ÍNDICE

5. ESTRUCTURAS ALGEBRAICAS **99**
5.1. LEY DE COMPOSICIÓN INTERNA 99
5.1.1. Asociatividad 100
5.1.2. Distributividad 101
5.1.3. Elemento Neutro 102
5.1.4. Conmutatividad 102
5.1.5. Elemento Inverso 102
5.2. ESTRUCTURAS ALGEBRAICAS 105
5.2.1. Grupo 105
5.2.2. Anillo 108
5.2.3. Dominio de Integridad 111
5.2.4. Cuerpo 112
5.3. EJERCICIOS PROPUESTOS 113

CAPÍTULO 5
ESTRUCTURAS ALGEBRAICAS

5.1. LEY DE COMPOSICIÓN INTERNA

Definición 5.1.1. Sea E un conjunto, $*$ se llama "ley de composición interna en E" si y sólo si

$$a * b = c \in E, \ \forall\, a, b \in E.$$

Observación 5.1.1.

1. $*$ también se llama "operación binaria interna en E.
2. Podemos decir que el conjunto E está cerrado para $*$.
3. $*$ es ley de composición interna en E si y sólo si $* : E \times E \to E$ es función.

Ejemplo 5.1.1.

1. *La adición es ley de composición interna en* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.
2. $*$ *definida en* $\mathbb{Z}$ *por* $a * b = a - b + ab$ *es ley de composición interna en* $\mathbb{Z}$.
3. *Si* A *es un conjunto y* $P(A) = \{X \,/\, X \subseteq A\}$ *entonces, la operación* $\cup$ *definida en* $P(A)$ *es ley de composición interna en* $P(A)$.

Proposición 5.1.1. *Sea* $*$ *ley de composición interna en* E *y* $a, b \in E$, *entonces*

a) $a = b \Rightarrow a * c = b * c, \ \forall\, c \in E.$

b) $a = b \Rightarrow c * a = c * b, \ \forall\, c \in E.$

Demostración.

a) $a = b \Rightarrow (a, c) = (b, c) \Rightarrow *(a, c) = *(b, c)$ es decir $a * c = b * c$.

b) Análogo.

□

5.1.1. Asociatividad

Definición 5.1.2. Sea $*$ ley de composición interna en E, decimos que $*$ es asociativa si y sólo si $a * (b * c) = (a * b) * c,\ \forall\, a, b, c \in E$.

Ejemplo 5.1.2.

1. *La adición en $\mathbb{Z}$ es asociativa.*
2. *La multiplicación es asociativa en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.*
3. *$*$ definida en $\mathbb{R}$ por $a * b = a + b + 2ab$ es asociativa ya que*

$$\begin{aligned} a * (b * c) &= a * (b + c + 2bc) \\ &= a + (b + c + 2bc) + 2a(b + c + 2bc) \\ &= a + b + c + 2bc + 2ab + 2ac + 4abc. \end{aligned}$$

Por otro lado

$$\begin{aligned} (a * b) * c &= (a + b + 2ab) * c \\ &= (a + b + 2ab) + c + 2(a + b + 2ab)c \\ &= a + b + 2ab + c + 2ac + 2bc + 4abc \end{aligned}$$

Como $a * (b * c) = (a * b) * c$ entonces $*$ es asociativa.

4. *$*$ definida en $\mathbb{R}$ por $a * b = a + 2b$ no es asociativa ya que, por ejemplo,*

$$\begin{aligned} 2 * (5 * 3) &= 2 * (5 + 2 \cdot 3) \\ &= 2 * (5 + 6) \\ &= 2 * 11 = 2 + 2 \cdot 11 \\ &= 24 \end{aligned}$$

no es igual a

$$\begin{aligned} (2 * 5) * 3 &= (2 + 2 \cdot 5) * 3 \\ &= (2 + 10) * 3 \\ &= 12 * 3 \\ &= 12 + 2 \cdot 3 \\ &= 18. \end{aligned}$$

5. *Si A es un conjunto y $P(A) = \{X \,/\, X \subseteq A\}$ entonces la operación $\cup$, $\cap$ definida en $P(A)$ es asociativa.*

5.1.2. Distributividad

Definición 5.1.3. Sean $*, \nabla$ dos leyes de composición interna en el conjunto E,

a) Se dice que $*$ distribuye por la izquierda sobre ∇ si y sólo si

$$a * (b \nabla c) = (a * b) \nabla (a * c), \ \forall\, a, b, c \in E.$$

b) Se dice que $*$ distribuye por la derecha sobre ∇ si y sólo si

$$(b \nabla c) * a = (b * a) \nabla (c * a), \ \forall\, a, b, c \in E.$$

c) Se dice que $*$ es distributiva sobre ∇ si y sólo si cumple a) y b).

Ejemplo 5.1.3.

1. *La multiplicación es distributiva con respecto de la adición en* $\mathbb{R}$ *ya que*

$$a \cdot (b + c) = a \cdot b + a \cdot c, \ \forall\, a, b, c \in \mathbb{R}$$

y

$$(a + b) \cdot c = a \cdot c + b \cdot c, \ \forall\, a, b, c \in \mathbb{R}.$$

2. *La adición no es distributiva con respecto de la multiplicación en* $\mathbb{R}$ *ya que, por ejemplo,* $2 + (5 \cdot 4) \neq (2 + 5) \cdot (2 + 4)$.

