

Sección 18 Anillos y Campos 1-28,34-51,54-56.  
 Sección 19 Dominios Enteros 1-14, 23-30  
 Sección 21 El campo de cocientes de un dominio integral 1,2,6,7,8,...,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

## Ejercicios 23

### División de Polinomios en $\mathbb{Z}_p[x]$

1. Dados  $f(x) = x^6 + 3x^5 + Ax^2 - 3x + 2$  y  $g(x) = x^2 + 2x - 3$  en  $\mathbb{Z}_7[x]$ , encuentra  $q(x)$  y  $r(x)$  según el algoritmo de división, de manera que  $f(x) = g(x)q(x) + r(x)$ , con  $r(x) = 0$  o de grado menor que el de  $g(x)$ .
2. Dados  $f(x) = -x^3 + 3x^5 + 4x^2 - 3x + 2$  y  $g(x) = 3x^2 + 2x - 3$  en  $\mathbb{Z}_7[x]$ , encuentra  $q(x)$  y  $r(x)$  según el algoritmo de división, de manera que  $f(x) = g(x)q(x) + r(x)$ , con  $r(x) = 0$  o de grado menor que el de  $g(x)$ .
3. Dados  $f(x) = x^5 - 2x^4 + 3x - 5$  y  $g(x) = 2x + 1$  en  $\mathbb{Z}[x]$ , encuentra  $q(x)$  y  $r(x)$  según el algoritmo de división, de manera que  $f(x) = g(x)q(x) + r(x)$ , con  $r(x) = 0$  o de grado menor que el de  $g(x)$ .
4. Dados  $f(x) = x^4 + 5x^3 - 3x^2$  y  $g(x) = 5x^2 - x + 2$  en  $\mathbb{Z}[x]$ , encuentra  $q(x)$  y  $r(x)$  según el algoritmo de división, de manera que  $f(x) = g(x)q(x) + r(x)$ , con  $r(x) = 0$  o de grado menor que el de  $g(x)$ .

### Grupos Multiplicativos Cíclicos de Campos Finitos

5. Encuentra todos los generadores del grupo multiplicativo cíclico de unidades del campo finito  $\mathbb{Z}_5$ .
6. Encuentra todos los generadores del grupo multiplicativo cíclico de unidades del campo finito  $\mathbb{Z}_7$ .
7. Encuentra todos los generadores del grupo multiplicativo cíclico de unidades del campo finito  $\mathbb{Z}_{17}$ .
8. Encuentra todos los generadores del grupo multiplicativo cíclico de unidades del campo finito  $\mathbb{Z}_{23}$ .

### Factorización de Polinomios en $\mathbb{Z}[x]$

9. El polinomio  $x^4 + 4$  se puede factorizar en factores lineales en  $\mathbb{Z}[x]$ . Encuentra esta factorización.
10. El polinomio  $x^3 + 2x^2 + 2x + 1$  se puede factorizar en factores lineales en  $\mathbb{Z}_7[x]$ . Encuentra esta factorización.

11. El polinomio  $2x^3 + 3x^2 - x - 5$  se puede factorizar en factores lineales en  $\mathbb{Z}_n[x]$ . Encuentra esta factorización.
12. ¿Es  $x^3 + 2x + 3$  un polinomio irreducible en  $\mathbb{Z}_5[x]$ ? ¿Por qué? Exprésalo como un producto de polinomios irreducibles en  $\mathbb{Z}_5[x]$ .
13. ¿Es  $2x^3 + x^2 + 2x + 2$  un polinomio irreducible en  $\mathbb{Z}_5[x]$ ? ¿Por qué? Exprésalo como un producto de polinomios irreducibles en  $\mathbb{Z}_5[x]$ .
14. Demuestra que  $f(x) = x^2 + 8x - 2$  es irreducible sobre  $\mathbb{Q}$ . ¿Es irreducible sobre  $\mathbb{E}$ ? ¿Sobre  $\mathbb{C}$ ?
15. Repite el Ejercicio 14 con  $g(x) = x^2 + 6x + 12$  en lugar de  $f(x)$ .
16. Demuestra que  $x^3 + 3x^2 - 8$  es irreducible sobre  $\mathbb{Q}$ .
17. Demuestra que  $x^4 - 22x^2 + 1$  es irreducible sobre  $\mathbb{Q}$ .

