Sección 45

En los Ejercicios 1 a 8, determine si el elemento es irreducible en el dominio indicado.

1. 5 en $\mathbb{Z}$

   Solución: Sí, 5 es irreducible en $\mathbb{Z}$.

2. -17 en $\mathbb{Z}$

   Solución: Sí, -17 es irreducible en $\mathbb{Z}$.

3. 14 en $\mathbb{Z}$

   Solución: No, $14 = 2 \cdot 7$ no es irreducible en $\mathbb{Z}$.

4. $2x - 3$ en $\mathbb{Z}[x]$

   Solución: Sí, $2x - 3$ es irreducible en $\mathbb{Z}[x]$.

5. $2x - 10$ en $\mathbb{Z}[x]$

   Solución: No, $2x - 10 = 2(x - 5)$ no es irreducible en $\mathbb{Z}[x]$.

6. $2x - 3$ en $\mathbb{Q}[x]$

   Solución: Sí, $2x - 3$ es irreducible en $\mathbb{Q}[x]$.

7. $2x - 10$ en $\mathbb{Q}[x]$

   Solución: Sí, $2x - 10$ es irreducible en $\mathbb{Q}[x]$, ya que 2 es una unidad en este dominio.

8. $2x - 10$ en $\mathbb{Z}_{11}[x]$

   Solución: Sí, $2x - 10$ es irreducible en $\mathbb{Z}_{11}[x]$, ya que 2 es una unidad en este dominio.

9. Si es posible, dé cuatro diferentes asociados de $2x - 7$ visto como un elemento de $\mathbb{Z}[x]$; de $\mathbb{Q}[x]$; de $\mathbb{Z}_{11}[x]$.

   Solución: (Ver la respuesta en el texto.)

10. Factorice el polinomio $4x^2 - 4x + 8$ en un producto de irreducibles viéndolo como un elemento del dominio integral $\mathbb{Z}[x]$; del dominio integral $\mathbb{Q}[x]$; del dominio integral $\mathbb{Z}_{11}[x]$.

    Solución: En $\mathbb{Z}[x]$, $4x^2 - 4x + 8 = (2)(2)(x^2 - x + 2)$. El polinomio cuadrático es irreducible porque sus ceros son números complejos.
    En $\mathbb{Q}[x]$, $4x^2 - 4x + 8$ ya es irreducible porque 4 es una unidad y los ceros del polinomio son números complejos.
    En $\mathbb{Z}_{11}[x]$, $4x^2 - 4x + 8 = (4x + 2)(x + 4)$. Encontramos la factorización descubriendo que -4 y 5 son ceros del polinomio. Nótese que 2 es una unidad.

11. En los Ejercicios 11 a 13, encuentre todos los mcd de los elementos dados de $\mathbb{Z}$.

    a) 234, 3250, 1690
    Solución: Procedemos factorizando el número más pequeño en irreducibles y, usando una calculadora, descubrimos cuáles irreducibles dividen a los números más grandes. Encontramos que $234 = 2 \cdot 117 = 2 \cdot 9 \cdot 13$. Nuestra calculadora muestra que 9 no divide 3250, pero 2 y 13 sí, y ambos 2 y 13 dividen 1690. Así, los mcd son 26 y -26.

b) 784, -1960, 448

Solución: Procedemos factorizando el número más pequeño en irreducibles y, usando una calculadora, descubrimos cuáles irreducibles dividen a los números más grandes. Encontramos que $448 = 4 \cdot 112 = 4 \cdot 4 \cdot 28 = 2^6 \cdot 7$. Nuestra calculadora muestra que 7 divide tanto 784 como 1960, y que la mayor potencia de 2 que divide 784 es 16 mientras que la mayor potencia que divide 1960 es 8. Así, los mcd son $8 \cdot 7 = 56$ y -56.

c) 2178, 396, 792, 594

Solución: Procedemos factorizando el número más pequeño en irreducibles y, usando una calculadora, descubrimos cuáles irreducibles dividen a los números más grandes. Encontramos que $396 = 6 \cdot 66 = 6 \cdot 6 \cdot 11 = 2^2 \cdot 3^2 \cdot 11$. Nuestra calculadora muestra que tanto 11 como 9 dividen a los otros tres números, pero 2178 y 594 no son divisibles por 4, pero sí son divisibles por 2. Así, los mcd son $11 \cdot 9 \cdot 2 = 198$ y -198.

