Contents

2. Operaciones y estructuras algebraicas.

Dado un conjunto A, llamamos operación binaria interna o ley de composición interna a cualquier función de $A \times A$ en A.

$$* : A \times A \to A \qquad *(a,b) = c \qquad a * b = c$$

Ejemplo 1 *Consideremos, en* $\mathbb{Z}_m = \mathbb{Z}/_{\equiv_{(mod\ m)}}$, *las operaciones definidas como:*

$$\begin{aligned} &+ : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m && \cdot : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m \\ &[a] + [b] = [a+b] && [a] \cdot [b] = [a \cdot b] \end{aligned}$$

Por ejemplo, para $m = 2$, $\mathbb{Z}_2 = \{[0],[1]\}$ *y la suma y el producto vienen representados en las siguientes tablas*

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

Recuerda que $[0]$ *y* $[1]$ *son conjuntos.*

Por ejemplo, para $m = 4$, $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ *y la suma y el producto vienen representados en las siguientes tablas*

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

y, para $m = 5$*, la suma y el producto vienen representados en las siguientes tablas*

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[3]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

Por ejemplo, para $m = 4$, $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ *y la suma y el producto vienen representados en las siguientes tablas*

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

y, para $m = 5$, *la suma y el producto vienen representados en las siguientes tablas*

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[3]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

¿Es cierto que $\mathbb{Z}_4 \subseteq \mathbb{Z}_5$*?*

2.1. Propiedades

Asociativa

Sea $*$ una operación interna en A. Decimos que $*$ tiene propiedad asociativa si satisface:

$$\text{Para todo } a, b, c \in A, \qquad a * (b * c) = (a * b) * c$$

Ejemplo 2 *En* $\mathbb{R}$

- *La suma y el producto tienen propiedad asociativa.*
- *La diferencia y la división, por el contrario, no.*

En $\wp(U)$

- *La unión y la intersección tienen propiedad asociativa.*
- *La diferencia y la diferencia simétrica, por el contrario, no.*

Conmutativa

Sea $*$ una operación interna en A. Decimos que $*$ tiene propiedad conmutativa si satisface:

$$\text{Para todo } a, b \in A, \qquad a * b = b * a$$

Ejemplo 3 *Las siguientes operaciones tienen propiedad conmutativa:*

- *La suma y el producto en* $\mathbb{Z}_m$ *(ejemplo 1)*
- *La unión, intersección y diferencia simétrica de conjuntos.*
- *La suma de matrices.*

Las siguientes operaciones no tienen propiedad conmutativa:

- *La diferencia de conjuntos.*
- *El producto de matrices.*
- *La composición de funciones.*

Distributiva

Sean $*$ y Δ dos operaciones internas en A.
Decimos que Δ es distributiva por la izda. respecto de $*$ si satisface:

$$\text{Para todo } a, b, c \in A, \qquad a\Delta(b * c) = (a\Delta b) * (a\Delta c)$$

Decimos que Δ es distributiva por la dcha. respecto de $*$ si satisface:

$$\text{Para todo } a, b, c \in A, \qquad (b * c)\Delta a = (b\Delta a) * (c\Delta a)$$

Decimos que Δ es distributiva respecto de $*$ si lo es por la izda. y por la dcha.

Proposición 4 *Sean $*$ y Δ operaciones internas en A y $X \subseteq A$ una parte estable para $*$ y Δ. Si Δ es distributiva respecto de $*$ en A, también lo es en X.*

Ejemplo 5

- *En $\mathbb{R}$, el producto es distributivo respecto de la suma.*
- *En $\mathbb{R}$, la suma no es distributiva respecto del producto.*
- *En $\mathbb{R}$, la división es distributiva por la dcha. respecto de la suma.*
- *En $\mathbb{R}$, la división no es distributiva por la izda. respecto de la suma.*
- *En $\wp(U)$, la unión es distributiva respecto de la intersección.*
- *En $\wp(U)$, la intersección es distributiva respecto de la unión.*