### Criterio de Eisenstein

18. Determina si el polinomio  $x^2 - 12$  satisface el criterio de Eisenstein para irreducibilidad sobre  $\mathbb{Q}$ .
19. Determina si el polinomio  $8x^3 + 6x^2 - 9x + 2A$  satisface el criterio de Eisenstein para irreducibilidad sobre  $\mathbb{Q}$ .
20. Determina si el polinomio  $4x^{10} - 9x^3 + 2Ax - 18$  satisface el criterio de Eisenstein para irreducibilidad sobre  $\mathbb{Q}$ .
21. Determina si el polinomio  $2x^{10} - 25x^3 + 10x^2 - 30$  satisface el criterio de Eisenstein para irreducibilidad sobre  $\mathbb{Q}$ .

### Encontrar las Raíces de un Polinomio

22. Encuentra todas las raíces de  $6x^4 + 17x^3 + 11x^2 + x - 10$  en  $\mathbb{Q}$ .

### Teoría

1. Demuestra que para  $p$  un número primo, el polinomio  $x^p + a$  en  $\mathbb{Z}_p[x]$  no es irreducible para ningún  $a \in \mathbb{Z}_p$ .
2. Si  $F$  es un campo y  $a^0$  es una raíz de  $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$  en  $F[x]$ , demuestra que  $1/a$  es una raíz de  $a_n + a_{n-1}x + \dots + a_0x^n$ .
3. (Teorema del Resto) Sea  $f(x) \in F[x]$ , donde  $F$  es un campo, y sea  $a \in F$ . Demuestra que el resto  $r(x)$  cuando  $f(x)$  se divide por  $x - a$ , de acuerdo con el algoritmo de división, es  $f(a)$ .
4. Sea  $\phi_m : \mathbb{Z}[x] \rightarrow \mathbb{Z}_m[x]$  dada por

$$\phi_m(a_0 + a_1x + a_2x^2 + \dots + a_nx^n) = \phi_m(a_0) + \phi_m(a_1)x + \phi_m(a_2)x^2 + \dots + \phi_m(a_n)x^n,$$

donde  $\phi_m$  es la aplicación natural mód  $m$  definida por  $\phi_m(a) = (\text{el resto de } a \text{ al dividirlo por } m)$  para  $a \in \mathbb{Z}$ .

- Demuestra que  $\phi_m$  es un homomorfismo de  $\mathbb{Z}[x]$  a  $\mathbb{Z}_m[x]$ .
- Demuestra que si  $f(x) \in \mathbb{Z}[x]$  y  $\phi_m(f(x))$  tienen ambas grado  $n$  y  $a \cdot \phi_m(f(x))$  no se factoriza en  $\mathbb{Z}_m[x]$  en dos polinomios de grado menor que  $n$ , entonces  $f(x)$  es irreducible en  $\mathbb{Q}[x]$ .
- Usa la parte (b) para demostrar que  $x^3 + 11x + 36$  es irreducible en  $\mathbb{Q}[x]$ . [Pista: Prueba con un valor primo de  $m$  que simplifique los coeficientes.]

