Ejercicios del Capítulo 2

Leyenda: $\heartsuit$ fácil, $\diamondsuit$ difícil, $\diamondsuit\diamondsuit$ muy difícil, $\circ$ opcional.

Sección 2.1

$\heartsuit$**1.** Demostrar que $\mathbb{Z}/6\mathbb{Z}$ no es un cuerpo. Hallar las unidades.

2. 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 $AP + BQ$.

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

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

5. 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 $x - a$.

6. 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 $\{1, \overline{x}, \overline{x}^2\}$.

7. 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.

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

9. 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 $\mathbb{Q}$.

10. 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 $s \in K$.

11. 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 $\sqrt[3]{5}$.

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

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

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

15. 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

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

17. 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.

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

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

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

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

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

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

23. 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.

$\diamondsuit$**24.** 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.

$\diamondsuit$**25.** 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

26. 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) $\mathbb{Q}(\sqrt{5}, \sqrt[6]{5})/\mathbb{Q}(\sqrt{5})$

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

$\heartsuit$**28.** Probar que $A/\mathbb{Q}$ es una extensión infinita, donde $A \subset \mathbb{C}$ son los números algebraicos sobre $\mathbb{Q}$.

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

30. 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 $[L : K]$.

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

32. 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 $\mathrm{mcm}(n_\alpha, n_\beta) | n$ 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 $n < n_\alpha \cdot n_\beta$.

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

34. 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 $\mathbb{Q}$.

$\heartsuit$**35.** 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.

$\heartsuit$**36.** 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 $\mathbb{Q}(\beta)$.

$\heartsuit$**37.** Si α es trascendente sobre K, ¿cuál es el grado de $K(\alpha)/K$?

38. 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.

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

40. 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.

41. 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.

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

43. 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.

44. 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.

$\diamondsuit$**45.** Calcular el polinomio mínimo de $\sqrt[3]{9} + \sqrt[3]{3} - 1$.

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

47. 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 $\mathbb{Q}\big(e^{2\pi i/p}\big)/\mathbb{Q}$.

48. 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 $\mathbb{Q}(\sqrt{nm})$.

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

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

51. 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.

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

$\diamondsuit$**53.** Probar que $\mathbb{R}$ no es una extensión simple de $\mathbb{Q}$.

$\diamondsuit$**54.** 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

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

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

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

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

58. 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.

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

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

$\diamondsuit$**61.** Crear un método para construir el pentágono regular.

62. 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).

63. 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.

64. 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.

65. ¿Se puede triplicar el cubo?

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

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

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

68. 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.

69. 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.

70. 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?

$\diamondsuit$**71.** Sea $P(x) = x^n(1-x)^n/n!$. Probar que si π^2 fuera una fracción con numerador a, entonces $E_n = a^n\pi \int_0^1 P(x) \operatorname{sen}(\pi x)\, dx$ sería un entero no nulo para todo n. Demostrar que $\lim E_n = 0$, llegando a una contradicción con que $\pi^2 \in \mathbb{Q}$.