Ejemplo 5.1.4. *Sean* $* : \mathbb{R}^+ \times \mathbb{R}^+ \to \mathbb{R}^+$ *tal que* $a * b = b^a$ *y* $\nabla : \mathbb{R}^+ \times \mathbb{R}^+ \to \mathbb{R}^+$ *tal que* $a \nabla b = a \cdot b$ *dos leyes de composición interna.*

a) Pruebe que $*$ *es distributiva por la izquierda con respecto de* ∇.

b) Pruebe que $*$ *no es distributiva por la derecha con respecto de* ∇.

Solución.

a) Debemos demostrar que $a * (b \nabla c) = (a * b) \nabla (a * c), \ \forall\, a, b, c \in \mathbb{R}^+$,

$$\begin{aligned} a * (b \nabla c) &= a * (b \cdot c) \\ &= (b \cdot c)^a \\ &= b^a \cdot c^a \\ &= (a * b) \nabla (a * c). \end{aligned}$$

b) Como $(a \nabla b) * c = (a \cdot b) * c = c^{a \cdot b}$ y $(a * c) \nabla (b * c) = c^a \nabla c^b = c^{a+b}$ y dado que $c^{a \cdot b} \neq c^{a+b}$ concluimos que $*$ no es distributiva por la derecha con respecto de ∇.

5.1.3. Elemento Neutro

Definición 5.1.4. Sea $*$ ley de composición interna en E, $e \in E$ se llama elemento neutro para $*$ si y sólo si $e * a = a * e = a$, $\forall\, a \in E$.

Ejemplo 5.1.5.

1. $0 \in \mathbb{R}$ *es neutro para la adición en los números reales.*
2. $1 \in \mathbb{R}$ *es neutro para la multiplicación en los números reales.*
3. $\cap : P(X) \times P(X) \to P(X)$ *donde* X *es un conjunto y* $P(X)$ *es el conjunto potencia de* X *tiene neutro* $e = X$ *ya que* $A \cap X = X \cap A = A$, $\forall\, A \in P(X)$.

Proposición 5.1.2. *Sea* $*$ *ley de composición interna en* E *entonces, si existe elemento neutro, éste es único.*

Demostración. Sean e, e_1 dos neutros para $*$, debemos demostrar que $e = e_1$; tenemos, $e * e_1 = e_1$ ya que e es neutro, por otro lado $e * e_1 = e$ ya que e_1 es neutro, así, $e = e_1$. □

5.1.4. Conmutatividad

Definición 5.1.5. Sea $*$ ley de composición interna en E, $*$ es conmutativa en E si y sólo si

$$a * b = b * a,\ \forall\, a, b \in E.$$

Ejemplo 5.1.6.

1. *La adición y la multiplicación son operaciones conmutativas en* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.
2. *La unión y la intersección de conjuntos son operaciones conmutativas en el conjunto potencia del conjunto* A.
3. *La operación* $*$ *definida en* $\mathbb{R}$ *tal que* $a * b = a + 2b$ *no es conmutativa, ya que, por ejemplo,* $3 * 2 = 7 \neq 2 * 3 = 8$.

5.1.5. Elemento Inverso

Definición 5.1.6. Sea $*$ ley de composición interna en E tal que existe elemento neutro $e \in E$ con respecto de $*$; se llama elemento inverso de $a \in E$ con respecto de $*$ al elemento $\bar{a} \in E$ tal que $a * \bar{a} = \bar{a} * a = e$, $\forall\, a \in E$.

Ejemplo 5.1.7. *Considere la operación* $*$ *definida en* $\mathbb{R}$ *por* $a * b = a + b + 2ab$ *tal que es asociativa y con neutro* $e = 0$. *¿Qué elementos* $a \in \mathbb{R}$ *tienen inverso* $\bar{a}$*?.*

Solución. Imponiendo la condición de inverso, se debe cumplir que $a * \bar{a} = e$, así,

$$\begin{aligned} a * \bar{a} = e &\Rightarrow a + \bar{a} + 2a\bar{a} = 0 \\ &\Rightarrow \bar{a}(1 + 2a) = -a \\ &\Rightarrow \bar{a} = \frac{-a}{2a+1} \end{aligned}$$

donde $a \neq -\frac{1}{2}$, por otro lado,

$$\begin{aligned} \bar{a} * a &= \frac{-a}{2a+1} * a \\ &= \frac{-a}{2a+1} + a + 2a\frac{-a}{2a+1} \\ &= a + \frac{-a - 2a\bar{a}}{2a+1} \\ &= 0 \end{aligned}$$

de donde $\forall\, a \in \mathbb{R} - \left\{-\frac{1}{2}\right\}$ existe $\bar{a} \in \mathbb{R}$ tal que $\bar{a} = \frac{-a}{2a+1}$.