## Soluciones

### Generadores de Grupos Multiplicativos Cíclicos en Campos Finitos

- Para  $2 \in \mathbb{Z}_5$ , tenemos que  $2^2 = 4$ ,  $2^3 = 3$ ,  $2^4 = 1$ , por lo que 2 genera el subgrupo multiplicativo  $\{1, 2, 3, 4\}$  de todas las unidades en  $\mathbb{Z}_5$ . Según el Corolario 6.16, los únicos generadores son  $2^1 = 2$  y  $2^3 = 3$ .
- Para  $2 \in \mathbb{Z}_7$ , encontramos que  $2^3 = 1$ , por lo que 2 no genera. Probando con 3, encontramos que  $3^2 = 2$ ,  $3^3 = 6$ ,  $3^4 = 4$ ,  $3^5 = 5$ , y  $3^6 = 1$ , por lo que 3 genera las seis unidades 1, 2, 3, 4, 5, 6 en  $\mathbb{Z}_7$ . Por el Corolario 6.16, los únicos generadores son  $3^1 = 3$  y  $3^5 = 5$ .
- Para  $2 \in \mathbb{Z}_{17}$ , encontramos que  $2^4 = -1$ , por lo que  $2^8 = 1$  y 2 no genera. Probando con 3, encontramos que  $3^2 = 9$ ,  $3^3 = 10$ ,  $3^4 = 13$ ,  $3^5 = 5$ ,  $3^6 = 15$ ,  $3^7 = 11$ ,  $3^8 = 16 = -1$ . Dado que el orden de 3 debe dividir 16, vemos que 3 debe tener orden 16, por lo que 3 genera las unidades en  $\mathbb{Z}_{17}$ . Por el Corolario 6.16, los únicos generadores son  $3^1 = 3$ ,  $3^3 = 10$ ,  $3^5 = 5$ ,  $3^7 = 11$ ,  $3^9 = 14$ ,  $3^{11} = 7$ ,  $3^{13} = 12$ , y  $3^{15} = 6$ .
- Para  $2 \in \mathbb{Z}_{23}$ , encontramos que  $2^2 = 4$ ,  $2^3 = 8$ ,  $2^4 = 16$ ,  $2^5 = 9$ ,  $2^6 = 18$ ,  $2^7 = 13$ ,  $2^8 = 3$ ,  $2^9 = 6$ ,  $2^{10} = 12$ , y  $2^{11} = 1$ , por lo que 2 no genera. Sin embargo, esta computación muestra que  $(-2)^{11} = -1$ . Dado que el orden de  $-2$  debe dividir 22, vemos que  $(-2)^1 = 2$  debe tener orden 22, por lo que  $(-2)^1$  genera las unidades en  $\mathbb{Z}_{23}$ . Por el Corolario 6.16, los únicos generadores son  $(-2)^1 = 2$ ,  $(-2)^3 = 15$ ,  $(-2)^5 = 14$ ,  $(-2)^7 = 10$ ,  $(-2)^9 = 17$ ,  $(-2)^{13} = 19$ ,  $(-2)^{15} = 7$ ,  $(-2)^{17} = 5$ ,  $(-2)^{19} = 20$ , y  $(-2)^{21} = 11$ .

### Factorización de Polinomios en $\mathbb{Z}[x]$

- En  $\mathbb{Z}_5$ , tenemos  $x^4 + 4 = x^4 - 1 = (x^2 + 1)(x^2 - 1)$ . Reemplazando 1 por -4 nuevamente, continuamos y descubrimos que  $(x^2 - 4)(x^2 - 1) = (x - 2)(x + 2)(x - 1)(x + 1)$ .
- Por inspección, -1 es una raíz de  $x^3 + 2x^2 + 2x + 1$  en  $\mathbb{Z}_7[x]$ . Ejecutando el algoritmo de división como se ilustra en nuestras respuestas a los Ejercicios 1 a 3, calculamos  $x^3 + 2x^2 + 2x + 1$  dividido por  $x - (-1) = x + 1$ , y encontramos que  $x^3 + 2x^2 + 2x + 1 = (x + 1)(x^2 + x + 1)$ . Por inspección, 2 y 4 son raíces de  $x^2 + x + 1$ . Así que la factorización es  $x^3 + 2x^2 + 2x + 1 = (x + 1)(x - 4)(x - 2)$ .
- Por inspección, 3 es una raíz de  $2x^3 + 3x^2 - 7x - 5$  en  $\mathbb{Z}_{11}[x]$ . Dividiendo por  $x - 3$  usando la técnica ilustrada en nuestras respuestas a los Ejercicios 1 a 3, encontramos que  $2x^3 + 3x^2 - 7x - 5 = (x - 3)(2)(x^2 - x - 1)$ . Por inspección, -3 y 4 son raíces de  $x^2 - x - 1$ , por lo que la factorización es  $2x^3 + 3x^2 - 7x - 5 = (x - 3)(x + 3)(2x - 8)$ .