12. En los Ejercicios 14 a 17, exprese el polinomio dado como el producto de su contenido con un polinomio primitivo en el DFI indicado.

a) $18x^2 - 12x + 48$ en $\mathbb{Z}[x]$

Solución: $18x^2 - 12x + 48 = 6(3x^2 - 2x + 8)$.

b) $18x^2 - 12x + 48$ en $\mathbb{Q}[x]$

Solución: Como cada $q \in \mathbb{Q}$ no nulo es una unidad en $\mathbb{Q}[x]$, podemos "factorizarçualquier constante racional no nula como el contenido (unidad) de este polinomio. Por ejemplo, $(1)(18x^2 - 12x + 48)$ y $\frac{1}{2}(36x^2 - 24x + 96)$ son dos de un número infinito de posibles respuestas.

c) $2x^2 - 3x + 6$ en $\mathbb{Z}[x]$

Solución: La factorización es $(1)(2x^2 - 3x + 6)$ porque el polinomio es primitivo.

d) $2x^2 - 3x + 6$ en $\mathbb{Z}_7[x]$

Solución: Como cada $a \in \mathbb{Z}_7$ no nulo es una unidad en $\mathbb{Z}_7[x]$, podemos "factorizarçualquier constante no nula como el contenido (unidad) de este polinomio. Por ejemplo,
$(1)(2x^2 - 3x + 6)$ y $(5)(6x^2 + 5x + 4)$ son dos de un número infinito de posibles respuestas.

25. Demuestre que si p es un primo en un dominio integral D, entonces p es irreducible.

Solución: Sea p un primo de D, y supongamos que $p = ab$ para algunos $a, b \in D$. Entonces $ab = (1)p$, por lo que p divide a ab y, por lo tanto, divide a a o b, porque p es un primo. Supongamos que $a = pc$. Entonces $p = (1)p = pcb$ y la cancelación en el dominio integral produce $1 = cb$, por lo que b es una unidad de D. Del mismo modo, si p divide b, concluimos que a es una unidad en D. Por lo tanto, a o b es una unidad, así que p es irreducible.

26. Demuestre que si p es un irreducible en un DFI, entonces p es un primo.

Solución: Sea p un irreducible en un DFI, y supongamos que p divide a ab. Debemos demostrar que p divide a a o p divide a b. Sea $ab = pc$, y factorizamos ab en irreducibles factorizando primero a en irreducibles, luego factorizando b en irreducibles, y finalmente tomando el producto de estas dos factorizaciones. Ahora, ab también podría factorizarse en irreducibles tomando p y una factorización de c en irreducibles. Dado que la factorización en irreducibles en un DFI es única hasta el orden y los asociados, debe ser que un asociado de

p aparece en la primera factorización, formada por los factores de a y los factores de b. Así, un asociado de p, digamos up, aparece en la factorización de a o en la factorización de b. Se deduce de inmediato que p divide a a o b.

27. Para un anillo conmutativo R con unidad, muestre que la relación $a \sim b$ si a es un asociado de b (es decir, si $a = bu$ para una unidad u en R) es una relación de equivalencia en R.

    Solución:

    - Reflexiva: $a = a \cdot 1$, por lo que $a \sim a$.
    - Simétrica: Supongamos $a \sim b$, de modo que $a = bu$ para una unidad u. Entonces u^{-1} es una unidad y $b = au^{-1}$, por lo que $b \sim a$.
    - Transitiva: Supongamos que $a \sim b$ y $b \sim c$. Entonces hay unidades u_1 y u_2 tales que $a = bu_1$ y $b = cu_2$. Sustituyendo, tenemos $a = cu_2u_1 = c(u_2u_1)$. Como el producto u_2u_1 de dos unidades es de nuevo una unidad, encontramos que $a \sim c$.

28. Sea D un dominio integral. El Ejercicio 37, Sección 18 mostró que $\langle U, \cdot \rangle$ es un grupo donde U es el conjunto de unidades de D. Muestre que el conjunto $D^* - U$ de los no unidades de D excluyendo el 0 está cerrado bajo la multiplicación. ¿Es este conjunto un grupo bajo la multiplicación de D?

