Matemática Discreta

Vaira, Stella - Fedonczuk, Miguel
Colliard, David - Cottonaro, Mariana

Lic en Sistemas de Información - FCyT - UADER

2022

Anillos.

Homomorfirmo de Anillos. Isomorfirmo de Anillos. Teorema Chino del Resto.

Ejemplo introductorio

Consideremos los anillos $(\mathbf{Z}, +, \cdot)$ y $(\mathbf{Z}_6, +, \cdot)$, donde la suma y el producto de $\mathbf{Z}_6$ se definen como en la sección 14.3.

Definimos $f: \mathbf{Z} \to \mathbf{Z}_6$ como $f(x) = [x]$. Por ejemplo, $f(1) = [1] = [7] = f(7)$ y $f(2) = f(8) = f(2 + 6k) = [2]$, para cualquier $k \in \mathbf{Z}$. (Así, f es sobre pero no inyectiva.)

Para $2, 3 \in \mathbf{Z}$, $f(2) = [2]$, $f(3) = [3]$ y tenemos que $f(2 + 3) = f(5) = [5] = [2] + [3] = f(2) + f(3)$ y $f(2 \cdot 3) = f(6) = [0] = [2][3] = f(2) \cdot f(3)$.

De hecho, para cualesquiera $x, y \in \mathbf{Z}$,

$$f(x + y) = [x + y] = [x] + [y] = f(x) + f(y),$$

($+$ en $\mathbf{Z}$ a la izquierda; $+$ en $\mathbf{Z}_6$ a la derecha)

$$f(x \cdot y) = [xy] = [x][y] = f(x) \cdot f(y).$$

(producto en $\mathbf{Z}$ a la izquierda; producto en $\mathbf{Z}_6$ a la derecha)

Este ejemplo nos lleva a la siguiente definición.

Definición

Sea $(R, +, \cdot)$ y $(S, \oplus, \odot)$ anillos. Una función $f : R \to S$ es un **homomorfirmos de anillos** si para todos a, b de R:

1. $f(a + b) = f(a) \oplus f(b)$
2. $f(a \cdot b) = f(a) \odot f(b)$

Si además, la función f es biyectiva, entonces tendremos un **isomorfismo de anillos**.

Ejemplo:

Para el anillo R del ejemplo 14.5 y el anillo $\mathbf{Z}_5$, la función $f: R \to \mathbf{Z}_5$ dada por

$$f(a) = [0], \qquad f(b) = [1], \qquad f(c) = [2], \qquad f(d) = [3], \qquad f(e) = [4]$$

es un isomorfismo de anillos.

Por ejemplo, $f(c + d) = f(a) = [0] = [2] + [3] + f(c) + f(d)$, mientras que $f(be) = f(e) = [4] = [1][4] = f(b)\, f(e)$. (Como no disponemos de otros métodos y teoremas, hay que verificar 25 igualdades de este tipo para que se preserven las operaciones binarias.)

+	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c
e	e	a	b	c	d

·	a	b	c	d	e
a	a	a	a	a	a
b	a	b	c	d	e
c	a	c	e	b	d
d	a	d	b	e	c
e	a	e	d	c	b

Teorema

Sea $f : (R, +, \cdot) \to (S, \oplus, \odot)$ es un homomorfismo de anillos, entonces para todo $a \in R$:

1. $f(z_R) = z_S$ con z_R y z_S neutros de R y S respectivamente.
2. $f(-a) = -f(a)$
3. $f(na) = nf(a)$ con n entero.
4. $f(a^n) = [f(a)]^n$, con n natural.
5. si A es un subanillo de R, entonces $f(A)$ es un subanillo de S.

Además, si $|S| > 1$:

1. si R tiene elemento unidad u_R, entonces $f(u_r)$ es el elemento unidad de S.
2. si a es una unidad de R, entonces $f(a)$ es una unidad en S, y $f(a^{-1}) = [f(a)]^{-1}$.
3. si R es conmutativo, entonces S es conmutativo.
4. si I es un ideal de R, entonces $f(I)$ es un ideal de S.

Ejemplo:

Sean $\mathbf{C}$ el cuerpo de los números complejos y S el anillo de las matrices reales 2×2 de la forma $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$; definimos $f: \mathbf{C} \to S$ como $f(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, para $a+bi \in \mathbf{C}$. Entonces

$$a+bi = c+di \Leftrightarrow a=c, b=d \Leftrightarrow \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix},$$

por lo que f es una función inyectiva. También es sobre. (¿Por qué?)

Además,

$$\begin{aligned} f((a+bi)+(x+yi)) &= f((a+x)+(b+y)i) \\ &= \begin{bmatrix} a+x & b+y \\ -(b+y) & a+x \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \\ &= f(a+bi) + f(x+yi), \end{aligned}$$

y

$$\begin{aligned} f((a+bi)(x+yi)) &= f((ax-by)+(bx+ay)i) \\ &= \begin{bmatrix} ax-by & bx+ay \\ -(bx+ay) & ax-by \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \\ &= f(a+bi) f(x+yi), \end{aligned}$$

De esta manera f es un isomorfirsmo entre los anillos dados.

¿Cómo podríamos utilizar este isomorfismo?