4. Por inspección,  $-1$  es una raíz de  $x^3 + 2x + 3$  en  $\mathbb{Z}_5[x]$ , por lo que el polinomio no es irreducible. Dividiendo por  $x + 1$  usando la técnica de los Ejercicios 1 a 3, obtenemos  $x^3 + 2x + 3 = (x + 1)(x^2 - x + 3)$ . Por inspección,  $-1$  y  $2$  son raíces de  $x^2 - x + 3$ , por lo que la factorización es  $x^3 + 2x + 3 = (x + 1)(x + 1)(x - 2)$ .

### Irreducibilidad y Factorización de Polinomios

1. Sea  $f(x) = 2x^3 + x^2 + 2x + 2$  en  $\mathbb{Z}_5[x]$ . Entonces  $f(0) = 2$ ,  $f(1) = 2$ ,  $f(-1) = -1$ ,  $f(2) = 1$ , y  $f(-2) = 1$ , por lo que  $f(x)$  no tiene ceros en  $\mathbb{Z}_5$ . Dado que  $f(x)$  es de grado 3, el Teorema 23.10 muestra que  $f(x)$  es irreducible sobre  $\mathbb{Z}_5$ .
2.  $f(x) = x^2 + 8x - 2$  satisface la condición de Eisenstein para irreducibilidad sobre  $\mathbb{Q}$  con  $p = 2$ . No es irreducible sobre  $\mathbb{R}$  porque la fórmula cuadrática muestra que tiene raíces reales  $(-8 \pm \sqrt{72})/2$ . Por supuesto, tampoco es irreducible sobre  $\mathbb{C}$ .
3. El polinomio  $g(x) = x^2 + 6x + 12$  es irreducible sobre  $\mathbb{Q}$  porque satisface la condición de Eisenstein con  $p = 3$ . También es irreducible sobre  $\mathbb{R}$  porque la fórmula cuadrática muestra que sus raíces son  $(-6 \pm \sqrt{-12})/2$ , que no están en  $\mathbb{R}$ . No es irreducible sobre  $\mathbb{C}$  porque sus raíces están en  $\mathbb{C}$ .
4. Si  $x^3 + 3x^2 - 8$  es reducible sobre  $\mathbb{Q}$ , entonces, por el Teorema 23.11, se factoriza en  $Z[x]$  y debe tener un factor lineal de la forma  $x - a$  en  $Z[x]$ . Entonces,  $a$  debe ser una raíz del polinomio y debe dividir a  $-8$ , por lo que las posibilidades son  $a = \pm 1, \pm 2, \pm 4, \pm 8$ . Calculando el polinomio en estos valores, encontramos que ninguno de ellos es raíz del polinomio, que es entonces irreducible sobre  $\mathbb{Q}$ .
5. Si  $x^4 - 22x^2 + 1$  es reducible sobre  $\mathbb{Q}$ , entonces, por el Teorema 23.11, se factoriza en  $Z[x]$  y debe ser un factor lineal en  $Z[x]$  o factorizar en dos cuadráticos en  $Z[x]$ . Las únicas posibilidades para un factor lineal son  $x \pm 1$ , y claramente ni  $1$  ni  $-1$  son raíces del polinomio, por lo que un factor lineal es imposible. Supongamos

$$x^4 - 22x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d).$$

Igualando coeficientes, vemos que el coeficiente  $x^3$  es  $0$ , por lo que  $a + c = 0$ , el coeficiente  $x^2$  es  $-22$ , por lo que  $ac + b + d = -22$ , el coeficiente  $x$  es  $0$ , por lo que  $bc + ad = 0$ , y el término constante es  $1$ , por lo que  $bd = 1$ . Entonces,  $b = d = 1$  o  $b = d = -1$ .

Supongamos  $b = d = 1$ . Entonces,  $-22 = ac + 1 + 1$ , así que  $ac = -24$ . Debido a que  $a + c = 0$ , tenemos  $a = -c$ , por lo que  $-c^2 = -24$ , lo cual es imposible para un entero  $c$ . Similarmente, si  $b = d = -1$ , deducimos que  $-c^2 = -20$ , lo cual también es imposible. Por lo tanto, el polinomio es irreducible.

### Criterio de Eisenstein

1. Sí, con  $p = 3$ .
2. Sí, con  $p = 3$ .
3. No, ya que  $2$  divide al coeficiente  $4$  de  $4x^{10} - 9x^3 + 2Ax - 18$  y  $32$  divide al término constante  $-18$ .

