Ejercicios

Sección 18 Anillos y Campos 1-28,34-51,54-56.
Sección 21 El campo de cocientes de un dominio integral 1,2,6,7,8,$\cdots$,17.
Sección 22 Anillo de polinomios 1-17 (impares) 24,25,26,27,28,19,30,31
Sección 23 Factorización de un polinomio sobre un campo 1-22, 34-37
Sección 26 Homomorfismos y anillos de factores 1-4, 17-25,38
Sección 27 Ideales primos y máximos 1-9, 24-38

Ejercicios 18

Cálculos

En los ejercicios del 1 al 6, calcula el producto en el anillo dado.

1. $(12)(16)$ en $\mathbb{Z}_{24}$ **Solución:** 0
2. $(16)(3)$ en $\mathbb{Z}_{32}$ **Solución:** 16
3. $(11)(-4)$ en $\mathbb{Z}_{15}$ **Solución:** 1
4. $(20)(-8)$ en $\mathbb{Z}_{26}$ **Solución:** 22
5. $(2,3)(3,5)$ en $\mathbb{Z}_5 \times \mathbb{Z}_9$ **Solución:** $(1,6)$
6. $(-3,5)(2,-4)$ en $\mathbb{Z}_4 \times \mathbb{Z}_{11}$ **Solución:** $(2,2)$

En los ejercicios del 7 al 13, decide si las operaciones de suma y multiplicación están definidas (cerradas) en el conjunto, y da una estructura de anillo. Si no se forma un anillo, explica por qué. Si se forma un anillo, indica si es conmutativo, si tiene unidad y si es un campo.

7. $n\mathbb{Z}$ con la suma y multiplicación usuales
   Solución: Sí, nZ para $n \in Z^+$ es un anillo conmutativo, pero sin elemento de unidad a menos que $n = 1$, y no es un campo.
8. $\mathbb{Z}^+$ con la suma y multiplicación usuales
   Solución: No, Z^+ no es un anillo; no hay identidad para la adición.
9. $\mathbb{Z}\times\mathbb{Z}$ con la suma y multiplicación por componentes
   Solución: Sí, $Z \times Z$ es un anillo conmutativo con unidad $(1,1)$, pero no es un campo porque $(2,0)$ no tiene inverso multiplicativo.
10. $2\mathbb{Z} \times \mathbb{Z}$ con la suma y multiplicación por componentes
    Solución: Sí, $2Z \times Z$ es un anillo conmutativo, pero sin elemento de unidad, y no es un campo.
11. Sea $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ con las operaciones de suma y multiplicación usuales.
    Solución: Sí, $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ es un anillo conmutativo con unidad, pero no es un campo porque el número 2 no tiene inverso multiplicativo.
12. Sea $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ con las operaciones de suma y multiplicación usuales.
    Solución: Sí, $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ es un anillo conmutativo con unidad y es un campo porque $\sqrt{2}$ tiene inverso multiplicativo.
13. Conjunto de todos los números complejos imaginarios puros ri para $r \in \mathbb{R}$ con las operaciones de suma y multiplicación usuales.
    Solución: No, R_i no está cerrado bajo la multiplicación.

En los Ejercicios del 14 al 19, Describa todas las unidades en el anillo dado:

14. $\mathbb{Z}$ **Solución:** En $\mathbb{Z}$: 1 y -1.
15. $\mathbb{Z} \times \mathbb{Z}$ **Solución:** En $\mathbb{Z} \times \mathbb{Z}$: $(1,1)$, $(1,-1)$, $(-1,1)$, y $(-1,-1)$.
16. $\mathbb{Z}_5$ **Solución:** En $\mathbb{Z}_5$: 1, 2, 3, y 4.
17. $\mathbb{Q}$ **Solución:** En $\mathbb{Q}$: Todos los elementos no nulos.
18. $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$ **Solución:** En $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$: $(1,q,1)$, $(-1,q,1)$, $(1,q,-1)$, y $(-1,q,-1)$ para cualquier $q \in \mathbb{Q}$ no nulo.
19. $\mathbb{Z}_4$ **Solución:** En $\mathbb{Z}_4$: 1 y 3.

20. Considere el anillo de matrices $M_2(\mathbb{Z}_2)$.

    a) Encuentre el orden del anillo, es decir, el número de elementos en él.

    b) Liste todas las unidades en el anillo.

    Solución:

    a) El orden del anillo es $2^4 = 16$.

    b) Las unidades son las matrices I_2, $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$, $\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}$, $\begin{bmatrix}0 & 1\\0 & 1\end{bmatrix}$, y $\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}$.

21. Si es posible, proporcione un ejemplo de un homomorfismo $\phi : R \to R'$, donde R y R' son anillos con unidad $1_R \neq 0_R$ y $1_{R'} \neq 0_{R'}$, y donde $\phi(1_R) \neq 0_{R'}$ y $\phi(1_R) \neq 1_{R'}$.
    Solución: (Ver respuesta en el texto).

22. (Álgebra lineal) Considere la aplicación det de $M_n(\mathbb{M})$ en $\mathbb{M}$, donde $\det(A)$ es el determinante de la matriz A para $A \in M_n(\mathbb{M})$. ¿Es det un homomorfismo de anillos? ¿Por qué o por qué no?
    Solución: Debido a que $\det(A+B)$ no tiene por qué ser igual a $\det(A) + \det(B)$, se concluye que det no es un homomorfismo de anillos. Por ejemplo, $\det(I_n + I_n) = 2^n$, pero $\det(I_n) + \det(I_n) = 1 + 1 = 2$.

23. Describa todos los homomorfismos de anillos de $\mathbb{Z}$ en $\mathbb{Z}$.
    Solución: Sea $\phi : \mathbb{Z} \to \mathbb{Z}$ un homomorfismo de anillos. Debido a que $1^2 = 1$, se deduce que $\phi(1)$ debe ser un entero cuyo cuadrado es igual a sí mismo, es decir, 0 o 1. Si $\phi(1) = 1$, entonces $\phi(n) = \phi(n \cdot 1) = n$, por lo que ϕ es la identidad en $\mathbb{Z}$. Si $\phi(1) = 0$, entonces $\phi(n) = \phi(n \cdot 1) = 0$, lo que también da un homomorfismo. Por lo tanto, hay dos homomorfismos posibles.

24. Describa todos los homomorfismos de anillos de $\mathbb{Z}$ en $\mathbb{Z} \times \mathbb{Z}$.
    Solución: Como en la solución anterior, se concluye que hay cuatro homomorfismos posibles: $\phi_1(n) = (0, 0)$, $\phi_2(n) = (n, 0)$, $\phi_3(n) = (0, n)$, y $\phi_4(n) = (n, n)$.