    Solución: Sea a y b no unidades en $D^* - U$. Supongamos que ab es una unidad, de modo que $(ab)c = 1$ para algún $c \in D$. Entonces $a(bc) = 1$ y a es una unidad, lo cual es contrario a nuestra elección de a. Por lo tanto, ab es de nuevo una no unidad, y $ab \neq 0$ porque D no tiene divisores de cero. Así, $ab \in D^* - U$. Vemos que $D^* - U$ no es un grupo, porque la identidad multiplicativa es una unidad y, por lo tanto, no está en $D^* - U$.

29. Sea D un DFI. Muestre que un divisor no constante de un polinomio primitivo en $D[x]$ es nuevamente un polinomio primitivo.

    Solución: Sea $g(x)$ un divisor no constante del polinomio primitivo $f(x)$ en $D[x]$. Supongamos que $f(x) = g(x)q(x)$. Como D es un DFI, sabemos que $D[x]$ también es un DFI. Factorizamos $f(x)$ en irreducibles factorizando cada uno de $g(x)$ y $q(x)$ en irreducibles, y luego tomando el producto de estas factorizaciones. Cada factor no constante que aparece es un irreducible en $D[x]$ y, por lo tanto, es un polinomio primitivo. Como el producto de polinomios primitivos es primitivo por el Corolario 45.26, vemos que el contenido de $g(x)q(x)$ es el producto del contenido de $g(x)$ y el contenido de $q(x)$, y debe ser el mismo (hasta un factor unidad) que el contenido de $f(x)$. Pero $f(x)$ tiene contenido 1 porque es primitivo. Así, $g(x)$ y $q(x)$ tienen contenido 1. Por lo tanto, $g(x)$ es un producto de polinomios primitivos, así que es primitivo por el Corolario 45.26.

30. Sea N un ideal en un PID D. Si N no es maximal, entonces hay un ideal propio N_1 de D tal que $N \subset N_1$. Si N_1 no es maximal, encontramos un ideal propio N_2 tal que $N_1 \subset N_2$. Continuando este proceso, construimos una cadena $N \subset N_1 \subset N_2 \subset \cdots \subset N_i$ de ideales propios, cada uno propiamente contenido en el siguiente excepto por el último ideal. Como un PID satisface la condición de la cadena ascendente, no podemos extender esto a una cadena infinita, por lo que después de un número finito de pasos debemos encontrar un ideal propio N_r que contenga a N y que no esté propiamente contenido en ningún ideal propio de D. Es decir, alcanzamos un ideal maximal N_r de D que contiene a N.

31. Factorice $x^3 - y^3$ en irreducibles en $\mathbb{Q}[x, y]$ y demuestre que cada uno de los factores es irreducible.

    Solución: Tenemos $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$. Por supuesto, $x - y$ es irreducible. Afirmamos que x^2+xy+y^2 es irreducible en $\mathbb{Q}[x, y]$. Supongamos que x^2+xy+y^2 se factoriza en un producto de dos polinomios que no son unidades en $\mathbb{Q}[x, y]$. Tal factorización tendría que ser de la forma $x^2 + xy + y^2 = (ax + by)(cx + dy)$ con a, b, c y d todos elementos no nulos de $\mathbb{Q}$. Consideremos el homomorfismo de evaluación $\phi_1 : (\mathbb{Q}[x])[y] \to \mathbb{Q}[x]$ tal que $\phi(y) = 1$. Aplicando ϕ_1 a ambos lados de dicha factorización obtendríamos $x^2+x+1 = (ax+b)(cx+d)$. Pero $x^2 + x + 1$ es irreducible en $\mathbb{Q}[x]$ porque sus ceros son complejos, por lo que no existe tal factorización. Esto muestra que $x^2 + xy + y^2$ es irreducible en $(\mathbb{Q}[x])[y]$, que es isomórfico a $\mathbb{Q}[x, y]$ bajo un isomorfismo que identifica $y^2 + yx + x^2$ y $x^2 + xy + y^2$.

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.