Podríamos calcular esta operación entre números complejos operando matricialmente como sigue:

$$(-8.3 + 9.9i) + \frac{(5.2 - 7.1i)^7}{(1.3 + 3.7i)^4}$$

$$\begin{bmatrix} -8.3 & 9.9 \\ -9.9 & -8.3 \end{bmatrix} + \begin{bmatrix} 5.2 & -7.1 \\ 7.1 & 5.2 \end{bmatrix}^7 \left(\begin{bmatrix} 1.3 & 3.7 \\ -3.7 & 1.3 \end{bmatrix}^4 \right)^{-1} = \begin{bmatrix} 8379.98 & 15122.7 \\ -15122.7 & 8379.98 \end{bmatrix}$$

$$8379.98 + 15122.7i.$$

Observemos el siguiente conjunto:

$$R = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

Sus elementos son ternas, y cada componente pertenece a $\mathbb{Z}_2$, $\mathbb{Z}_3$ y $\mathbb{Z}_5$, respectivamente. De esta manera la cantidad de elementos de R es $|R| = |\mathbb{Z}_2| \cdot |\mathbb{Z}_3| \cdot |\mathbb{Z}_5| = 30$.
Se definen las operaciones adición y multiplicación en R como sigue:

$$(a_1, a_2, a_3) \oplus (b_1, b_2, b_3) = (a_1 + b_1, a_2 + b_2, a_3 + b_3)$$

Addition in R — Addition in $\mathbb{Z}_2$ — Addition in $\mathbb{Z}_3$ — Addition in $\mathbb{Z}_5$

$$(a_1, a_2, a_3) \odot (b_1, b_2, b_3) = (a_1 \cdot b_1, a_2 \cdot b_2, a_3 \cdot b_3).$$

Multiplication in R — Multiplication in $\mathbb{Z}_2$ — Multiplication in $\mathbb{Z}_3$ — Multiplication in $\mathbb{Z}_5$

Se puede demostrar que la estructura $(R, \oplus, \odot)$ es un anillo.
Sus elementos treinta son:

(0, 0, 0)	(1, 2, 0)	(0, 1, 0)	(1, 0, 0)	(0, 2, 0)	(1, 1, 0)
(1, 1, 1)	(0, 0, 1)	(1, 2, 1)	(0, 1, 1)	(1, 0, 1)	(0, 2, 1)
(0, 2, 2)	(1, 1, 2)	(0, 0, 2)	(1, 2, 2)	(0, 1, 2)	(1, 0, 2)
(1, 0, 3)	(0, 2, 3)	(1, 1, 3)	(0, 0, 3)	(1, 2, 3)	(0, 1, 3)
(0, 1, 4)	(1, 0, 4)	(0, 2, 4)	(1, 1, 4)	(0, 0, 4)	(1, 2, 4)

Resolver las siguientes operaciones:

1. $(1, 2, 3) \oplus (1, 0, 3) \odot (1, 1, 0)$
2. $(1, 2, 2) \odot (1, 1, 3)$
3. $(1, 2, 2) \odot (1, 2, 3)$

Teorema Chino del Resto

Sea la descomposición factorial de $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, los anillos $\mathbb{Z}_n$ y $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$ son isomorfos, con $m_1 = p_1^{e_1}$, $m_2 = p_2^{e_2}, \ldots, m_k = p_k^{e_k}$

Ejemplo:
$\mathbb{Z}_{30}$ y $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ lo son. Las operaciones involucradas en cada estructura son adición y multiplicación, cada una en su respectivo módulo. A continuación se puede ver que la siguiente función $f : \mathbb{Z}_{30} \to \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ determina un homomorfirmo entre los anillos.

$$
\begin{aligned}
f(x+y) &= ((x+y) \bmod 2,\ (x+y) \bmod 3,\ (x+y) \bmod 5) \\
&= (x \bmod 2,\ x \bmod 3,\ x \bmod 5) \oplus (y \bmod 2,\ y \bmod 3,\ y \bmod 5) \\
&= f(x) \oplus f(y),
\end{aligned}
$$

$$
\begin{aligned}
f(xy) &= (xy \bmod 2,\ xy \bmod 3,\ xy \bmod 5) \\
&= (x \bmod 2,\ x \bmod 3,\ x \bmod 5) \odot (y \bmod 2,\ y \bmod 3,\ y \bmod 5) \\
&= f(x) \odot f(y)
\end{aligned}
$$

Además, la tabla muestra que la función es biyectiva (uno a uno); y de esta manera los anillos involucrados resultan **isomorfos**.

x (in $\mathbf{Z}_{30}$)	$f(x)$ (in R)	x (in $\mathbf{Z}_{30}$)	$f(x)$ (in R)	x (in $\mathbf{Z}_{30}$)	$f(x)$ (in R)
0	(0, 0, 0)	10	(0, 1, 0)	20	(0, 2, 0)
1	(1, 1, 1)	11	(1, 2, 1)	21	(1, 0, 1)
2	(0, 2, 2)	12	(0, 0, 2)	22	(0, 1, 2)
3	(1, 0, 3)	13	(1, 1, 3)	23	(1, 2, 3)
4	(0, 1, 4)	14	(0, 2, 4)	24	(0, 0, 4)
5	(1, 2, 0)	15	(1, 0, 0)	25	(1, 1, 0)
6	(0, 0, 1)	16	(0, 1, 1)	26	(0, 2, 1)
7	(1, 1, 2)	17	(1, 2, 2)	27	(1, 0, 2)
8	(0, 2, 3)	18	(0, 0, 3)	28	(0, 1, 3)
9	(1, 0, 4)	19	(1, 1, 4)	29	(1, 2, 4)

De esta manera, utilizando la tabla, podríamos hallar fácilmente:

1. $(1, 2, 3) \oplus (1, 0, 3) \odot (1, 1, 0)$
2. $(1, 2, 2)^{-1}$
3. $(1, 2, 2) \odot X = (1, 2, 3) \oplus (1, 0, 3) \odot (1, 1, 0)$