25. Describa todos los homomorfismos de anillos de $\mathbb{Z} \times \mathbb{Z}$ en $\mathbb{Z}$.
    Solución: Similar a las soluciones anteriores, hay cuatro homomorfismos posibles: $\phi_1(n, m) = 0$, $\phi_2(n, m) = n$, $\phi_3(n, m) = m$, y $\phi_4(n, m) = n + m$. Sin embargo, ϕ_4 no es un homomorfismo porque $\phi_4(n, m) \neq (n+m)\cdot(1, 1) = (n+m, n+m)$ para algunos $n, m \in \mathbb{Z}$.

26. ¿Cuántos homomorfismos hay de $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ en $\mathbb{Z}$?
    Solución: Similar a la solución anterior, hay cuatro homomorfismos posibles: $\phi_1(n, m, p) = 0$, $\phi_2(n, m, p) = n$, $\phi_3(n, m, p) = m$, y $\phi_4(n, m, p) = p$.

27. Considere la solución de la ecuación $X^2 = I_3$ en el anillo $M_3(\mathbb{R})$. Si $X^2 = I_3$ implica $X^2 - I_3 = 0$, la matriz cero, entonces factorizando, obtenemos $(X - I_3)(X + I_3) = 0$, de donde $X = I_3$ o $X = -I_3$. ¿Es correcto este razonamiento? Si no lo es, señale el error y, si es posible, proporcione un contraejemplo para la conclusión.
    Solución: (Ver respuesta en el texto).

28. Encuentre todas las soluciones de la ecuación $x^2+x-6 = 0$ en el anillo $\mathbb{Z}_{14}$ mediante la factorización del polinomio cuadrático. Compare con el Ejercicio 27.
    Solución: Las soluciones de $x^2 + x - 6 = 0$ en $\mathbb{Z}_{14}$ son $x = 2$, $x = 4$, $x = 9$, y $x = 11$.

Conceptos

En los Ejercicios 29 y 30, corrige la definición del término en cursiva sin hacer referencia al texto, si es necesario, de manera que esté en una forma aceptable para su publicación.

29. Un *campo* F es un anillo con unidad no nula tal que el conjunto de elementos no nulos de F es un grupo bajo la multiplicación.

Solución: La definición es incorrecta. Inserta la palabra "conmutativo" antes de "anillo" o "grupo". Un campo F es un anillo conmutativo con unidad no nula tal que el conjunto de elementos no nulos de F es un grupo bajo la multiplicación.

30. Una unidad en un anillo es un elemento con inverso multiplicativo.
Solución: La definición es incorrecta. No hemos definido ningún concepto de magnitud para elementos de un anillo. Una unidad en un anillo con unidad no nula es un elemento que tiene un inverso multiplicativo.

31. Da un ejemplo de un anillo que tenga dos elementos a y b tales que $ab = 0$, pero ninguno de los dos es cero.
Solución: En el anillo $\mathbb{Z}_6$, tenemos $2 \cdot 3 = 0$, así que tomamos $a = 2$ y $b = 3$.

32. Da un ejemplo de un anillo con unidad $1 \neq 0$ que tenga un subanillo con unidad no nula $1' \neq 1$. [Pista: Considera un producto directo o un subanillo de $\mathbb{Z}_6$.]
Solución: $\mathbb{Z} \times \mathbb{Z}$ tiene unidad $(1, 1)$; sin embargo, el subanillo $\mathbb{Z} \times \{0\}$ tiene unidad $(1, 0)$. Además, $\mathbb{Z}_6$ tiene unidad 1, mientras que el subanillo $\{0, 2, 4\}$ tiene unidad 4 y el subanillo $\{0, 3\}$ tiene unidad 3.

33. Marca cada afirmación como verdadera o falsa:

    a) Todo campo es también un anillo. **Verdadero**

    b) Todo anillo tiene una identidad multiplicativa. **Falso**

    c) Todo anillo con unidad tiene al menos dos unidades. **falso**

    d) Todo anillo con unidad tiene a lo sumo dos unidades. **Falso**

    e) Es posible que un subconjunto de algún campo sea un anillo pero no un subcampo, bajo las operaciones inducidas. **Verdadero**

    f) Las leyes distributivas para un anillo no son muy importantes. **Falso**

    g) La multiplicación en un campo es conmutativa. **Verdadero**

    h) Los elementos no nulos de un campo forman un grupo bajo la multiplicación en el campo. **Verdadero**

    i) La suma en todo anillo es conmutativa. **Falso**

    j) Todo elemento en un anillo tiene un inverso aditivo. **Verdadero**

Teoría

34. Demuestra que la multiplicación definida en el conjunto F de funciones en el Ejemplo 18.4 satisface los axiomas M2 y M3 para un anillo.
Solución: Sean $f, g, h \in F$. Ahora, $[(fg)h](x) = [(fg)(x)]h(x) = [f(x)g(x)]h(x)$. Debido a que la multiplicación en R es asociativa, continuamos con $[f(x)g(x)]h(x) = f(x)[g(x)h(x)] = f(x)[(gh)(x)] = [f(gh)](x)$. Así que $(fg)h$ y $f(gh)$ tienen el mismo valor en cada $x \in R$, por lo que son la misma función y el axioma 2 se cumple. Para el axioma 3, usamos las leyes distributivas en R y tenemos $[f(g+h)](x) = f(x)[(g+h)(x)] = f(x)[g(x)+h(x)] = f(x)g(x)+g(x)h(x) = (fg)(x) + (fh)(x) = (fg + fh)(x)$, por lo que $f(g+h)$ y $fg+fh$ son la misma función y se cumple la ley distributiva izquierda. La ley distributiva derecha se demuestra de manera similar.

35. Muestra que el mapa de evaluación Φ del Ejemplo 18.10 satisface el requisito multiplicativo para un homomorfismo.
Solución: Para $f, g \in F$, tenemos $\Phi_a(f + g) = (f + g)(a) = f(a) + g(a) = \Phi_a(f) + \Phi_a(g)$. Pasando a la multiplicación, tenemos $\Phi_a(fg) = (fg)(a) = f(a)g(a) = \Phi_a(f)\Phi_a(g)$. Así que Φ_a es un homomorfismo.

36. Completa el argumento esbozado después de las Definiciones 18.12 para demostrar que el isomorfismo proporciona una relación de equivalencia en una colección de anillos.
Solución: Solo necesitamos verificar la propiedad multiplicativa.

- Reflexiva: El mapa de identidad ι de un anillo R en sí mismo satisface $\iota(ab) = ab = \iota(a)\iota(b)$, por lo que se cumple la propiedad reflexiva.
- Simétrica: Sea $\phi : R \to R_0$ un isomorfismo. Sabemos de la teoría de grupos que $\phi^{-1} : R_0 \to R$ es un isomorfismo del grupo aditivo de R_0 con el grupo aditivo de R. Para $\phi(a), \phi(b) \in R_0$, tenemos $\phi^{-1}(\phi(a)\phi(b)) = \phi^{-1}(\phi(ab)) = ab = \phi^{-1}(\phi(a))\phi^{-1}(\phi(b))$.
- Transitiva: Sean $\phi : R \to R_0$ y $\psi : R_0 \to R_{00}$ isomorfismos de anillos. El Ejercicio 27 de la Sección 3 muestra que $\psi\phi$ es un isomorfismo tanto de la estructura binaria aditiva como de la estructura binaria multiplicativa. Así que $\psi\phi$ es nuevamente un isomorfismo de anillos.