Proposición 5.1.3. *Sea $*$ ley de composición interna en E tal que $*$ es asociativa y con elemento neutro e entonces, si $a \in E$ tiene inverso, este es único.*

Demostración. Sean $\overline{x_1}, \overline{x_2}$ dos inversos de x entonces se cumple $\overline{x_1} * x = x * \overline{x_1} = e$ y además $\overline{x_2} * x = x * \overline{x_2} = e$, $\forall\, x \in E$; debemos demostrar que $\overline{x_1} = \overline{x_2}$, veámoslo,

$$\begin{aligned} \overline{x_1} &= \overline{x_1} * e \\ &= \overline{x_1} * (x * \overline{x_2}) \\ &= (\overline{x_1} * x) * \overline{x_2} \\ &= e * \overline{x_2} \\ &= \overline{x_2}. \end{aligned}$$

□

Proposición 5.1.4. *Sea $*$ ley de composición interna en E tal que $*$ es asociativa y con elemento neutro e tal que $a, b \in E$ tienen elemento inverso $\bar{a}, \bar{b}$, entonces,*

a) $\overline{(\bar{a})} = a$.

b) $\overline{(a * b)} = \bar{b} * \bar{a}$.

Demostración.

b) Si demostramos que $c = \bar{b} * \bar{a}$ es tal que $(a * b) * c = e$ y $c * (a * b) = e$, habremos demostrado que c es inverso de $a * b$; veámoslo,

$$\begin{aligned}(a*b)*c &= (a*b)*\left(\bar{b}*\bar{a}\right)\\ &= a*\left[b*\left(\bar{b}*\bar{a}\right)\right]\\ &= a*\left[\left(b*\bar{b}\right)*\bar{a}\right]\\ &= a*\left[e*\bar{a}\right]\\ &= a*\bar{a}\\ &= e.\end{aligned}$$

Análogamente, $c * (a * b) = e$, así, el inverso de $a * b$ es $\bar{b} * \bar{a}$ de donde se cumple

$$\overline{(a*b)} = \bar{b} * \bar{a}.$$

□

Ejemplo 5.1.8. *Considere la operación $*$ definida en $\mathbb{R}$ por $a * b = a + b + 2ab$ tal que es asociativa, con neutro $e = 0$ y $\bar{a} = \frac{-a}{2a+1}$ con $a \neq -\frac{1}{2}$.*

a) Resuelva la ecuación $\overline{(2 * \bar{x})} = 3$.

b) Resuelva la inecuación $\overline{(-2 * \bar{x})} \leq 2$.

Solución. Conviene aplicar la propiedad $\overline{(a * b)} = \bar{b} * \bar{a}$, tenemos,

a)

$$\begin{aligned}\overline{(2*\bar{x})} = 3 &\Rightarrow x*\bar{2} = 3\\ &\Rightarrow x*\frac{-2}{2\cdot 2+1} = 3\\ &\Rightarrow x*-\frac{2}{5} = 3\\ &\Rightarrow x-\frac{2}{5}+2\left(-\frac{2}{5}\right)x = 3\\ &\Rightarrow \frac{1}{5}x = \frac{17}{5}\end{aligned}$$

de donde $x = 17$.

b)

$$\begin{aligned}\overline{(-2*\bar{x})} \leq 2 &\Rightarrow x*\overline{-2} \leq 2\\ &\Rightarrow x*\frac{-(-2)}{2(-2)+1} \leq 2\\ &\Rightarrow x*-\frac{2}{3} \leq 2\\ &\Rightarrow x-\frac{2}{3}+2\left(-\frac{2}{3}\right)x \leq 2\\ &\Rightarrow -\frac{1}{3}x \leq \frac{8}{3}\\ &\Rightarrow x \geq -8.\end{aligned}$$

La solución es $[-8, \infty[- \left\{-\frac{1}{2}\right\}$.

5.2. ESTRUCTURAS ALGEBRAICAS

Cuando dotamos a un conjunto de una o más leyes de composición es que estamos dando a dicho conjunto cierta *estructura*. Una estructura, por consiguiente, queda definida por los axiomas que rigen las relaciones y las operaciones de las que está dotada. En lo que sigue estudiaremos, brevemente, las estructuras fundamentales del álgebra: grupos, anillos, cuerpos y espacios vectoriales.

5.2.1. Grupo

Definición 5.2.1. Un *grupo* es un par $(G, *)$ donde,

1. G es un conjunto.
2. $*$ es ley de composición interna en G tal que,
   a) $a * (b * c) = (a * b) * c, \ \forall\, a, b, c \in G$.
   b) Existe $e \in G$ tal que $a * e = e * a = a, \ \forall\, a \in G$.
   c) Si $a \in G$ entonces existe $\bar{a} \in G$ tal que $a * \bar{a} = \bar{a} * a = e$.

Observación 5.2.1. Decimos que el grupo $(G, *)$ es conmutativo si la operación $*$ es conmutativa.

Ejemplo 5.2.1. *1.* $(Z, +)$ *es grupo conmutativo.*

2. $(\mathbb{R} - \{0\}, \cdot)$ *es un grupo conmutativo.*

3. $(\mathbb{Q}^+, *)$ *tal que* $a * b = \frac{ab}{2}$ *es grupo conmutativo.*

Proposición 5.2.1. *Sea* $(G, *)$ *un grupo entonces,* $a * c = b * c \Leftrightarrow a = b$, $a, b, c \in G$.

Demostración.

