Ejercicios del Capítulo 3

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

Sección 3.1

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

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

3. 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.

4. 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.

5. 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.

6. 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 $[E : K] = 2$.

7. 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.

8. 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.

9. 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.

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

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

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

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

$\diamondsuit$**14.** 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 $\cos(6\pi/7)$.

15. 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 $\mathbb{Q}(\sqrt[5]{5})/\mathbb{Q}$.

16. 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.

17. 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.

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

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

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

21. 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.

22. 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.

23. 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 $|\langle g\rangle| = n$, $|\langle h\rangle| = m \Rightarrow |\langle gh\rangle| = \mathrm{mcm}(n,m)$.

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

∘**25.** 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 $K = \mathbb{F}_p$.

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

◊**27.** 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.

28. 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.

29. 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.

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

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

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

33. 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 $\alpha \in K$.

34. 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 $K(\alpha) = K(\alpha^p)$.

35. 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.

♢♢**36.** 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 $\operatorname{char}(K)$ tal que α^n es separable.

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

♢♢**38.** 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

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

40. 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*).

41. 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.

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

43. Este ejercicio determina $\operatorname{Aut}(\mathbb{R}/\mathbb{Q})$.

i) Probar que cada $\sigma \in \operatorname{Aut}(\mathbb{R}/\mathbb{Q})$ 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 $\text{Aut}(\mathbb{R}/\mathbb{Q}) = \{\text{Id}\}$.

44. 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.

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

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

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

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

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

50. 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.

51. 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 $\mathcal{G}(L/K)$.

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

53. 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.

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

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

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

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

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

59. 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 $\mathbb{Q}$.

60. 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 $X^2-(x+y)X+xy\in\mathbb{Q}(x+y,xy)[X]$.

$\diamondsuit$**61.** Calcular $\mathcal{G}(\mathbb{Q}(x)/\mathbb{Q})$.

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

$\heartsuit$**63.** ¿Por qué $\mathcal{G}(L/H')\supset H$ es trivial?

64. 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 $x_2 = \cos\frac{2\pi}{17} \cdot \cos\frac{26\pi}{17}$.

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

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

67. 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.

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

69. 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 $\langle \sigma, \tau \ :\ \sigma \in H,\ \tau \in N\rangle'$.

70. 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 $\mathcal{G}(L/K)$.

$\diamondsuit$**71.** Sea L el cuerpo de descomposición de un polinomio sin raíces múltiples. Digamos $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$ con $P = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) \in K[x]$, $\alpha_i \neq \alpha_j$. Sea $L_j = K(\alpha_1, \alpha_2, \dots, \alpha_j)$ 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.

72. 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.

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

74. 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 $\frac{1}{2} + \zeta^2 + \zeta^3$.

75. 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.

$\heartsuit$**76.** 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?

77. 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 $\mathbb{Q}(\sqrt{2})$.

78. 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

79. 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 $\mathbb{Q}$.

80. 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 $[L : M_2]$.

81. 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 $\mathbb{Q}(\sqrt[3]{17}, \sqrt{17}) = \mathbb{Q}(\sqrt[3]{17} + \sqrt{17})$.

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

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

84. 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 $\mathbb{Q}$.

♡**85.** 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, $\mathbb{Q} \subset M \subset L$.

86. 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?

87. 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.

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

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

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

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

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

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

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

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

96. 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 $K \subset M \subset L$?

97. 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 $[L_3 : \mathbb{Q}] = q$.

98. 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 $[E : L] = 2$.

99. 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 $\mathbb{F}_2(\beta)$.

100. 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*).

101. 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 $\mathbb{Z}_2$.

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

103. 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 $\mathcal{G}(M_2/(M_1 \cap M_2))$.

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

105. 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.

106. 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.

$\diamondsuit\diamondsuit$**107.** 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 $\mathbb{Q}(e^{2\pi i/p})$.

108. 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?

$\circ$**109.** 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 $a, b, c, \dots \in K(V)$ 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 $(Ax + Bb + Cc + \dots - V)$ permutando de todas las formas posibles $b, c, \ldots$ pero sin cambiar V.