Matemática Discreta

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

Lic en Sistemas de Información - FCyT - UADER

2022

Anillos.

Propiedades. Subestructuras de un anillo.

Teorema

En cualquier anillo $(R, +, \cdot)$
a) el elemento neutro z es único
b) el inverso aditivo de cada elemento del anillo es único.

Demostración:

a) Si R tiene más de una identidad aditiva, sean z_1, z_2 dos de tales elementos. Entonces

$$z_1 = z_1 + z_2 = z_2.$$

Ya que z_2 es una identidad aditiva

Ya que z_1 es una identidad aditiva

b) Para $a \in R$, supongamos que existen dos elementos $b, c \in R$ tales que $a + b = b + a = z$ y $a + c = c + a = z$. Entonces $b = b + z = b + (a + c) = (b + a) + c = z + c = c$. (El lector debe indicar la condición que establece cada igualdad.)

Observación:

a) De ahora en más el inverso aditivo de un elemento a se denotará como $-a$

b) Hablaremos de *resta* en un anillo haciendo referencia a $x - y = x + (-y)$

TEOREMA 14.2 (*Las leyes de cancelación para la suma*) Para cualesquiera $a, b, c \in R$,

a) $a + b = a + c \Rightarrow b = c$, y
b) $b + a = c + a \Rightarrow b = c$.

TEOREMA 14.3 Para cualquier anillo $(R, +, \cdot)$ y cualquier $a \in R$, tenemos $az = za = z$.

TEOREMA 14.4 Dado un anillo $(R, +, \cdot)$ y $a, b \in R$,

a) $-(-a) = a$,
b) $a(-b) = (-a)b = -(ab)$, y
c) $(-a)(-b) = ab$.

TEOREMA 14.5 Para un anillo $(R, +, \cdot)$,

a) Si R tiene un elemento unidad, entonces es único, y
b) si R tiene un elemento unidad y x es una unidad de R, entonces el inverso multiplicativo de x es único.

TEOREMA 14.7 Si $(F, +, \cdot)$ es un cuerpo, entonces es un dominio de integridad.

TEOREMA 14.8 Un dominio de integridad *finito* $(D, +, \cdot)$ es un cuerpo.

Definición 14.5 Para un anillo $(R, +, \cdot)$, un subconjunto no vacío S de R es un *subanillo* de R si $(S, +, \cdot)$ (es decir, S con la suma y producto de R restringidos a S) es un anillo.

TEOREMA 14.10 Para cualquier anillo $(R, +, \cdot)$, si $\emptyset \neq S \subseteq R$,

a) entonces $(S, +, \cdot)$ es un subanillo de R si y sólo si para todos $a, b \in S$, tenemos que $a - b \in S$ y $ab \in S$;

b) y si S es finito, entonces $(S, +, \cdot)$ es un subanillo de R si y sólo si para todos $a, b \in S$, tenemos que $a + b, ab \in S$. (De nuevo, la ayuda adicional proviene de una condición de ser finito.)

Ejemplo 14.11 Consideremos el anillo $R = M_2(\mathbf{Z})$ y el subconjunto

$$S = \left\{ \begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix} \middle| x, y \in \mathbf{Z} \right\}$$

de R. Cuando $x = y = 0$, se sigue que $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in S$ y $S \neq \emptyset$. Así, ahora analizamos cualquier par de elementos de S; es decir, dos matrices de la forma

$$\begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix} \quad \text{y} \quad \begin{bmatrix} \upsilon & \upsilon+w \\ \upsilon+w & \upsilon \end{bmatrix},$$

donde $x, y, \upsilon, w \in \mathbf{Z}$. Tenemos que

$$\begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix} - \begin{bmatrix} \upsilon & \upsilon+w \\ \upsilon+w & \upsilon \end{bmatrix} = \begin{bmatrix} x-\upsilon & (x-\upsilon)+(y-w) \\ (x-\upsilon)+(y-w) & x-\upsilon \end{bmatrix},$$

por lo que S es cerrado en la resta. Al pasar a la multiplicación, tenemos

$$\begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix}\begin{bmatrix} \upsilon & \upsilon+w \\ \upsilon+w & \upsilon \end{bmatrix}$$

$$= \begin{bmatrix} x\upsilon+(x+y)(\upsilon+w) & x(\upsilon+w)+(x+y)\upsilon \\ (x+y)\upsilon+x(\upsilon+w) & (x+y)(\upsilon+w)+x\upsilon \end{bmatrix}$$

$$= \begin{bmatrix} x\upsilon+x\upsilon+y\upsilon+xw+yw & x\upsilon+xw+x\upsilon+y\upsilon \\ x\upsilon+y\upsilon+x\upsilon+xw & x\upsilon+y\upsilon+xw+yw+x\upsilon \end{bmatrix}$$

$$= \begin{bmatrix} x\upsilon+x\upsilon+y\upsilon+xw+yw & (x\upsilon+x\upsilon+y\upsilon+xw+yw)+(-yw) \\ (x\upsilon+x\upsilon+y\upsilon+xw+yw)+(-yw) & x\upsilon+x\upsilon+y\upsilon+xw+yw \end{bmatrix},$$

por lo que S también es cerrado en la multiplicación.

Recurrimos entonces a la parte (a) del teorema 14.10 y tenemos que S es un subanillo de R.

Definición 14.6 Un subconjunto no vacío I de un anillo R es un *ideal* de R si para todos $a, b \in I$ y todo $r \in R$, tenemos que (a) $a - b \in I$ y (b) $ar, ra \in I$.

Un ideal es un subanillo, pero el recíproco no siempre se cumple: $(\mathbf{Z}, +, \cdot)$ es un subanillo de $(\mathbf{Q}, +, \cdot)$ pero no es un ideal, ya que, por ejemplo, $(1/2)9 \notin \mathbf{Z}$ aunque $(1/2) \in \mathbf{Q}$, $9 \in \mathbf{Z}$. Por otro lado, todos los subanillos del ejemplo 14.8(a) son ideales de $(\mathbf{Z}, +, \cdot)$.

EJERCICIOS 14.2

10. Sea $R = M_2(\mathbf{Z})$ y sea S el subconjunto de R dado por

$$S = \left\{ \begin{bmatrix} x & x-y \\ x-y & y \end{bmatrix} \middle| x, y \in \mathbf{Z} \right\}.$$

Demuestre que S es un subanillo de R.

15. **a)** Para $R = M_2(\mathbf{Z})$, demuestre que

$$S = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \middle| a \in \mathbf{Z} \right\}$$

es un subanillo de R.

b) ¿Cuál es el elemento unidad de R?

c) ¿Tiene S un elemento unidad?

d) ¿Tiene S propiedades que R no tenga?

e) ¿Es S un ideal de R?

20. Sea $(R, +, \cdot)$ el anillo (finito) conmutativo con elemento unidad, dado por las tablas 14.6(a) y (b).

Tabla 14.6

$+$	z	u	a	b
z	z	u	a	b
u	u	z	b	a
a	a	b	z	u
b	b	a	u	z

(a)

$\cdot$	z	u	a	b
z	z	z	z	z
u	z	u	a	b
a	z	a	b	u
b	z	b	u	a

(b)

a) Verifique que R es un cuerpo.
b) Encuentre un subanillo de R que no sea un ideal.
c) Sean x, y incógnitas. Resuelva el siguiente sistema de ecuaciones lineales en R : $bx + y = u$; $x + by = z$.