Ejercicios del Capítulo 4

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

Sección 4.1

$\heartsuit$**1.** Probar que si un grupo finito no trivial G no tiene subgrupos propios, $G \cong \mathbb{Z}_p$.

2. 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?

$\heartsuit$**3.** Dar una serie de composición para $\mathbb{Z}_{p^k}$.

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

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

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

$\heartsuit$**7.** 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.

$\heartsuit$**8.** Demostrar que todo subgrupo de índice dos es normal.

9. 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.

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

11. Demostrar que S_4 es soluble.

12. Dar dos series de composición para S_4.

13. 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.

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

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

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

17. 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.

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

$\circ$**19.** 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 $N_1(H_1 \cap H_2)/N_1(H_1 \cap N_2) \cong H_1 \cap H_2/(H_1 \cap N_2)(H_2 \cap N_1)$.

$\diamondsuit$**20.** Se llaman *clases de conjugación* en un grupo G, a las clases de equivalencia de la relación $g_1 \mathcal{R} g_2 \Leftrightarrow g_1 = h^{-1} g_2 h$. 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.

$\diamondsuit$**21.** 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.

$\diamondsuit\diamondsuit$**22.** 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

$\heartsuit$**23.** Demostrar que todo $P \in \mathbb{R}[x]$ es soluble por radicales.

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

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

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

$\heartsuit$**27.** Probar que si una raíz de un polinomio irreducible en $\mathbb{Q}[x]$ está en una extensión radical, entonces lo están todas.

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

29. 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.

30. 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.

31. 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.

32. 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.

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

34. 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.

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

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

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

38. 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.

♢**39.** 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 $f \in K[x_1, x_2, \dots, x_n]$ 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.

♢♢**40.** 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.

41. 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.

♢♢**42.** 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

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

44. 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 $\Delta_4(P) = \Delta_3(Q)$.

45. 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.

46. 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 $\mathbb{Z}_4$.

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

48. 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 $L = \mathbb{Q}(\sqrt{\Delta}, \alpha)$.

49. 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.

50. 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 $\sqrt{b(a^2 - 4b)} \notin K$;

51. 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.

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

$\diamondsuit$**53.** 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 $e^{\pi i/10}$.

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

55. 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.

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