37. Muestra que si U es la colección de todas las unidades en un anillo $(R, +, \cdot)$ con unidad, entonces $(U, \cdot)$ es un grupo. [Advertencia: Asegúrate de mostrar que U está cerrado bajo la multiplicación.]
Solución: Sean $u, v \in U$. Entonces existen $s, t \in R$ tales que $us = su = 1$ y $vt = tv = 1$. Estas ecuaciones muestran que s y t también son unidades en U. Luego, $(ts)(uv) = t(su)v = t1v = tv = 1$ y $(uv)(ts) = u(vt)s = u1s = 1$, por lo que uv es nuevamente una unidad y U está cerrado bajo la multiplicación. Por supuesto, la multiplicación en U es asociativa porque la multiplicación en R es asociativa. La ecuación $1 \cdot 1 = 1$ muestra que 1 es una unidad. Mostramos anteriormente que una unidad u en U tiene un inverso multiplicativo s en U. Así que U es un grupo bajo la multiplicación.

38. Muestra que $a^2 - b^2 = (a + b)(a - b)$ para todo a y b en un anillo R si y solo si R es conmutativo.
Solución:

Ahora $(a + b)(a - b) = a^2 + ba - ab - b^2$ es igual a $a^2 - b^2$ si y solo si $ba - ab = 0$, es decir, si y solo si $ba = ab$. Pero $ba = ab$ para todo $a, b \in R$ si y solo si R es conmutativo.

39. Sea $(R, +)$ un grupo abeliano. Muestra que $(R, +, \cdot)$ es un anillo si definimos $ab = 0$ para todo $a, b \in R$.
Solución:

Solo necesitamos verificar los axiomas 2 y 3 del anillo. Para el axioma 2, tenemos $(ab)c = 0c = 0 = a0 = a(bc)$. Para el axioma 3, tenemos $a(b+c) = 0 = 0+0 = ab+ac$ y $(a + b)c = 0 = 0 + 0 = ac + bd$.

40. Muestra que los anillos $2\mathbb{Z}$ y $3\mathbb{Z}$ no son isomorfos. Muestra que los campos K y C no son isomorfos.
Solución:

Si $\phi : 2\mathbb{Z} \to 3\mathbb{Z}$ es un isomorfismo, entonces, por teoría de grupos para los grupos aditivos, sabemos que $\phi(2) = 3$ o $\phi(2) = -3$, por lo que $\phi(2n) = 3n$ o $\phi(2n) = -3n$. Supongamos que $\phi(2n) = 3n$. Entonces, $\phi(4) = 6$, mientras que $\phi(2)\phi(2) = (3)(3) = 9$. Así que $\phi(2n) = 3n$ no da un isomorfismo, y un cálculo similar muestra que $\phi(2n) = -3n$ tampoco da un isomorfismo. R y C no son isomorfos porque cada elemento en el campo C es un cuadrado, mientras que -1 no es un cuadrado en R.

41. (Exponentiación de primer año) Sea p un número primo. Muestra que en el anillo $\mathbb{Z}_p$ tenemos $(a + b)^p = a^p + b^p$ para todos los $a, b \in \mathbb{Z}_p$. [Pista: Observa que el desarrollo binómico usual para $(a + b)^n$ es válido en un anillo conmutativo.]
Solución:

En un anillo conmutativo, tenemos $(a+b)^2 = a^2+ab+ba+b^2 = a^2+ab+ab+b^2 = a^2+2ab+b^2$. Ahora, el teorema binómico simplemente cuenta la cantidad de cada tipo de producto $a^i b^{n-i}$ que aparece en $(a+b)^n$. Mientras nuestro anillo sea conmutativo, cada término de la suma $(a+b)^n$ se puede escribir como un producto de factores a y b con todos los factores a escritos primero, por lo que la expansión binómica usual es válida en un anillo conmutativo.

En $\mathbb{Z}_p$, el coeficiente i de $a^i b^{p-i}$ en la expansión de $(a+b)^p$ es un múltiplo de p si $1 \leq i \leq p-1$. Debido a que $p \cdot a = 0$ para todo $a \in \mathbb{Z}_p$, vemos que los únicos términos no nulos en la expansión corresponden a $i = 0$ e $i = p$, es decir, b^p y a^p.

42. Muestra que el elemento de unidad en un subcampo de un campo debe ser la unidad del campo completo, a diferencia del Ejercicio 32 para anillos.
Solución:

Sea F un campo y supongamos que $u^2 = u$ para u no nulo en F. Multiplicando por u^{-1}, obtenemos $u = 1$. Esto muestra que 0 y 1 son las únicas soluciones de la ecuación $x^2 = x$ en un campo. Ahora, sea K un subcampo de F. La unidad de K satisface la ecuación $x^2 = x$ en K, y por lo tanto también en F, y por lo tanto debe ser la unidad 1 de F.

43. Muestra que el inverso multiplicativo de una unidad en un anillo con unidad es único.
Solución:

Sea u una unidad en un anillo R. Supongamos que $su = us = 1$ y $tu = ut = 1$. Entonces $s = s1 = s(ut) = (su)t = 1t = t$. Por lo tanto, el inverso de una unidad es único.

44. Un elemento a de un anillo R es idempotente si $a^2 = a$.

a. Muestra que el conjunto de todos los elementos idempotentes de un anillo conmutativo está cerrado bajo la multiplicación.

b. Encuentra todos los idempotentes en el anillo $\mathbb{Z}_6 \times \mathbb{Z}_{12}$.

