times H$ también lo es.

251. Demostrar que S_4 es soluble.

252. Dar dos series de composición para S_4.

253. Dado un grupo finito G se define su *conmutador* como $C(G) = \langle g^{-1}h^{-1}gh \ : \ g, h \in G\rangle$. Demostrar que $C(G)$ es un subgrupo normal y $G/C(G)$ es abeliano. Deducir que si $C(G)$ es soluble, G también lo es.

254. Demostrar que una cadena de subgrupos normales $\{e\} = G_0 \subsetneqq G_1 \subsetneqq G_2 \cdots \subsetneqq G_n = G$, $G_i \triangleleft G_{i+1}$, $0 \leq i < n$, no es serie de composición si y sólo si para algún i existe un subgrupo H tal que $G_i \triangleleft H \triangleleft G_{i+1}$ con $H \neq G_i, G_{i+1}$.

255. Demostrar con detalle que todo grupo finito tiene al menos una serie de composición.

256. Demostrar que un grupo G es soluble si y sólo si existe una cadena de subgrupos $\{e\} = G_0 \triangleleft G_1 \triangleleft G_2 \cdots \triangleleft G_n = G$, tal que G_{i+1}/G_i es abeliano, $0 \leq i < n$.

257. Dado un grupo G sea $l(G)$ la longitud de su serie de composición (el teorema de Jordan-Hölder asegura que está bien definida). Demostrar que si $H \subsetneqq G$ y G es soluble, entonces $l(H) < l(G)$. Nota: Si G no es soluble, hay contraejemplos.

258. Hallar todas las series de composición de $\mathbb{Z}_4 \times S_3$.

∘**259.** Proceder como en la prueba del teorema de Jordan-Hölder para deducir que si $N_1 \triangleleft H_1 \triangleleft G$, $N_2 \triangleleft H_2 \triangleleft G$, entonces $N_1(H_1 \cap H_2)/N_1(H_1 \cap N_2) \cong H_1 \cap H_2/(H_1 \cap N_2)(H_2 \cap N_1)$.

♢**260.** Se llaman *clases de conjugación* en un grupo G, a las clases de equivalencia de la relación $g_1 \mathcal{R} g_2 \Leftrightarrow g_1 = h^{-1}g_2h$. Demostrar que el cardinal de cada clase de conjugación divide a $|G|$. *Indicación*: Definir $H_g = \{h \in G \ : \ h^{-1}gh = g\}$ y probar que hay una biyección entre los elementos de la clase de conjugación que contiene a g y los cogrupos de G/H_g.

♢**261.** Demostrar que en un grupo de orden p^n, con p primo, las clases de conjugación con un solo elemento conforman un subgrupo normal no trivial. Deducir de ello que todo grupo de orden p^n es soluble.

♢♢**262.** Demostrar que cualquier grupo de orden 100 es soluble. *Indicación*: La dificultad radica en gran medida en recordar los teoremas de Sylow.

Sección 4.2

♡**263.** Demostrar que todo $P \in \mathbb{R}[x]$ es soluble por radicales.

264. Demostrar que M/K radical y L/M radical $\Rightarrow L/K$ radical.

265. Si $\alpha, \beta \in \mathbb{C}$ están en sendas extensiones radicales de $\mathbb{Q}$, probar que $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ es radical.

266. Sea α en una extensión radical de K. Probar que $L(\alpha)/K(\alpha)$ radical $\Rightarrow L/K$ radical.

♡**267.** Probar que si una raíz de un polinomio irreducible en $\mathbb{Q}[x]$ está en una extensión radical, entonces lo están todas.

268. Dar tres ejemplos de quínticas no solubles por radicales.

269. Probar que si las raíces de $P \in \mathbb{Q}[x]$ son iguales salvo multiplicar por elementos de K, entonces P es soluble por radicales. *Indicación*: La terminología "abeliano" viene del estudio que hizo Abel de este tipo de polinomios.

270. Sea $P \in \mathbb{Q}[x]$ un polinomio irreducible de grado primo $\partial P = p > 3$. Usando un resultado de teoría de grupos se puede probar que el grupo de Galois G de su cuerpo de descomposición tiene un elemento de orden p. Dando esto por supuesto, demostrar que si P tiene exactamente dos raíces complejas entonces $G \cong S_p$ y P no es soluble por radicales.

271. Demostrar que existe $P \in \mathbb{Q}[x]$ con $\partial P = 5$ y $\mathcal{G}(L/\mathbb{Q}) \cong \mathbb{Z}_5$, donde L es el cuerpo de descomposición de L.

272. Probar detalladamente que $\{\mathrm{Id}\} \subset \langle\sigma\rangle \subset \langle\sigma, \tau\rangle \subset A_4 \subset S_4$ con $\sigma = (1,2)(3,4)$ y $\tau = (1,3)(2,4)$, es realmente una serie de composición de S_4.

273. Demostrar que para resolver una ecuación de cuarto grado, se necesitan a lo más raíces cuadradas y cúbicas.

274. Verificar que si $\alpha = (1,2,3,4,5)$ ó $\alpha = (1,2)(3,4)$ entonces $(3,4,5)^{-1}\alpha^{-1}(3,4,5)\alpha$ es un 3-ciclo.

275. Explicar por qué los 3-ciclos en S_n generan todas las permutaciones pares.

276. Refinar el problema anterior, probando que los 3-ciclos de la forma $(1,a,b) \in S_n$ generan A_n.

♡**277.** Dar un ejemplo de un polinomio de sexto grado no soluble por radicales.