$\Rightarrow$) Si $a * c = b * c$ debemos demostrar que $a = b$.

$$\begin{aligned} a * c = b * c &\Rightarrow (a * c) * \bar{c} = (b * c) * \bar{c} \\ &\Rightarrow a * (c * \bar{c}) = b * (c * \bar{c}) \\ &\Rightarrow a * e = b * e \\ &\Rightarrow a = b. \end{aligned}$$

$\Leftarrow$) Propuesto.

□

Proposición 5.2.2. *Sea $(G,*)$ un grupo, $a,b \in G$ entonces, la ecuación $a*x=b$ tiene solución única en G.*

Demostración.

$$\begin{aligned} a*x=b &\Rightarrow \bar{a}*(a*x)=\bar{a}*b \\ &\Rightarrow (\bar{a}*a)*x=\bar{a}*b \\ &\Rightarrow e*x=\bar{a}*b \\ &\Rightarrow x=\bar{a}*b. \end{aligned}$$

Es claro que $\bar{a}*b$ es solución y única. □

Ejemplo 5.2.2.

1. *$(C,+)$ donde $C=\{(a,b)\,/\,a,b\in\mathbb{R}\}$ es el conjunto de los números complejos y la adición esta definida por $(a,b)+(c,d)=(a+c,b+d),\ \forall\,(a,b),(c,d)\in\mathbb{C}$, es un grupo conmutativo.*

2. *$(M(2,\mathbb{R}),+)$ donde $M(2,\mathbb{R})=\{\left(\begin{smallmatrix} a & c \\ b & d\end{smallmatrix}\right)\,/\,a,b,c,d\in\mathbb{R}\}$ es el conjunto de las matrices cuadradas de tamaño 2 en $\mathbb{R}$ y la suma se define por:*

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

es un grupo conmutativo donde

$$\begin{pmatrix} a & c \\ b & d\end{pmatrix}=\begin{pmatrix} e & g \\ f & h\end{pmatrix}\Leftrightarrow (a=e,c=g,b=f,d=h).$$

Ejemplo 5.2.3. *Demuestre que las dos funciones; $f(x)=x$, $g(x)=\frac{1}{x}$, $x\in\mathbb{Q}-\{0\}$, tienen estructura de grupo bajo la composición de funciones.*

Solución. Como

$$\begin{aligned} (f\circ g)(x) &= f\left(g(x)\right)=f\left(\tfrac{1}{x}\right)=\frac{1}{x}=g(x) \\ (g\circ f)(x) &= g\left(f(x)\right)=g(x)=\frac{1}{x}=g(x) \\ (g\circ g)(x) &= g\left(g(x)\right)=g\left(\tfrac{1}{x}\right)=x=f(x) \\ (f\circ f)(x) &= f\left(f(x)\right)=f(x)=x=f(x), \end{aligned}$$

entonces la composición es ley de composición interna en $A=\{f(x),g(x)\}$.

Estos resultados podemos escribirlos es la siguiente tabla de doble entrada

$\circ$	$f(x)$	$g(x)$
$f(x)$	$f(x)$	$g(x)$
$g(x)$	$g(x)$	$f(x)$

Es inmediato que,

El elemento neutro es $e = f(x)$.

El elemento inverso de $f(x)$ es $f(x)$; el elemento inverso de $g(x)$ es $g(x)$.

La asociatividad la puede probar Ud.

Así, $(A, \circ)$ es grupo; además es grupo conmutativo.

Ejemplo 5.2.4. *Sea* $(\mathbb{Z}, *)$ *tal que* $a * b = a + b - 2$, $a, b \in \mathbb{Z}$. *Demuestre que* $(\mathbb{Z}, *)$ *es grupo.*

Solución. Claramente $*$ es ley de composición interna en $\mathbb{Z}$. Debemos demostrar que $*$ es asociativa, posee neutro e inverso en $\mathbb{Z}$.

i)

$$\begin{aligned} a * (b * c) &= a * (b + c - 2) \\ &= a + (b + c - 2) - 2 \\ &= a + b + c - 4. \end{aligned}$$

$$\begin{aligned} (a * b) * c &= (a + b - 2) * c \\ &= (a + b - 2) + c - 2 \\ &= a + b + c - 4. \end{aligned}$$

así, $a * (b * c) = (a * b) * c$, $\forall\, a, b, c \in \mathbb{Z}$.

ii) Debemos probar que existe neutro e tal que $a * e = e * a = a$, $\forall\, a \in \mathbb{Z}$. Imponiendo la condición $a * e = a$ tenemos,

$$a * e = a \Rightarrow a + e - 2 = a \Rightarrow e = 2.$$

Ahora debemos verificar que el neutro opera por la derecha. Tenemos,

$$e * a = 2 * a = 2 + a - 2 = a;$$

así, el neutro es $e = 2$.

iii) Debemos demostrar que, para todo $a \in \mathbb{Z}$ existe $\bar{a} \in \mathbb{Z}$ tal que $\bar{a} * a = a * \bar{a} = 2$. Imponiendo la condición $\bar{a} * a = 2$ tenemos,

$$\bar{a} * a = 2 \Rightarrow \bar{a} + a - 2 = 2 \Rightarrow \bar{a} = 4 - a.$$

Por otro lado, como $a * \bar{a} = a * (4 - a) = a + (4 - a) - 2 = 2$ entonces $\bar{a} = 4 - a$.