Solución:

a. Si $a^2 = a$ y $b^2 = b$ y el anillo es conmutativo, entonces $(ab)^2 = abab = aabb = a^2b^2 = ab$, lo que muestra que los idempotentes están cerrados bajo la multiplicación.

b. Probando todos los elementos, encontramos que los idempotentes en $Z6$ son 0, 1, 3 y 4, mientras que los idempotentes en $Z12$ son 0, 1, 4 y 9. Por lo tanto, los idempotentes en $Z6 \times Z12$ son:

- $(0,0)$
- $(1,0)$
- $(3,0)$
- $(4,0)$
- $(0,1)$
- $(1,1)$
- $(3,1)$
- $(4,1)$
- $(0,4)$
- $(1,4)$
- $(3,4)$
- $(4,4)$
- $(0,9)$
- $(1,9)$
- $(3,9)$
- $(4,9)$

45. (Álgebra lineal) Recuerda que para una matriz A de $m \times n$, la traspuesta A^T de A es la matriz cuya j-ésima columna es la j-ésima fila de A. Muestra que si A es una matriz de $m \times n$ tal que $A^T A$ es invertible, entonces la matriz de proyección $P = A(A^T A)^{-1} A^T$ es idempotente en el anillo de matrices $n \times n$.
Solución:

Tenemos

$$\begin{aligned} P^2 &= [A(A^T A)^{-1} A^T][A(A^T A)^{-1} A^T] \\ &= A[(A^T A)^{-1}(A^T A)](A^T A)^{-1} A \\ &= AIn(A^T A)^{-1} A^T \\ &= A(A^T A)^{-1} A^T = P \end{aligned}$$

46. Un elemento a de un anillo R es nilpotente si $a^n = 0$ para algún $n \in \mathbb{Z}^+$. Muestra que si a y b son elementos nilpotentes de un anillo conmutativo, entonces $a+b$ también es nilpotente.

Solución:

Como se explica en la respuesta al Ejercicio 41, la expansión binomial es válida en un anillo conmutativo. Supongamos que $a^n = 0$ y $b^m = 0$ en R. Ahora, $(a+b)^{m+n}$ es una suma de términos que contienen como factor $a^i b^{m+n-i}$ para $0 \leq i \leq m+n$. Si $i \geq n$, entonces $a^i = 0$, por lo que cada término con un factor $a^i b^{m+n-i}$ es cero. Por otro lado, si $i < n$, entonces $m+n-i > m$, por lo que $b^{m+n-i} = 0$ y cada término con un factor $a^i b^{m+n-i}$ es cero. Por lo tanto, $(a+b)^{m+n} = 0$, por lo que $a+b$ es nilpotente.

47. Muestra que un anillo R no tiene ningún elemento nilpotente distinto de cero si y solo si 0 es la única solución de $x^2 = 0$ en R.

Solución:

Si R no tiene elementos nilpotentes no nulos, entonces la única solución de $x^2 = 0$ es 0, ya que cualquier solución no nula sería un elemento nilpotente. Recíprocamente, supongamos que la única solución de $x^2 = 0$ es 0 y supongamos que $a \neq 0$ es nilpotente. Sea n el menor entero positivo tal que $a^n = 0$. Si n es par, entonces $a^{n/2} \neq 0$, pero $(a^{n/2})^2 = a^n = 0$, por lo que $a^{n/2}$ es una solución no nula de $x^2 = 0$, lo cual es contrario a la suposición. Por lo tanto, R no tiene elementos nilpotentes no nulos.

48. Muestra que un subconjunto S de un anillo R da un subanillo de R si y solo si se cumplen las siguientes condiciones:

    1. $0 \in S$.
    2. Para todo $a, b \in S$, $a - b \in S$.
    3. Para todo $a, b \in S$, $ab \in S$.

Solución:

Es claro que si S es un subanillo de R, entonces las tres condiciones deben cumplirse. Recíprocamente, supongamos que las condiciones se cumplen. Las dos primeras condiciones y el Ejercicio 45 de la Sección 5 muestran que $\langle S, + \rangle$ es un grupo aditivo. La condición final muestra que la multiplicación está cerrada en S. Por supuesto, las leyes asociativas y distributivas se cumplen para los elementos de S, porque realmente se cumplen para todos los elementos en R. Por lo tanto, S es un subanillo de R.

49. a. Muestra que la intersección de subanillos de un anillo R es nuevamente un subanillo de R.

    b. Muestra que la intersección de subcampos de un campo F es nuevamente un subcampo de F.

Solución:

a. Sea R un anillo y sean $H_i \leq R$ para $i \in I$. El Teorema 7.4 muestra que $H = \cap_{i \in I} H_i$ es un grupo aditivo. Sean $a, b \in H$. Entonces $a, b \in H_i$ para $i \in I$, por lo que $ab \in H_i$ para $i \in I$, porque H_i es un subanillo de R. Por lo tanto, $ab \in H$, por lo que H está cerrado bajo la multiplicación. Claramente, las leyes asociativas y distributivas se cumplen para los elementos de H, porque realmente se cumplen para todos los elementos en R. Por lo tanto, H es un subanillo de R.

b. Sea F un campo y sean $K_i \leq F$ para $i \in I$. La parte (a) muestra que $K = \cap_{i \in I} K_i$ es un anillo. Sea $a \in K$, $a \neq 0$. Entonces $a \in K_i$ para $i \in I$, por lo que $a^{-1} \in K_i$ para $i \in I$, porque los Ejercicios 42 y 43 muestran que la unidad en cada K_i es la misma que en F y que los inversos son únicos. Por lo tanto, $a^{-1} \in K$. Por supuesto, la multiplicación en K es conmutativa porque la multiplicación en F es

conmutativa. Por lo tanto, K es un subcampo de F.

50. Sea R un anillo y sea a un elemento fijo de R. Sea $I_a = \{x \in R \mid ax = 0\}$. Muestra que I_a es un subanillo de R.
Solución:

Mostramos que Ia satisface las condiciones del Ejercicio 48. Debido a que $a * 0 = 0$, vemos que $0 \in Ia$. Sea $c, d \in Ia$. Luego, $ac = ad = 0$, por lo que $a(c-d) = ac-ad = 0 - 0 = 0$; por lo tanto, $(c - d) \in Ia$. Además, $a(cd) = (ac)d = 0d = 0$, por lo que $cd \in Ia$. Esto completa la verificación de las propiedades en el Ejercicio 48.

51. Sea R un anillo y a un elemento fijo de R. Sea R_a el subanillo de R que es la intersección de todos los subanillos de R que contienen a a (ver Ejercicio 49). El anillo Ra es el subanillo de R generado por a. Demuestra que el grupo abeliano $\{R_a, +\}$ está generado (en el sentido de la Sección 7) por $\{a^n \mid n \in \mathbb{Z}^+\}$.
Solución:

Claramente, a^n está en cada subanillo que contiene a a, por lo tanto, Ra contiene a^n para cada entero positivo n. Así, el grupo aditivo $\langle Ra, +\rangle$ contiene el grupo aditivo G generado por $S = \{a^n \mid n \in \mathbb{Z}^+\}$. Afirmamos que $G = Ra$. Solo necesitamos mostrar que G está cerrado bajo la multiplicación. Ahora bien, G consta de cero y todas las sumas finitas de términos de la forma a^n o $-a^m$. Por las leyes distributivas, el producto de dos elementos que son sumas finitas de potencias positivas e inversos de potencias positivas de a también puede escribirse como tal suma, y por lo tanto, también está en G. Por lo tanto, G es un subanillo que contiene a a y está contenido en Ra, por lo que debemos tener $G = Ra$.