2.2. Elementos Particulares

Elemento Neutro

Un elemento $e \in A$ es neutro para $*$ si satisface que

$$\text{Para todo } a \in A, \quad a * e = e * a = a$$

Ejemplo 6

- 0 *es elemento neutro para la suma en* $\mathbb{R}$. *(*$a + 0 = a$ *para todo* $a \in \mathbb{R}$*)*
- 1 *es elemento neutro para el producto en* $\mathbb{R}$. *(*$a \cdot 1 = a$ *para todo* $a \in \mathbb{R}$*)*
- 1 *es elemento neutro para la división en* $\mathbb{R}$. *(*$a/1 = a$ *para todo* $a \in \mathbb{R}$*)*

2.2. Elementos Particulares

Elemento Neutro

Un elemento $e \in A$ es neutro para $*$ si satisface que

$$\text{Para todo } a \in A, \quad a * e = e * a = a$$

Ejemplo 6 • 0 *es elemento neutro para la suma en* $\mathbb{R}$. *(*$a + 0 = a$ *para todo* $a \in \mathbb{R}$*)*

- 1 *es elemento neutro para el producto en* $\mathbb{R}$. *(*$a \cdot 1 = a$ *para todo* $a \in \mathbb{R}$*)*
- 1 *es elemento neutro para la división en* $\mathbb{R}$. *(*$a/1 = a$ *para todo* $a \in \mathbb{R}$*)*
  Ojo: no es cierto ya que no podemos asegurar que $1/a = a$ *para todo* $a \in \mathbb{R}$
- $\varnothing$ *es elemento neutro para la unión de conjuntos en* $\wp(U)$.
- U *es elemento neutro para la intersección de conjuntos en* $\wp(U)$.

Proposición 7 *El elemento neutro, si existe, es único.*

Simétrico de un elemento

Sea $*$ una operación interna en A y $e \in A$ el elemento neutro. Decimos que b es simétrico de a si satisface que

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

Si un elemento tiene simétrico decimos que es simetrizable.

Proposición 8 *Sea $*$ una operación interna con propiedad asociativa. Si un elemento es simetrizable, su simétrico es único.*

Ejemplo 9 *La siguiente operación no tiene propiedad asociativa:*

$*$	1	2	3	4
1	1	2	3	4
2	2	3	4	1
3	3	4	1	1
4	4	1	1	3

En adelante, si $*$ tiene propiedad asociativa y a es simetrizable, denotaremos por a' al único simétrico de a.

Proposición 10 *Sea $*$ una operación interna con elemento neutro. Si b es simétrico de a entonces a es simétrico de b. En particular, si $*$ tiene propiedad asociativa, $(a')' = a$*

Proposición 11 *Sea $*$ una operación interna en A con propiedad asociativa y $a \in A$ un elemento simetrizable. Las siguientes ecuaciones tienen solución única:*

$$a * x = b \qquad\qquad x * a = b$$

Proposición 12 *Sea $*$ una operación interna en A con propiedad asociativa. Si $a, b \in A$ son elementos simetrizables, $a * b$ también lo es y*

$$(a * b)' = b' * a'$$

Elementos simplificables o regulares

Sea $*$ una operación interna en A y $c \in A$. Decimos que:

- c es regular por la izda. si para todo $a, b \in A$,

$$c * a = c * b \text{ implica que } a = b$$

- c es regular por la dcha. si para todo $a, b \in A$,

$$a * c = b * c \text{ implica que } a = b$$

Decimos que c es regular si lo es por la izda. y por la dcha. Si todos los elementos de A son regulares, decimos que $*$ satisface la ley de simplificación.