Concluimos que $(\mathbb{Z}, *)$ es grupo.

Ejemplo 5.2.5. *Sea $A = \{a, b\}$ y $(A, *)$ un grupo. Demuestre que el grupo es conmutativo.*

Solución. Debemos demostrar que $a * b = b * a$. Como $(A, *)$ es grupo entonces debe poseer neutro e; supongamos que $e = b$ entonces

$$a * b = a * e = a = e * a = b * a.$$

Ejemplo 5.2.6. *Sea $*$ una ley de composición interna definida en $\mathbb{Q} \times \mathbb{Q}$ tal que $(a, b) * (c, d) = (ac, bc + d)$. Se sabe que $(A, *)$ es grupo donde $A = \{(1, x) \,/\, x \in \mathbb{Q}\}$; determine el neutro e en A.*

Solución. Sea $e = (1, p) \in A$ tal elemento neutro; imponiendo la condición de neutro debe cumplir, $(1, x) * (1, p) = (1, p) * (1, x) = (1, x)$, $\forall\, (1, x) \in A \times A$.

De $(1, x) * (1, p) = (1, x)$ tenemos $(1, x + p) = (1, x)$, de aquí concluimos $x + p = x$, de donde $p = 0$, así, el neutro lateral derecho es $e = (1, 0)$.

Ahora debemos verificar que es neutro lateral izquierdo, tenemos, $e * (1, x) = (1, 0) * (1, x) = (1, 0 + x) = (1, x)$, $\forall\, (1, x) \in A$, luego, $e = (1, 0)$.

Ejemplo 5.2.7. *Sea $\{x, y\} \subseteq \mathbb{Z}_3$. Pruebe que $(x + y)^3 = x^3 + y^3$.*

Solución.

$$\begin{aligned} (x+y)^3 &= (x+y)(x+y)(x+y) \\ &= x^3 + 3x^2y + 3xy^2 + x^3 \\ &= x^3 + y^3, \end{aligned}$$

ya que $3 \equiv 0 (\text{mod } 3)$.

5.2.2. Anillo

Definición 5.2.2. El trío $(A, +, \cdot)$ se llama anillo si y sólo si

a) $(A, +)$ es grupo conmutativo.

b) $\cdot$ es ley de composición interna en A.

c) $\cdot$ es asociativa.

d) $\cdot$ es distributiva con respecto de $+$.

Definición 5.2.3. Sea $(A, +, \cdot)$ un anillo, entonces,

a) $(A, +, \cdot)$ es conmutativo si y sólo si $\cdot$ es conmutativa.

b) $(A, +, \cdot)$ es un Anillo con unidad si y sólo si existe elemento neutro para $\cdot$.

Ejemplo 5.2.8.

1. $(Z, +, \cdot)$ *es anillo.*
2. $(E, +, \cdot)$ *es anillo, donde* $E = \{x \in \mathbb{Z} \,/\, x$ *es un número par*$\}$.
3. $(Z, +, \otimes)$ *donde* $a \otimes b = 2ab$ *es anillo.*
4. $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ *tal que* $(a, b) + (c, d) = (a + c, b + d)$ *y* $(a, b) \cdot (c, d) = (ac, bd)$ *es anillo.*
5. $(C, +, \cdot)$ *tal que* $C = \mathbb{R} \times \mathbb{R}$, $(a, b) + (c, d) = (a + c, b + d)$, $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$ *es un anillo.*
6. $(\mathbb{Z}_4, +, \cdot)$ *es anillo.*
7. $(M(2, \mathbb{R}), +, \cdot)$ *es anillo donde*

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} x & z \\ y & w \end{pmatrix} = \begin{pmatrix} ax + cy & az + cw \\ bx + dy & bz + dw \end{pmatrix}.$$

Proposición 5.2.3. *Sea* $(A, +, \cdot)$ *un anillo con neutro aditivo 0 e inverso aditivo de a el elemento* $-a$. *Se cumple,*

a) $a \cdot 0 = 0 \cdot a = 0, \ \forall\, a \in A$.

b) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b), \ \forall\, a, b \in A$.

Demostración.

a)

$$\begin{aligned} a \cdot 0 = 0 + a \cdot 0 &= [-(a \cdot a) + (a \cdot a)] + a \cdot 0 \\ &= -(a \cdot a) + [a \cdot a + a \cdot 0] \\ &= -(a \cdot a) + a(a + 0) \\ &= -(a \cdot a) + a \cdot a \\ &= 0. \end{aligned}$$

Análogamente se demuestra que $0 \cdot a = 0$.

b) Demostraremos que $(-a) \cdot b$ y $-(a \cdot b)$ son inversos aditivos de $a \cdot b$, entonces, por la unicidad del inverso concluiremos que

$$\begin{aligned} (-a) \cdot b &= -(a \cdot b) \\ &= (-a) \cdot b + a \cdot b \\ &= (-a + a) \cdot b \\ &= 0 \cdot b \\ &= 0, \end{aligned}$$

así, $(-a) \cdot b$ es inverso aditivo de $a \cdot b$.