278. Sea P un polinomio irreducible de $\mathbb{Q}[x]$ con $\partial P = 4$ y cuerpo de descomposición L. Demostrar que si P tiene dos raíces reales, entonces $\mathcal{G}(L/Q)$ es isomorfo a S_4 o a D_8.

♢**279.** Sea un subgrupo $H \subset G$ tal que H no contiene a ningún subgrupo normal no trivial de G. Probar que G es isomorfo a un subgrupo de S_m con $m = |G|/|H|$. Deducir de ello que al permutar las variables de una función $f \in K[x_1, x_2, \ldots, x_n]$ de todas las formas posibles, si se obtienen más de dos funciones distintas, entonces se obtienen al menos n. *Indicación*: Comenzar probando que cada $g \in G$ está totalmente determinado por su acción sobre los cogrupos de G/H.

♢♢**280.** Sea $L/\mathbb{Q}$ una extensión de Galois tal que para cualquier par de subcuerpos M_1, M_2, hay una relación de inclusión (esto es, $M_1 \subset M_2$ o $M_2 \subset M_1$). Demostrar que $L/\mathbb{Q}$ es radical. *Indicación*: Utilizar los teoremas de Sylow y que por un problema anterior los grupos de orden p^n son solubles.

281. Usando un resultado de teoría de grupos que implica que un grupo de orden múltiplo de orden 5 siempre tiene un elemento de orden 5, simplificar la prueba de que $P \in \mathbb{Q}[x]$, $\partial P = 5$, irreducible con exactamente tres raíces reales $\Rightarrow$ P no es soluble por radicales.

♢♢**282.** Sea $P \in \mathbb{Q}[x]$ irreducible de grado primo p y sea L su cuerpo de descomposición. Demostrar que si P es soluble por radicales entonces cualquier serie de composición de $\mathcal{G}(L/\mathbb{Q})$ debe tener primer grupo no trivial $G_1 \cong \mathbb{Z}_p$.

Sección 4.3

283. Hallar los posibles grupos de Galois de una cúbica no irreducible en $\mathbb{Q}[x]$.

284. Demostrar que si $\alpha_1, \alpha_2, \alpha_3$ y α_4 son raíces de $P \in \mathbb{Q}[x]$, $\partial P = 4$, entonces $\alpha_1\alpha_2 + \alpha_3\alpha_4$, $\alpha_1\alpha_3 + \alpha_2\alpha_4$, $\alpha_1\alpha_4 + \alpha_2\alpha_3$ son raíces de cierto $Q \in \mathbb{Q}[x]$ con $\partial Q = 3$ y se cumple $\Delta_4(P) = \Delta_3(Q)$.

285. Sea L el cuerpo de descomposición de polinomio de cuarto grado irreducible sobre $\mathbb{Q}$. Demostrar que $\mathcal{G}(L/\mathbb{Q})$ es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4$, D_8, A_4 o S_4.

286. Encontrar ejemplos explícitos de polinomios de cuarto grado irreducibles sobre $\mathbb{Q}$, tales que el grupo de Galois de su cuerpo de descomposición sea isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ y a $\mathbb{Z}_4$.

287. Resolver con radicales $x^3 + x + 3 = 0$.

288. Demostrar que si $P \in \mathbb{Q}[x]$ es un polinomio cúbico irreducible y α es una de sus raíces, su cuerpo de descomposición es $L = \mathbb{Q}(\sqrt{\Delta}, \alpha)$.

289. Sea $P \in \mathbb{Q}[x]$ irreducible de grado n. Demostrar que $\sqrt{\Delta_n(P)} \in \mathbb{Q}$ si y sólo si el grupo de Galois (identificado como grupo de permutaciones de las raíces) de su cuerpo de descomposición es un subgrupo de A_n.

290. Sea K un cuerpo de característica distinta de 2 y $x^4+ax^2+b \in K[x]$ irreducible. Probar que el grupo de Galois de su cuerpo de descomposición es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ si $\sqrt{b} \in K$; es isomorfo a $\mathbb{Z}_4$ si $\sqrt{b} \notin K$ y $\sqrt{b(a^2-4b)} \in K$; y es isomorfo a D_8 si $\sqrt{b} \notin K$ y $\sqrt{b(a^2-4b)} \notin K$;

291. Si $P \in \mathbb{Q}[x]$ es un polinomio irreducible de tercer grado con sus tres raíces reales, probar que no existe ninguna extensión radical real que contenga a las tres. Esto es, no se puede resolver la ecuación $P(x) = 0$ sólo con radicales reales.

292. Probar con detalle que el polinomio mínimo sobre $\mathbb{Q}$ de $e^{2\pi i/n}$ debe pertenecer a $\mathbb{Z}[x]$.

$\diamondsuit$**293.** Demostrar que el polinomio mínimo de $e^{2\pi i/n}$ sobre $\mathbb{Q}$ es $P = \prod_{d|n}(x^{n/d}-1)^{\mu(d)}$, donde $\mu(d)$ es la función de Möbius, que vale 1 si $d = 1$, $(-1)^r$ si d es producto de r primos distintos, y cero en otro caso. Utilizar este resultado para hallar el polinomio mínimo sobre $\mathbb{Q}$ de $e^{\pi i/10}$.

294. Demostrar que el polinomio mínimo de $e^{2\pi i/p^2}$ sobre $\mathbb{Q}$ es $x^{p(p-1)} + x^{p(p-2)} + \cdots + x^p + 1$.

295. Demostrar con detalle que si p es primo, todos los coeficientes del polinomio $(a_n x^{np} + a_{n-1}x^{(n-1)p} + \cdots + a_1 x^p + a_0) - (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)^p$ son divisibles por p.

296. Hallar todos los n menores que 260 tales que el polígono regular de n lados sea construible con regla y compás.