52. (Teorema Chino del Residuo para dos congruencias) Sean r y s enteros positivos tales que $\gcd(r, s) = 1$. Usa el isomorfismo en el Ejemplo 18.15 para mostrar que para $m, n \in \mathbb{Z}$, existe un entero x tal que $x \equiv m \pmod r$ y $x \equiv n \pmod s$.
Solución: El Ejemplo 18.15 muestra que el mapa $\phi : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$ donde $\phi(a) = a \cdot (1, 1)$ es un isomorfismo. Sea $b = \phi^{-1}(m, n)$. Calculando $b \cdot (1, 1)$ por componentes, vemos que la suma de $1+1+\ldots+1$ para b términos da m en $\mathbb{Z}_r$ y da n en $\mathbb{Z}_s$. Así, viendo a b como un entero en $\mathbb{Z}$, tenemos que $b \equiv m \pmod r$ y $b \equiv n \pmod s$.

53. a. Enuncia y demuestra la generalización del Ejemplo 18.15 para un producto directo con n factores.

b. Demuestra el Teorema Chino del Residuo: Sean $a_i, b_i \in \mathbb{Z}^+$ para $i = 1, 2, \ldots, n$, y $\gcd(b_i, b_j) = 1$ para $i \neq j$. Entonces, existe un $x \in \mathbb{Z}^+$ tal que $x \equiv a_i \pmod{b_i}$ para $i = 1, 2, \ldots, n$.
Solución:

a. Enunciado: Sean $b_1, b_2, \ldots, b_n$ enteros tales que $\gcd(b_i, b_j) = 1$ para $i \neq j$. Entonces, $\mathbb{Z}_{b_1 b_2 \ldots b_n}$ es isomorfo a $\mathbb{Z}_{b_1} \times \mathbb{Z}_{b_2} \times \ldots \times \mathbb{Z}_{b_n}$ con un isomorfismo ϕ donde $\phi(1) = (1, 1, \ldots, 1)$.

b. Prueba: Por la hipótesis de que $\gcd(b_i, b_j) = 1$ para $i \neq j$, sabemos que el grupo imagen es cíclico y que $(1, 1, \ldots, 1)$ genera el grupo. Dado que el grupo dominio es cíclico generado por 1, sabemos que ϕ es un isomorfismo de grupos aditivos. Queda por demostrar que $\phi(ms) = \phi(m)\phi(s)$ para m y s en el grupo dominio. Esto sigue del hecho de que el componente i-ésimo de $\phi(ms)$ en el grupo imagen es $(ms) \cdot 1$, lo cual es igual al producto de m términos de 1 por s términos de 1 según las leyes distributivas en un anillo.

54. Considera $(S, +, \cdot)$, donde S es un conjunto y $+$ y $\cdot$ son operaciones binarias en S tales que

- $(S, +)$ es un grupo,

- $(S^*, \cdot)$ es un grupo donde S^* consiste en todos los elementos de S excepto el elemento neutro aditivo,
- $a(b + c) = (ab) + (ac)$ y $(a + b)c = (ac) + (be)$ para todo $a, b, c \in S$.

Demuestra que $\{S, +, \cdot\}$ es un cuerpo. [Sugerencia: Aplica las leyes distributivas a $(1 + 1)(a + b)$ para probar la conmutatividad de la adición.]

Solución:

Nótese que $a^0 = 0$ para todo $a \in S$ sigue de las leyes distributivas, por lo que la asociatividad de la multiplicación para productos que contienen un factor 0 se cumple, y la asociatividad en el grupo $\langle S^*, \cdot \rangle$ se encarga de la asociatividad para otros productos. Todos los demás axiomas necesarios para verificar que S es un cuerpo siguen de inmediato de las dos afirmaciones dadas sobre grupos y las leyes distributivas dadas, excepto por la conmutatividad de la adición.

Las leyes distributivas de izquierda seguidas de las leyes distributivas de derecha dan $(1 + 1)(a + b) = (1 + 1)a + (1 + 1)b = a + a + b + b$. Las leyes distributivas de derecha seguidas de las leyes distributivas de izquierda dan $(1 + 1)(a + b) = 1(a + b) + 1(a + b) = a + b + a + b$. Así, $a+a+b+b = a+b+a+b$ y por cancelación en el grupo aditivo, obtenemos $a+b = b+a$.

55. Un anillo R es un anillo booleano si $a^2 = a$ para todo $a \in R$, es decir, cada elemento es idempotente. Demuestra que todo anillo booleano es conmutativo.

Solución:

Sea $a, b \in R$ donde R es un anillo booleano. Tenemos $a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$. Así, en un anillo booleano, $ab = -ba$. Tomando $b = a$, vemos que $aa = -aa$, por lo que $a = -a$. Así, cada elemento es su propio inverso aditivo, entonces $-ba = ba$. Combinando nuestras ecuaciones $ab = -ba$ y $-ba = ba$, obtenemos $ab = ba$, mostrando que R es conmutativo.

56. (Para estudiantes con conocimientos en leyes de teoría de conjuntos) Para un conjunto S, sea $P(S)$ la colección de todos los subconjuntos de S. Define las operaciones binarias $+$ y $\cdot$ en $P(S)$ como

$$A + B = (A \setminus B) \cup (B \setminus A),$$
$$A \cdot B = A \cap B,$$

para $A, B \in P(S)$.

a. Da las tablas para $+$ y $\cdot$ en $P(S)$, donde $S = \{a, b\}$. [Sugerencia: $P(S)$ tiene cuatro elementos.]

b. Demuestra que para cualquier conjunto S, $\{P(S), +, \cdot\}$ es un anillo booleano (ver Ejercicio 55).

Solución:

a.

$+$	$\emptyset$	$\{a\}$	$\{b\}$	S
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	S
$\{a\}$	$\{a\}$	$\emptyset$	S	$\emptyset$
$\{b\}$	$\{b\}$	S	$\emptyset$	$\emptyset$
S	S	$\emptyset$	$\emptyset$	S

$\cdot$	$\emptyset$	$\{a\}$	$\{b\}$	S
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\emptyset$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\emptyset$
S	$\emptyset$	$\emptyset$	$\emptyset$	S

b. La conmutatividad de la suma se verifica directamente de las tablas.

Verificamos la asociatividad de la suma; es más fácil pensar en términos de los elementos en $(A + B) + C$ y los elementos en $A + (B + C)$. Por definición, la suma de dos conjuntos contiene los elementos en precisamente uno de los conjuntos. Por lo tanto, $A + B$ consiste en los elementos que están en cualquiera de los conjuntos A

o B, pero no en ambos. Por lo tanto, $(A + B) + C$ consiste en los elementos que están precisamente en uno de los tres conjuntos A, B, C. Claramente, $A + (B + C)$ produce este mismo conjunto, por lo que la suma es asociativa.