Por otro lado, es inmediato que $-(a \cdot b)$ es inverso aditivo de $a \cdot b$. De manera análoga se demuestra que $a \cdot (-b) = -(a \cdot b)$.

□

Corolario 5.2.1. *Si $(A, +, \cdot)$ es un anillo entonces $a \cdot b \neq 0 \Rightarrow a \neq 0 \wedge b \neq 0$, $\forall\, a, b \in A$.*

En efecto, usando la contrapositiva y la parte a) de la proposición anterior tenemos, $(a = 0 \vee b = 0) \Rightarrow a \cdot b = 0$.

Observación 5.2.2. El recíproco del corolario no se cumple, ya que, por ejemplo

a) En el anillo $(M(2, \mathbb{R}), +, \cdot)$ se tiene

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

1. En el anillo $(\mathbb{Z}_4, +, \cdot)$ se tiene $\bar{2} \cdot \bar{2} = \bar{0}$.

Definición 5.2.4. Un anillo conmutativo es un triple $(A, +, \cdot)$ tal que

a) $(A, +, \cdot)$ es anillo.

b) $\cdot$ es conmutativa.

Ejemplo 5.2.9.

1. *$(Z, +, \cdot)$ es anillo conmutativo.*
2. *El anillo $(M(2, \mathbb{R}), +, \cdot)$ no es conmutativo.*
3. *En general $(\mathbb{Z}_m, +, \cdot)$ es anillo conmutativo.*
4. *El anillo $(M(2, \mathbb{R}), +, \cdot)$ no es conmutativo ya que por ejemplo,*

$$\begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 5 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 1 & 0 \end{pmatrix}.$$

Definición 5.2.5. Un anillo con identidad es un triple $(A, +, \cdot)$ tal que

a) $(A, +, \cdot)$ es anillo.

b) Existe $1 \in A$ tal que $1 \cdot a = a \cdot 1 = a$, $\forall\, a \in A$.

Ejemplo 5.2.10.

1. *$(\mathbb{Z}, +, \cdot)$ es anillo con unidad.*

2. $(M(2,\mathbb{R}),+,\cdot)$ *es anillo con* $1=\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$.

3. $(\mathbb{R}\times\mathbb{R},+,*)$ *tal que* $(a,b)+(c,d)=(a+c,b+d)$ *y* $(a,b)*(c,d)=(ac,bd)$ *es anillo con unidad* $1=(1,1)$.

4. $(C,+,\cdot)$ *tal que* $C=\mathbb{R}\times\mathbb{R}$, $(a,b)+(c,d)=(a+c,b+d)$, $(a,b)*(c,d)=(ac-bd,ad+bc)$ *es un anillo con unidad* $1=(1,0)$.

5. $(\mathbb{Z}_4,+,\cdot)$ *es anillo conmutativo con unidad.*

5.2.3. Dominio de Integridad

Una de las formas para solucionar una ecuación de segundo grado es factorizar, allí usamos la proposición $(a\cdot b=0)\Leftrightarrow(a=0\vee b=0)$, sin embargo existen algunos conjuntos donde esto no ocurre, por ejemplo, en $\mathbb{Z}_4$ tenemos $\bar{2}\cdot\bar{2}=\bar{0}$.

Definición 5.2.6. Sea $(A,+,\cdot)$ un anillo. Si $a,b\in A$ son no nulos tal que $a\cdot b=0$ con 0 el neutro para + entonces, a y b se llaman *divisores del cero.*

Ejemplo 5.2.11.

1. $(\mathbb{Z}_6,+,\cdot)$ *es anillo con divisores del cero.*

2. $(M(2,\mathbb{R}),+,\cdot)$ *es anillo con divisores del cero.*

Teorema 5.2.1. *Un anillo* $(A,+,\cdot)$ *no tiene divisores del cero si y sólo si es válida la ley de cancelación para la multiplicación.*

Demostración.

$\Rightarrow$) Sea $(A,+,\cdot)$ un anillo sin divisores del cero y $a,b,c\in A$ tal que $c\neq 0$, debemos demostrar que si $a\cdot c=b\cdot c$ entonces $a=b$, veámoslo,

$$a\cdot c=b\cdot c\Rightarrow a\cdot c-b\cdot c=0\Rightarrow(a-b)\cdot c=0;$$

como $(A,+,\cdot)$ es un anillo sin divisores del cero y $c\neq 0$ entonces $a-b=0$, de donde, $a=b$.

$\Leftarrow$) Supongamos que se cumple la cancelación para la multiplicación, debemos demostrar que $a\cdot b=0\Rightarrow(a=0\vee b=0)$. Si $a\neq 0$ entonces

$$a\cdot b=0\Rightarrow a\cdot b=a\cdot 0$$

de donde $b=0$.

□

Definición 5.2.7. Un *dominio de integridad* es un triple $(A,+,\cdot)$ tal que

a) $(A,+,\cdot)$ es anillo conmutativo con identidad.

b) $(a \neq 0 \wedge b \neq 0) \Rightarrow a \cdot b \neq 0)$ donde el neutro para $+$ es 0.