Proposición 13 *Si $*$ una operación interna en A con propiedad asociativa, todo elemento simetrizable es regular.*

Elementos absorbentes

Sea $*$ una operación interna en A y $c \in A$. Decimos que c es absorbente si, para todo $a \in A$, se satisface que:

$$a * c = c * a = c$$

Ejemplo 14

- *0 es elemento absorbente para el producto en $\mathbb{R}$.*
- *$\varnothing$ es elemento absorbente para la intersección en $\wp(U)$.*
- *U es elemento absorbente para la unión en $\wp(U)$.*

2.3. Semigrupos y Grupos

$(A, *)$ es semigrupo si satisface:

$*$ es una operación interna en A
P. Asociativa
P. Conmutativa (Opcional "Abeliano")
E. Neutro (Opcional "con Elemento Neutro")

$(A, *)$ es grupo si satisface:

$*$ es una operación interna en A
P. Asociativa
P. Conmutativa (Opcional "Abeliano")
E. Neutro
Todos los elementos simetrizables

Sea $A \neq \varnothing$. Decimos que $(A, *)$ es un grupo si satisface las siguientes condiciones:

- $*$ es una operación binaria interna en A.
- $*$ satisface la propiedad asociativa.
- Tiene elemento neutro.
- Todo elemento tiene simétrico.

Si, además, $*$ tiene propiedad conmutativa decimos que es grupo abeliano.

Proposición 15 *Sea $(G, *)$ un grupo.*

1. *El elemento neutro es único.*
2. *Cualquier elemento tiene un único simétrico.*
3. $(a')' = a$
4. *Para todo $a, b \in G$, $(a * b)' = b' * a'$.*
5. *Todos los elementos son regulares.*
6. *Las ecuaciones $a * x = b$ y $x * a = b$ tienen solución única.*

2.4. Anillos y cuerpos

$(A, *, \Delta)$ es anillo si satisface:

$*$ es una operación interna en A	Δ es una operación interna en A
P. Asociativa P. Conmutativa E. Neutro Todos los elementos simetrizables	P. Asociativa P. Conmutativa (Op. "conmutativo") E. Neutro (Op. "con E. Unidad")
Δ distributiva respecto de $*$	

$(A, *, \Delta)$ es un anillo si

- $(A, *)$ es grupo abeliano.
- (A, Δ) es semigrupo.
- Δ es distributiva respecto de $*$.

Si $(A, *, \Delta)$ es un anillo, para $*$ usaremos notación aditiva y para Δ notación multiplicativa.

Teorema 16 (Regla de los Signos) *Sea* $(A, +, \cdot)$ *un anillo. Para todo* $a, b \in A$ *se cumple*

i. $0a = a0 = 0$

ii. $a(-b) = (-a)b = -(ab)$

iii. $ab = (-a)(-b)$

Ejemplo 17 $(\mathbb{Z}_5, +, \cdot)$ *es un anillo conmutativo con elemento unidad.*

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

Ejemplo 18 $(\mathbb{Z}_6, +, \cdot)$ *es un anillo conmutativo con elemento unidad.*

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[2]$	$[0]$	$[2]$	$[4]$	$[0]$	$[2]$	$[4]$
$[3]$	$[0]$	$[3]$	$[0]$	$[3]$	$[4]$	$[3]$
$[4]$	$[0]$	$[4]$	$[2]$	$[4]$	$[4]$	$[2]$
$[5]$	$[0]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

Un elemento $a \in A \setminus \{0\}$ es divisor de cero si:

existe $b \in A \setminus \{0\}$ tal que $ab = 0$ o $ba = 0$

Proposición 19 *Sea* $(A, +, \cdot)$ *un anillo y* $a \in A$. a *es regular si y solo si no es* 0 *ni divisor de cero.*

2.4.1. Cuerpos

$(A, *, \Delta)$ es cuerpo si satisface:

$*$ es una operación interna en A	Δ es una operación interna en A
P. Asociativa P. Conmutativa E. Neutro (cero) Todos los el. simetrizables	P. Asociativa P. Conmutativa E. Neutro Todos los el. simetrizables salvo el cero
Δ distributiva respecto de $*$	

$(K, +, \cdot)$ es un cuerpo si

- $(K, +)$ es grupo abeliano.
- $(K \setminus \{0\}, \cdot)$ es grupo.
- $\cdot$ es distributiva respecto de $+$.

Proposición 20 *Sea $(K, +, \cdot)$ un cuerpo.*

1. *No tiene divisores de cero.*
2. *Las ecuaciones $ax = b$ y $xa = b$ con $a \neq 0$ tienen solución única.*