El conjunto vacío $\emptyset$ actúa como la identidad aditiva, ya que $A + \emptyset = (A \cup \emptyset) - (A \cap \emptyset) = A - \emptyset = A$ para todo $A \in P(S)$.

Para $A \in P(S)$, tenemos $A + A = (A \cup A) - (A \cap A) = A - A = \emptyset$, por lo que cada elemento de $P(S)$ es su propio inverso aditivo. Esto demuestra que $\langle P(S), + \rangle$ es un grupo abeliano.

Para la asociatividad de la multiplicación, notamos que $(A \cdot B) \cdot C = (A \cap B) \cap C = A \cap (B \cap C) = A \cdot (B \cdot C)$.

Para la ley distributiva izquierda, nuevamente pensamos en términos de los elementos en los conjuntos. El conjunto $A \cdot (B + C) = A \cap (B + C)$ consiste en todos los elementos de A que están en precisamente uno de los dos conjuntos B, C. Este conjunto contiene todos los elementos en $A \cap B$ o en $A \cap C$, pero no en ambos. Esto es precisamente el conjunto $(A \cdot B) + (A \cdot C)$. La ley distributiva derecha se puede demostrar con un argumento similar.

Hemos demostrado que $\langle P(S), +, \cdot \rangle$ es un anillo. Debido a que $A \cdot A = A \cap A = A$, vemos a partir de la definición en el Ejercicio 55 que también es un anillo booleano.

Ejercicios 21

Sección 21 1-2 y 6-17.

Cálculos

1. Describe el campo F de cocientes del subdominio integral $D = \{n + mi \mid n, m \in \mathbb{Z}\}$ de $\mathbb{C}$. "Describir"significa dar los elementos de $\mathbb{C}$ que forman el campo de cocientes de D en $\mathbb{C}$. (Los elementos de D son los enteros gaussianos).

   Solución:

   El campo de cocientes de D es $\{q_1 + q_2 i \mid q1, q2 \in \mathbb{Q}\}$.

2. Describe (en el sentido del Ejercicio 1) el campo F de cocientes del subdominio integral $D = \{n + m\sqrt{2} \mid n, m \in \mathbb{Z}\}$ de $\mathbb{R}$.

   Solución:

   Debido a que

   $$\begin{aligned} \frac{1}{a + b\sqrt{2}} &= \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} \\ &= \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \end{aligned}$$

   Vemos que $\{q_1 + q_2\sqrt{2} \mid q_1, q_2 \in \mathbb{Q}\}$ es un campo y debe ser el campo de cocientes.

Teoría

La contrucción

Sea D un dominio entero que deseamos agrandar a un campo de cocientes F. Un esbozo a grandes rasgos de los pasos a seguir es el siguiente:

1. Definir cuáles serán los elementos de F
2. Definir en F las operaciones binarias de suma y multiplicación.
3. Comprobar que se cumplan todos los axiomas de campo, para mostrar que F es un campo bajo estas operaciones.
   a) La suma en F es conmutativa.
   b) La suma es asociativa.
   c) $[(0, 1)]$ es una identidad para la suma en F.

d) $[(-a, b)]$ es un inverso aditivo para $[(a, b)]$ en F.

e) La multiplicación en F es asociativa.

f) La multiplicación en F es conmutativa.

g) Las leyes distributivas valen en F.

h) $[(1, 1)]$ es una identidad multiplicativa en F.

i) Si $[(a, b)]$ e F no es la identidad aditiva, entonces $a \neq 0$ en D y $[(b, a)]$ es un inverso multiplicativo para $[(a, b)]$.

4. Mostrar que F puede contener a D como un subdominio entero.

Ejercicios

6. Demostrar la Parte 2 (Suma Asociativa) del Paso 3. Puedes asumir cualquier parte previa del Paso 3.
Solución:
Tenemos

$$\begin{aligned}
&[(a, b)] + ([(c, d)] + [(e, f)]) \\
&= [(a, b)] + [(cf + de, df)] \\
&= [(adf + bcf + bde, bdf)] \\
&= [(ad + bc, bd)] + [(e, f)] \\
&= ([(a, b)] + [(c, d)]) + [(e, f)].
\end{aligned}$$

Así que la adición es asociativa.

7. Demostrar la Parte 3 del Paso 3. Puedes asumir cualquier parte previa del Paso 3.
Solución:
Tenemos $[(0, 1)] + [(a, b)] = [(0b + 1a, 1b] = [(a, b)]$. Por la Parte 1 del Paso 3, también tenemos $[(a, b)] + [(0, 1)] = [(a, b)]$.

8. Demostrar la Parte 4 del Paso 3. Puedes asumir cualquier parte previa del Paso 3.
Solución:
Tenemos $[(-a, b)] + [(a, b)] = [(-ab + ba, b^2)] = [(0, b^2)]$.

Pero $[(0, b^2)] \sim [(0, 1)]$ porque $(0)(1) = (b^2)(0) = 0$. Así que $[(-a, b)] + [(a, b)] = [(0, 1)]$. Por la Parte 1 del Paso 3, también tenemos $[(a, b)] + [(-a, b)] = [(0, 1)]$.

9. Demostrar la Parte 5 del Paso 3. Puedes asumir cualquier parte previa del Paso 3.

Ahora

$$\begin{aligned}
[(a, b)]([(c, d)][(e, f)]) &= [(a, b)][(ce, df)] \\
&= [(ace, bdf)] \\
&= [(ac, bd)][(e, f)] \\
&= ([(a, b)][(c, d)])[(e, f)].
\end{aligned}$$

Así que la multiplicación es asociativa.

10. Demostrar la Parte 6 del Paso 3. Puedes asumir cualquier parte previa del Paso 3.
Solución:
Tenemos

$$\begin{aligned}
[(a, b)][(c, d)] &= [(ac, bd)] \\
&= [(ca, db)] \\
&= [(c, d)][(a, b)]
\end{aligned}$$

Así que la multiplicación es conmutativa.

11. Demostrar la Parte 7 del Paso 3. Puedes asumir cualquier parte previa del Paso 3.
Solución:
Para la ley distributiva izquierda, tenemos

$$\begin{aligned}
&[(a, b)][(c, d)] + [(a, b)][(e, f)] \\
&= [(ac, bd)] + [(ae, bf)] \\
&= [(acbf + bdae, bdbf)] \\
&\sim [(acf + ade, bdf)] \quad \text{porque} \quad (acbf + bdae)bdf \\
&= acbfbdf + bdaebdf \\
&= bdbf(acf + ade),
\end{aligned}$$

Ya que la multiplicación en D es conmutativa. La ley distributiva derecha sigue de la Parte 6.