Observación 5.2.3. Sea $(A, +, \cdot)$ un dominio de integridad, entonces,

a) $(a \cdot c = b \cdot c) \Rightarrow a = b,\ \forall\, a, b, c \in A,\ c \neq 0.$

b) La ecuación $a \cdot x = b$, $a \neq 0$ tiene solución única.

c) $a \cdot b = 0 \Rightarrow (a = 0 \vee b = 0)$.

Ejemplo 5.2.12.

1. $(\mathbb{Z}_5, +, \cdot)$ *es dominio de integridad.*
2. $(C, +, \cdot)$ *tal que* $C = \mathbb{R}\times\mathbb{R}$, $(a, b)+(c, d) = (a+c, b+d)$, $(a, b)\cdot(c, d) = (ac-bd, ad+bc)$ *es dominio de integridad.*

Observación 5.2.4. En el anillo $(\mathbb{Z}_4, +, \cdot)$, la ecuación $2 \cdot x = 0$ tiene dos soluciones, naturalmente que nos interesa una estructura tal que una ecuación del tipo $a \cdot x = b$ tenga solución única; en la estructura de *cuerpo* una ecuación del tipo $a \cdot x = b$ tiene solución y es única.

5.2.4. Cuerpo

Definición 5.2.8. El triple $(A, +, \cdot)$ es un *cuerpo* si y sólo si

a) $(A, +, \cdot)$ es anillo conmutativo con unidad 1.

b) $\forall\, a \in A - \{0\}\ \exists\, a^{-1} \in A$ tal que $a \cdot a^{-1} = 1$.

Ejemplo 5.2.13.

1. $(\mathbb{Z}_3, +, \cdot)$ *es cuerpo.*
2. $(C, +, \cdot)$ *tal que* $C = \mathbb{R}\times\mathbb{R}$; $(a, b)+(c, d) = (a+c, b+d)$, $(a, b)*(c, d) = (ac-bd, ad+bc)$ *es cuerpo donde* $(a, b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$.

Observación 5.2.5.

a) Si $(A, +, \cdot)$ es un cuerpo entonces $(A, +, \cdot)$ es dominio de integridad; en efecto, sólo falta demostrar que $(a \neq 0 \wedge b \neq 0) \Rightarrow a \cdot b \neq 0$; lo demostraremos usando la contrapositiva $(a \cdot b = 0) \Rightarrow (a = 0 \vee b = 0)$.

   Supongamos que $a \cdot b = 0$ y que $b \neq 0$, entonces $(a \cdot b) \cdot b^{-1} = 0 \cdot b^{-1}$, de aquí deducimos que $a = 0$, lo que constituye una contradicción.

1. El recíproco no es cierto, es decir, $(A, +, \cdot)$ dominio de integridad no implica que $(A, +, \cdot)$ sea un cuerpo, ya que, por ejemplo, $(Z, +, \cdot)$ es dominio de integridad y sin embargo no es un cuerpo.

5.3. EJERCICIOS PROPUESTOS

Ejercicio 5.1. Decida si las siguientes operaciones son o no ley de composición interna en el conjunto declarado.

a) $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ tal que $a * b = ab + 2$.

b) $*$ definida en $\mathbb{Z} - \{0\}$ tal que $x * y = \frac{x}{y} + 2$.

c) $\circ$ definida en $\mathbb{Z}$ tal que $a \circ b = (a + b)^2$.

d) $*$ definida en $\mathbb{Z}$ tal que $a * b = \frac{a+b-2}{3}$.

e) $*$ definida en $\mathbb{Q}$ tal que $a * b = \frac{a+b-2}{3}$.

f) La multiplicación usual definida en $A = \{1, 0, 2\}$; $B = \{0, 1\}$; $C = \{2, 4, 6, \ldots\}$.

g) $\cup : P(A) \times P(A) \to P(A)$ donde A es un conjunto y $P(A)$ es la potencia de A.

Ejercicio 5.2. Sea $*$ ley de composición interna definida en el conjunto E, demuestre que

a) $(a = b) \Rightarrow a * c = b * c$, $\forall\, a, b, c \in E$.

b) $(a = b) \Rightarrow c * a = c * b$, $\forall\, a, b, c \in E$.

Ejercicio 5.3. Decida cuáles de las siguientes "leyes de composición internas" son asociativas.

a) $*$ definida en $\mathbb{R}$ tal que $a * b = a + b + ab$.

b) $*$ definida en $\mathbb{R}$ tal que $a * b = a + 2b$.

c) La unión de conjuntos, $\cup : P(A) \times P(A) \to P(A)$.

Ejercicio 5.4. Decida cuáles de las siguientes "leyes de composición internas" tienen neutro e para la operación binaria interna definida.

a) $\cap : P(A) \times P(A) \to P(A)$ tal que $(P, R) \to P \cap R$, donde A es un conjunto y $P(A)$ es la potencia de A.

b) $*$ definida en $\mathbb{Q}^+$ tal que $a * b = \frac{ab}{2}$.

c) $*$ definida en $\mathbb{R}$ tal que $a * b = a + b + 1$.

d) $*$ definida en $\mathbb{R}$ tal que $x * y = xy + x$.

Ejercicio 5.5. Sea $*$ una ley de composición interna en el conjunto E. Demuestre que, si existe elemento neutro para $*$, éste elemento es único.