4. Sí, con  $p = 5$ .

### Encontrar las Raíces de un Polinomio

1. Encuentra todas las raíces de  $6x^4 + 17x^3 + 11x^2 + x - 10$  en  $\mathbb{Q}$ .

1. Observa que  $x^2 = x \cdot x$  y  $x^2 + 1 = (x+1)^2$  son reducibles en  $\mathbb{Z}_p$ . Para un número primo impar  $p$  y  $a \in \mathbb{Z}_p$ , sabemos que  $(-a)^p + a = -a^p + a = -a + a = 0$  por el Corolario 20.2. Por lo tanto,  $x^p + a$  tiene a  $-a$  como raíz, por lo que es reducible sobre  $\mathbb{Z}_p$  para todo primo  $p$ . [De hecho, el teorema binómico y el Corolario 20.2 muestran que  $x^p + a = (x+a)^p$ .

2. Dado que  $f(a) = a_0 + a_1a + \dots + a_na^n = 0$  y  $a^n \neq 0$ , al dividir por  $a^n$ , obtenemos  $a_0 \left(\frac{1}{a}\right)^n + a_1 \left(\frac{1}{a}\right)^{n-1} + \dots + a_n = 0$ , que es lo que queríamos mostrar.

3. Por el Teorema 23.1, sabemos que  $f(x) = q(x)(x-a) + c$  para alguna constante  $c \in F$ . Aplicando el homomorfismo de evaluación  $\phi_a$  a ambos lados de esta ecuación, obtenemos  $f(a) = q(a)(a-a) + c = q(a) \cdot 0 + c = c$ , por lo que el resto  $r(x) = c$  es realmente  $f(a)$ .

4. a. Sea  $f(x) = \sum_{i=0}^{\infty} a_i x^i$  y  $g(x) = \sum_{i=0}^{\infty} b_i x^i$ . Entonces,

$$\sigma_m(f(x) + g(x)) = \sum_{i=0}^{\infty} (\sigma_m(a_i) + \sigma_m(b_i)) x^i = \sigma_m(f(x)) + \sigma_m(g(x)),$$

y

$$\sigma_m(f(x) \cdot g(x)) = \sum_{n=0}^{\infty} \left( \sum_{i=0}^n \sigma_m(a_i b_{n-i}) \right) x^n = \sigma_m(f(x)) \cdot \sigma_m(g(x)),$$

por lo que  $\sigma_m$  es un homomorfismo. Si  $h(x) \in \mathbb{Z}_m[x]$ , entonces si  $k(x)$  es el polinomio en  $\mathbb{Z}[x]$  obtenido de  $h(x)$  al considerar solo los coeficientes como elementos de  $\mathbb{Z}$  en lugar de  $\mathbb{Z}_m$ , vemos que  $\sigma_m(k(x)) = h(x)$ , por lo que el homomorfismo  $\sigma_m$  es sobre  $\mathbb{Z}_m[x]$ .

b. Supongamos que  $f(x) = g(x)h(x)$  para  $g(x), h(x) \in \mathbb{Z}[x]$  con los grados tanto de  $g(x)$  como de  $h(x)$  menores que el grado  $n$  de  $f(x)$ . Aplicando el homomorfismo  $\sigma_m$ , vemos que  $\sigma_m(f(x)) = \sigma_m(g(x)) \cdot \sigma_m(h(x))$  es una factorización de  $\sigma_m(f(x))$  en dos polinomios de grado menor que el grado  $n$  de  $\sigma_m(f(x))$ , lo cual es contrario a la hipótesis. Por lo tanto,  $f(x)$  es irreducible en  $\mathbb{Q}[x]$ .

c. Tomando  $m = 5$ , vemos que  $\sigma_5(x^3 + 17x + 36) = x^3 + 2x + 1$ , el cual no tiene ninguno de los cinco elementos 0, 1, -1, 2, -2 de  $\mathbb{Z}_5$  como cero, y por lo tanto, es irreducible sobre  $\mathbb{Z}_5$  por el Teorema 23.10. Por la Parte (b), concluimos que  $x^3 + 17x + 36$  es irreducible sobre  $\mathbb{Q}$ .

### 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.