12. Sea R un anillo conmutativo no nulo, y sea T un subconjunto no vacío de R cerrado bajo la multiplicación y que no contiene ni 0 ni divisores de 0. Comenzando con $R \times T$ y siguiendo exactamente la construcción de esta sección, podemos demostrar que el anillo R puede ampliarse a un

anillo parcial de cocientes $Q(R, T)$. Piensa en esto durante unos 15 minutos; repasa la construcción y observa por qué las cosas aún funcionan. En particular, muestra lo siguiente:

a. $Q(R, T)$ tiene unidad aunque R no la tenga.

b. En $Q(R, T)$, cada elemento no nulo de T es una unidad.

Solución:

a. Debido a que T no es vacío, existe un $a \in T$. Entonces, $[(a, a)]$ es la unidad en $Q(R, T)$, ya que $[(a, a)][(b, c)] = [(ab, ac)] \sim [(b, c)]$ ya que $abc = acb$ en el anillo conmutativo R.

b. Un elemento no nulo $a \in T$ se identifica con $[(aa, a)]$ en $Q(R, T)$. Debido a que T no tiene divisores de cero, $[(a, aa)] \in Q(R, T)$, y vemos que $[(aa, a)][(a, aa)] = [(aaa, aaa)] \sim [(a, a)]$ porque $aaaa = aaaa$. Vimos en la parte a que $[(a, a)]$ es la unidad en $Q(R, T)$. La conmutatividad de $Q(R, T)$ muestra que $[(a, aa)][(aa, a)]$ también es la unidad, así que $a \in T$ tiene inverso en $Q(R, T)$ si $a \neq 0$.

13. Demostrar a partir del Ejercicio 12 que todo anillo conmutativo no nulo que contiene un elemento a que no es divisor de 0 puede ampliarse a un anillo conmutativo con unidad. Comparar con el Ejercicio 30 de la Sección 19.
Solución:
Solo necesitamos tomar $T = \{a^n \mid n \in \mathbb{Z}^+\}$ en el Ejercicio 12. Esta construcción es completamente diferente de la de la Sección 19, Ejercicio 30.

14. Con referencia al Ejercicio 12, ¿cuántos elementos hay en el anillo $Q(\mathbb{Z}_4, \{1, 3\})$?
Solución:
Hay cuatro elementos, ya que 1 y 3 ya son unidades en $\mathbb{Z}_4$.

15. Con referencia al Ejercicio 12, describe el anillo $Q(\mathbb{Z}, \{2^n \mid n \in \mathbb{Z}^+\})$, describiendo un subanillo de R al que es isomorfo.
Solución:
Es isomorfo al anillo D de todos los números racionales que se pueden expresar como cociente de enteros con denominador una potencia de 2, como se describe en la respuesta al Ejercicio 5.

16. Con referencia al Ejercicio 12, describe el anillo $Q(2\mathbb{Z}, \{6^n \mid n \in \mathbb{Z}^+\})$ describiendo un subanillo de R al que es isomorfo.
Solución:
Es isomorfo al anillo de todos los números racionales que se pueden expresar como cociente de enteros con denominador una potencia de 6. El 3 en $3\mathbb{Z}$ no restringe el numerador, ya que 1 se puede recuperar como $[(6, 6)]$, 2 como $[(12, 6)]$, etc.

17. Con referencia al Ejercicio 12, supongamos que eliminamos la condición de que T no tenga divisores de 0 y simplemente requerimos que T no vacío y que no contenga 0 esté cerrado bajo la multiplicación. El intento de ampliar R a un anillo conmutativo con unidad en el que cada elemento no nulo de T sea una unidad debe fallar si T contiene un elemento a que es un divisor de 0, ya que un divisor de 0 no puede ser una unidad. Intenta descubrir dónde una construcción paralela a la del texto pero comenzando con $R \times T$ primero tiene problemas. En particular, para $R = \mathbb{Z}_6$ y $T = \{1, 2, 4\}$, ilustra la primera dificultad encontrada. [Sugerencia: Está en el Paso 1.]
Solución:
Se encuentra en problemas cuando intentamos probar la propiedad transitiva en la demostración del Lema 21.2, ya que la cancelación multiplicativa puede no cumplirse. Para $R = \mathbb{Z}_6$ y $T = \{1, 2, 4\}$, tenemos que $(1, 2) \sim (2, 4)$ porque $(1)(4) = (2)(2) = 4$ y $(2, 4) \sim (2, 1)$ porque $(2)(1) = (4)(2)$ en $\mathbb{Z}_6$, pero $(1, 2) \not\cong (2, 1)$ porque $(1)(1) \neq (2)(2)$ en $\mathbb{Z}_6$.

Cálculos

En los Ejercicios 1 a 4, encuentra la suma y el producto de los polinomios dados en el anillo polinómico indicado.

1. $f(x) = 4x-5$, $g(x) = 2x^2-4x+2$ en $\mathbb{Z}_8[x]$.
   Solución:
   $f(x)+g(x) = 2x^2+5, \quad f(x)g(x) = 6x^2+4x+6.$

2. $f(x) = x+1$, $g(x) = x+1$ en $\mathbb{Z}_2[x]$.
   Solución:
   ¿$f(x)+g(x) = 0, \quad f(x)g(x) = x^2+1.$

3. $f(x) = 2x^2+3x+4$, $g(x) = 3x^2+2x+3$ en $\mathbb{Z}_6[x]$.
   Solución:
   $f(x)+g(x) = 5x^2+5x+1, \quad f(x)g(x) = x^3+5x.$

4. $f(x) = 2x^3+4x^2+3x+2$, $g(x) = 3x^4+2x+4$ en $\mathbb{Z}_5[x]$.
   Solución:
   $f(x)+g(x) = 3x^4+2x^3+4x^2+1,$
   $f(x)g(x) = x^7+2x^6+4x^5+x^3+2x^2+x+3.$

5. ¿Cuántos polinomios hay de grado ≤ 3 en $\mathbb{Z}_2[x]$? (Incluye 0.)
   Solución:
   Un polinomio de la forma ax^3+bx^2+cx+d , donde cada a, b, c, d puede ser 0 o 1. Por lo tanto, hay $2 \cdot 2 \cdot 2 \cdot 2 = 16$ polinomios de este tipo en total.

6. ¿Cuántos polinomios hay de grado ≤ 2 en $\mathbb{Z}_5[x]$? (Incluye 0.)
   Solución:
   Un polinomio de la forma ax^2+bx+c , donde cada a, b, c puede ser $0, 1, 2, 3$ o 4. Así que hay $5 \cdot 5 \cdot 5 = 125$ polinomios de este tipo en total.

En los Ejercicios 7 y 8, $F = E = \mathbb{C}$ en el Teorema 22.4. Calcula para el homomorfismo de evaluación indicado.