Ejercicio 5.6. Decida cuales de las siguientes "leyes de composición internas" son conmutativas para la operación binaria interna definida.

a) $*$ definida en $\mathbb{R}$ tal que $a * b = a + b + 3ab$.

b) $*$ definida en $\mathbb{R}$ tal que $a * b = a - b + 2ab$.

Ejercicio 5.7. Determine la tabla de multiplicar para $*$ definida en el conjunto $E = \{1, 2, 3, 4\}$ tal que $a * b = \text{máx}\{a, b\}$.

Ejercicio 5.8. Sea $*$ ley de composición interna definida en el conjunto E tal que la operación es asociativa y tiene neutro e. Demuestre que, si $x \in E$ tiene inverso $\bar{x}$ entonces éste es único.

Ejercicio 5.9. En T se define la ley de composición interna $*$ por $a * b = a + b - ab$. Estudie la asociatividad, conmutatividad, elemento neutro y elemento inverso.

Ejercicio 5.10. En $\mathbb{Z}$ se define la operación binaria interna $*$ tal que $a * b = a + b^2$. Estudie la asociatividad, conmutatividad, elemento neutro y elemento inverso.

Ejercicio 5.11. En $\mathbb{Q} \times \mathbb{Q}$ se define $\oplus$ por $(a, b) \oplus (c, d) = (ac, ad + b)$. Estudie la asociatividad, conmutatividad, elemento neutro y elemento inverso.

Ejercicio 5.12. En el conjunto $S = \{a, b, c\}$ se define $*$ por la siguiente tabla,

$*$	a	b	c
a	a	b	c
b	b	a	c
c	c	c	c

Estudie la asociatividad, conmutatividad, elemento neutro y elemento inverso.

Ejercicio 5.13. En $\mathbb{Z}$ se definen las operaciones binarias internas $*$ y $\circ$ por $a*b = a+b+1$ y $a \circ b = a + b + ab$.

a) ¿Es el par $(\mathbb{Z}, *)$ un grupo?.

b) ¿Es el par $(\mathbb{Z}, \circ)$ un grupo?.

c) ¿Es $*$ distributiva con respecto de $\circ$?.

d) ¿ Es $\circ$ distributiva con respecto de $*$?.

Ejercicio 5.14. Sea $A = \{a, b\}$ y $(A, *)$ un grupo. Demuestre que el grupo es conmutativo.

Ejercicio 5.15. Sea $(G, *)$ un grupo, demuestre que,

a) $a * c = b * c \Leftrightarrow a = b,\ \forall\, a, b, c \in G$.

b) La ecuación $a * x = b$ tiene solución única en G.

Ejercicio 5.16. Demuestre que $(C, +)$ es un grupo si $C = \{(x, y) \,/\, x, y \in \mathbb{R}\}$ es el conjunto de los números complejos donde $(a, b) + (c, d) = (a + c, b + d)$.

Ejercicio 5.17. Demuestre que $(M(2, \mathbb{R}), +)$ donde $M(2, \mathbb{R}) = \{\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \,/\, a, b, c, d \in \mathbb{R}\}$ es el conjunto de las matrices cuadradas de tamaño 2 en $\mathbb{R}$ y

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

es un grupo, donde $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} e & g \\ f & h \end{smallmatrix}\right)$ si y sólo si $a = e$, $b = f$, $c = g$, $d = h$.

Ejercicio 5.18. En $\mathbb{R}^+$ definimos las operaciones binarias internas $*$ y $\circ$ tal que $a * b = b^a$ y $a \circ b = ab$. Demuestre que $*$ distribuye por la izquierda a $\circ$ pero que no lo hace por la derecha.

Ejercicio 5.19. Demuestre que el par $(\mathbb{R} - \{-1\}, *)$ es un grupo donde $a * b = a + b + ab$. Resuelva la ecuación $2 * x * 6 = 18$.

Ejercicio 5.20. Demuestre que el trío $(Z, +, \otimes)$ es un anillo donde $+$ es la suma usual y $a \oplus b = 2ab$.

Ejercicio 5.21. Demuestre que el trío $(M(2, \mathbb{R}), +, \cdot)$ con las características dadas en el Ejercicio 5.17 y

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} e & g \\ f & h \end{pmatrix} = \begin{pmatrix} ae + cf & ag + ch \\ be + df & bg + dh \end{pmatrix}$$

es un anillo.

Ejercicio 5.22. Demuestre que el trío $(C, +, \cdot)$ con las características del Ejercicio 5.16 y donde $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$ es un anillo.

Ejercicio 5.23. Demuestre que $(\mathbb{Z}_4, +, \cdot)$ es un anillo.

Ejercicio 5.24. Sea $(A, +, \cdot)$ un anillo con neutro aditivo 0 y opuesto aditivo de $a \in A$ el elemento $-a$. Demuestre que,

a) $a \cdot 0 = 0 \cdot a = 0, \ \forall\, a \in A.$

b) $(-a)b = a(-b) = -(ab), \ \forall\, a, b \in A.$

Ejercicio 5.25. ¿Los anillos de los Ejercicios 5.21 y 5.22 son dominio de integridad?.

Ejercicio 5.26. Demuestre que, un anillo $(A, +, \cdot)$ no tiene divisores del cero si y sólo si es valida la ley de cancelación para la multiplicación.