Matemática Discreta

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

Lic en Sistemas de Información - FCyT - UADER

2022

Anillos.

La estructura de anillo: definición y ejemplos.

Anillo

Si R es un conjunto no vacío con dos operaciones binarias cerradas, denotadas con $+$ y $\cdot$ (que pueden ser diferentes de la suma y producto usuales). Entonces $(R, +, \cdot)$ es un *anillo* si para todos $a, b, c \in R$ se cumplen las siguientes condiciones:

1. $a + b = b + a$. (ley de conmutativa de $+$)
2. $a + (b + c) = (a + b) + c$ (ley asociativa de $+$)
3. $\exists z \in R$ tal que $a + z = z + a = a$, $\forall a \in R$ (Identidad para $+$)
4. $\forall a \in R$, $\exists b \in R /\ a + b = b + a = z$ (inverso bajo $+$)
5. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (ley asociativa de $\cdot$)
6. $a \cdot (b + c) = a \cdot b + a \cdot c$, y $(b + c) \cdot a = b \cdot a + c \cdot a$ (distributivas)

Al trabajar con la segunda operación, en vez de escribir $a \cdot b$ se escribe con frecuencia ab. Además por medio de Inducción matemática se puede probar que dichas propiedades sobre las operaciones se pueden extender para n elementos del anillo definido.

Ejemplo 1

Con las operaciones binarias (cerradas) de la suma y producto usuales, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son anillos. En todos estos anillos, la identidad de la suma z es el entero 0 y el inverso aditivo de cualquier número x es $-x$.

Ejemplo 2

Sea $M_2(\mathbb{Z})$ el conjunto de todas las matrices 2×2 con elementos enteros. En $M_2(\mathbb{Z})$, dos matrices son iguales si sus elementos correspondientes son iguales en $\mathbb{Z}$. Se definen $+$ y $\cdot$ como sigue:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$$

Conocidas como suma y producto usuales entre matrices.

Se puede probar que $(M_2(\mathbb{Z}), +, \cdot)$ es un anillo. Como se puede ver fácilmente, la identidad z y el inverso aditivos de A son respectivamente:

$$z = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad (-A) = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$$

Observar qué ocurre con estas multiplicaciones:

$$\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 3 & 7 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 7 \\ 4 & 7 \end{bmatrix} \qquad \begin{bmatrix} 3 & 7 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 10 & 13 \\ 1 & 2 \end{bmatrix}$$

Entonces...

$$\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Entonces...

Sea $(R, +, \cdot)$ un anillo.

1. Si $ab = ba$, $\forall a, b \in R$, entonces R es un *anillo conmutativo.*
2. El anillo R no tiene *divisores propios de cero* si para cualquiera $a, b \in R$, $ab = z$ implica que $a = z$ o $b = z$.
3. Si un elemento $u \in R$ es tal que $u \neq z$ y $au = ua = a$ para todo $a \in R$, decimos que u es *elemento unidad* (o identidad para el producto) de R. Entonces R es un *anillo con unidad.*

Ejemplo 1

Analicemos si la estructura $(\mathbb{Z}, \oplus, \odot)$, con las operaciones definidas a continuación, es un anillo:

$$x \oplus y = x + y - 1 \qquad x \odot y = x + y - xy$$

Ejemplo 2
Sea $\mathsf{U} = \{1, 2\}$ y $R = \mathsf{P}(\mathsf{U})$. Definimos $+$ y $\cdot$ sobre los elementos de R como:

$$A + B = A \Delta B = (A \cup B) - (A \cap B) \qquad A \cdot B = A \cap B$$

Como el conjunto de partes de U es finito, podemos ver los resultados en las siguientes tablas. Analicemos si dicha estructura es un anillo:

$+ (\Delta)$	$\emptyset$	$\{1\}$	$\{2\}$	$\mathcal{U}$
$\emptyset$	$\emptyset$	$\{1\}$	$\{2\}$	$\mathcal{U}$
$\{1\}$	$\{1\}$	$\emptyset$	$\mathcal{U}$	$\{2\}$
$\{2\}$	$\{2\}$	$\mathcal{U}$	$\emptyset$	$\{1\}$
$\mathcal{U}$	$\mathcal{U}$	$\{2\}$	$\{1\}$	$\emptyset$

$\cdot (\cap)$	$\emptyset$	$\{1\}$	$\{2\}$	$\mathcal{U}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$	$\{1\}$
$\{2\}$	$\emptyset$	$\emptyset$	$\{2\}$	$\{2\}$
$\mathcal{U}$	$\emptyset$	$\{1\}$	$\{2\}$	$\mathcal{U}$

Ejemplo 3

Para $R = \{a, b, c, d, e\}$, definimos $+$ y $\cdot$ mediante las siguientes tablas:

$+$	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

$\cdot$	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

Dicha estructura es un anillo. Analizar algunas de las propiedades que la hacen un anillo, identificar el elemento unidad, la identidad para $+$, el inverso aditivo de cada elemento, y si tiene divisores propios de cero.

Sea R un anillo con *elemento unidad* u. Si $a, b \in R$ y $ab = ba = u$, entonces b es un *inverso multiplicativo* de q y a es *una unidad* de R.

Sea R un anillo conmutativo con elemento unidad. Entonces:

1. R es un *dominio de integridad* si R no tiene *divisores propios de cero.*
2. R es un *cuerpo* (o campo) si todo elemento distinto de cero en R es *una unidad.*

Analice si los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ con la suma y producto usuales son dominio de integridad y cuerpos. Lo mismo para los ejemplos 1, 2 y 3 presentados anteriormente.

Ejemplo 4
Sea $R = \{s, t, v, w, x, y\}$. Definimos $+$ y $\cdot$ por medio de las siguientes tablas.

$+$	s	t	v	w	x	y
s	s	t	v	w	x	y
t	t	v	w	x	y	s
v	v	w	x	y	s	t
w	w	x	y	s	t	v
x	x	y	s	t	v	w
y	y	s	t	v	w	x

$\cdot$	s	t	v	w	x	y
s	s	s	s	s	s	s
t	s	t	v	w	x	y
v	s	v	x	s	v	x
w	s	w	s	w	s	w
x	s	x	v	s	x	v
y	s	y	x	w	v	t

Se puede probar que dicha estructura es un anillo. Analizar algunas de las propiedades que la hacen un anillo, y si posee elemento unidad, y en tal caso, hallar las unidades.