7. $\phi_2(x^2+3)$.
   Solución:
   $\phi_2(x^2+3) = 2^2+3 = 7$

8. $\phi_i(2x^3-x^2+3x+2)$.
   Solución: $\phi_i(2x^3-x^2+3x+2) = 2 \cdot 1^3 - 1 \cdot 1^2 + 3 \cdot 1 + 2 = 4$

En los Ejercicios 9 al 11, $F = E = \mathbb{Z}_7$ en el Teorema 22.4. Calcula para el homomorfismo de evaluación indicado.

9. $\phi_3[(x^4+2x)(x^3-3x^2+3)]$.
   Solución:
   $$\begin{aligned}&\phi_3[(x^4+2x)(x^3-3x^2+3)]\\ &= \phi_3(x^4+2x) \cdot \phi_3(x^3-3x^2+3)\\ &= (3^4+6) \cdot (3^3-3 \cdot 3^2+3)\\ &= (4+6) \cdot (3) = 2.\end{aligned}$$

10. $\phi_5[(x^3+2)(4x^2+3)(x^7+3x^2+1)]$.
    Solución:
    $$\begin{aligned}&\phi_5[(x^3+2)(4x^2+3)(x^7+3x^2+1)]\\ &= \phi_5(x^3+2) \cdot \phi_5(4x^2+3) \cdot \phi_5(x^7+3x^2+1)\\ &= (5^3+2) \cdot (4 \cdot 5^2+3) \cdot (5^7+3 \cdot 5^2+1)\\ &= (6+2) \cdot (2+3) \cdot (1+5+1) = (1) \cdot (5) \cdot (4) = 6.\end{aligned}$$

11. $\phi_4(3x^{106}+5x^k+2x^{53})$.
    Solución:
    $$\begin{aligned}&\phi_4(3x^{106}+5x^{99}+2x^{53})\\ &= 3 \cdot 4^{106}+5 \cdot 4^{99}+2 \cdot 4^{53}\\ &= 3 \cdot (1)+5 \cdot (1)+2 \cdot (1) = 5+5+4 = 0.\end{aligned}$$

En los Ejercicios 12 al 15, encuentra todas las raíces en el campo finito indicado del polinomio dado con coeficientes en ese campo.

12. x^2+1 en $\mathbb{Z}_2$ tiene 1 como única raíz.
    Solución:
    $1^2+1 = 0$, pero $0^2+1 = 0$, así que 1 es la única raíz.

13. x^3+2x+2 en $\mathbb{Z}_7$ tiene 2 y 3 como únicas raíces.
    Solución:
    Sea $f(x) = x^3+2x+2$. Entonces, $f(0) = 2, f(1) = 5, f(2) = 0, f(3) = 0, f(-3) = 4, f(-2) = 4$ y $f(-1) = 6$, así que 2 y 3 son las únicas raíces.

14. $x^5 + 3x^3 + x^2 + 2x$ en $\mathbb{Z}_5$ tiene 0 y 4 como únicas raíces.
Solución:
Sea $f(x) = x^5 + 3x^3 + x^2 + 2x$. Entonces, $f(0) = 0, f(1) = 2, f(2) = 4, f(-2) = 4$, y $f(-1) = 0$, así que 0 y 4 son las únicas raíces.

15. $f(x)g(x)$, donde $f(x) = x^3 + 2x^2 + 5$ y $g(x) = 3x^2 + 2x$ en $\mathbb{Z}_7$ tiene 0, 2 y 4 como únicas raíces.
Solución:
Dado que $\mathbb{Z}_7$ es un campo, $f(a)g(a) = 0$ si y solo si $f(a) = 0$ o $g(a) = 0$. Sea $f(x) = x^3 + 2x^2 + 5$ y $g(x) = 3x^2 + 2x$ Entonces, $f(0) = 5, f(1) = 1, f(2) = 0, f(3) = 1, f(-3) = 3, f(-2) = 5$, y $f(-1) = 6$, mientras que $g(0) = 0, g(1) = 5, g(2) = 2, g(3) = 5$, $g(-3) = 0, g(-2) = 1$, y $g(-1) = 1$. Por lo tanto, las raíces de $f(x)g(x)$ son $0, 2$, y 4.

16. Sea $\phi : \mathbb{Z}_8[x] \to \mathbb{Z}_5$ un homomorfismo de evaluación como en el Teorema 22.4. Usa el teorema de Fermat para evaluar $03x^{231} + 3x^{111} - 2x^{53} + 1 = 1$.
Solución:

$$\begin{aligned}
&\phi_3(x^{231} + 3x^{117} - 2x^{53} + 1) \\
&= 3^{231} + 3^{118} - 2 \cdot (3^{53}) + 1 \\
&= (3^4)^{57} + (3^4)^{29} - 2 \cdot (3^4)^{13} + 1 \\
&= 81^{57} + 81^{29} - 2 \cdot 81^{13} + 1 \\
&= (80 + 1)^{57} + (80 + 1)^{29} - 2 \cdot (80 + 1)^{13} + 1 \\
&= 2 + 4 - 1 + 1 = 6.
\end{aligned}$$

17. Usa el teorema de Fermat para encontrar todas las raíces en $\mathbb{Z}_5$ de $2x^{219} + 3x^{18} + 2x^5 + 3x^{44}$.
Solución:
Sea $f(x) = 2x^{219} + 3x^{74} + 2x^{57} + 3x^{44}$. Entonces, $f(0) = 0, f(1) = 2 + 3 + 2 + 3 = 0$, $f(2) = 1 + 2 + 4 + 3 = 0, f(-2) = 4 + 2 + 1 + 3 = 0$, y $f(-1) = 3 + 3 + 3 + 3 = 2$. Por lo tanto, las raíces de $f(x)$ son $0, 1, 2$, y 3.

Ejercicio 24

Sea $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ y $g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$ polinomios en $D[x]$ con a_n y b_m ambos distintos de cero. Dado que D es un dominio integral, sabemos que $a_n b_m \neq 0$, por lo que $f(x)g(x)$ es distinto de cero porque su término de mayor grado tiene coeficiente $a_n b_m$. Según se afirma en el texto, $D[x]$ es un anillo conmutativo con unidad, y hemos demostrado que no tiene divisores de cero, por lo que es un dominio integral.

Ejercicio 25

a) Las unidades en $D[x]$ son las unidades en D, ya que un polinomio de grado n multiplicado por un polinomio de grado m da como resultado un polinomio de grado nm, como se demostró en el ejercicio anterior. Por lo tanto, un polinomio de grado 1 no puede ser multiplicado por nada en $D[x]$ para dar 1, que es un polinomio de grado 0.

b) Son las unidades en $\mathbb{Z}$, es decir, 1 y -1.

c) Son las unidades en $\mathbb{Z}_7$, es decir, 1, 2, 3, 4, 5 y 6.

Bibliografía

1. John B. Fraleigh, Neal E. Brand. *A First Course in Abstract Algebra, 7th Edition*, Pearson.
2. Thomas W. Judson. *Abstract Algebra, Theory and Applications*, Stephen F. Austin State University.