MATEMÁTICA DISCRETA
Estructuras Algebraicas

Prof. Sergio Salinas

Facultad de Ingeniería
Universidad Nacional de Cuyo

Segundo semestre 2024

Contenido

Introducción al álgebra abstracta

Operaciones binarias

Suma, resta, multiplicación y división son ejemplos de operaciones binarias sobre conjuntos de números.

Operaciones binarias

Suma, resta, multiplicación y división son ejemplos de operaciones binarias sobre conjuntos de números.

Definición

Una operación binaria en un conjunto A es una función $f : A \times A \to A$ donde se cumplen las siguientes propiedades:

Operaciones binarias

Suma, resta, multiplicación y división son ejemplos de operaciones binarias sobre conjuntos de números.

Definición

Una operación binaria en un conjunto A es una función $f : A \times A \to A$ donde se cumplen las siguientes propiedades:
i) f asigna un elemento $f(a, b)$ de A a cada par ordenado (a, b) de elementos de A (cerrada),

Operaciones binarias

Suma, resta, multiplicación y división son ejemplos de operaciones binarias sobre conjuntos de números.

Definición

Una operación binaria en un conjunto A es una función $f : A \times A \to A$ donde se cumplen las siguientes propiedades:
i) f asigna un elemento $f(a, b)$ de A a cada par ordenado (a, b) de elementos de A (cerrada),
ii) sólo un elemento de A se asigna a cada par ordenado (a, b).

Operaciones binarias

En cada caso determinar si se trata de una operación binaria:

1. Sea $A = \mathbb{Z}$ se define $a * b$ como $a + b$.

Operaciones binarias

En cada caso determinar si se trata de una operación binaria:

1. Sea $A = \mathbb{Z}$ se define $a * b$ como $a + b$. ✓

Operaciones binarias

En cada caso determinar si se trata de una operación binaria:

1. Sea $A = \mathbb{Z}$ se define $a * b$ como $a + b$. ✓
2. Sea $A = \mathbb{R}$ se define $a * b$ como $\frac{a}{b}$.

Operaciones binarias

En cada caso determinar si se trata de una operación binaria:

1. Sea $A = \mathbb{Z}$ se define $a * b$ como $a + b$. ✓
2. Sea $A = \mathbb{R}$ se define $a * b$ como $\frac{a}{b}$. ✗

Operaciones binarias

En cada caso determinar si se trata de una operación binaria:

1. Sea $A = \mathbb{Z}$ se define $a * b$ como $a + b$. ✓
2. Sea $A = \mathbb{R}$ se define $a * b$ como $\frac{a}{b}$. ✗
3. Sea $A = \mathbb{Z}^+$ se define $a * b$ como $a - b$.

Operaciones binarias

En cada caso determinar si se trata de una operación binaria:

1. Sea $A = \mathbb{Z}$ se define $a * b$ como $a + b$. ✓
2. Sea $A = \mathbb{R}$ se define $a * b$ como $\frac{a}{b}$. ✗
3. Sea $A = \mathbb{Z}^+$ se define $a * b$ como $a - b$. ✗

Operaciones binarias

En cada caso determinar si se trata de una operación binaria:

1. Sea $A = \mathbb{Z}$ se define $a * b$ como $a + b$. ✓
2. Sea $A = \mathbb{R}$ se define $a * b$ como $\frac{a}{b}$. ✗
3. Sea $A = \mathbb{Z}^+$ se define $a * b$ como $a - b$. ✗
4. Sea $A = \mathbb{Z}$ se define $a * b$ un número menor que a y b.

Operaciones binarias

En cada caso determinar si se trata de una operación binaria:

1. Sea $A = \mathbb{Z}$ se define $a * b$ como $a + b$. ✓
2. Sea $A = \mathbb{R}$ se define $a * b$ como $\frac{a}{b}$. ✗
3. Sea $A = \mathbb{Z}^+$ se define $a * b$ como $a - b$. ✗
4. Sea $A = \mathbb{Z}$ se define $a * b$ un número menor que a y b. ✗

Operaciones binarias

En cada caso determinar si se trata de una operación binaria:

1. Sea $A = \mathbb{Z}$ se define $a * b$ como $a + b$. ✓
2. Sea $A = \mathbb{R}$ se define $a * b$ como $\frac{a}{b}$. ✗
3. Sea $A = \mathbb{Z}^+$ se define $a * b$ como $a - b$. ✗
4. Sea $A = \mathbb{Z}$ se define $a * b$ un número menor que a y b. ✗
5. Sea $A = \mathbb{R}$ se define $a * b =$máximo(a, b).

Operaciones binarias

En cada caso determinar si se trata de una operación binaria:

1. Sea $A = \mathbb{Z}$ se define $a * b$ como $a + b$. ✓
2. Sea $A = \mathbb{R}$ se define $a * b$ como $\frac{a}{b}$. ✗
3. Sea $A = \mathbb{Z}^+$ se define $a * b$ como $a - b$. ✗
4. Sea $A = \mathbb{Z}$ se define $a * b$ un número menor que a y b. ✗
5. Sea $A = \mathbb{R}$ se define $a * b =$máximo(a, b). ✓

Operaciones binarias

En cada caso determinar si se trata de una operación binaria:

1. Sea $A = \mathbb{Z}$ se define $a * b$ como $a + b$. ✓
2. Sea $A = \mathbb{R}$ se define $a * b$ como $\frac{a}{b}$. ✗
3. Sea $A = \mathbb{Z}^+$ se define $a * b$ como $a - b$. ✗
4. Sea $A = \mathbb{Z}$ se define $a * b$ un número menor que a y b. ✗
5. Sea $A = \mathbb{R}$ se define $a * b =$máximo(a, b). ✓
6. Sea $A = P(S)$ para algún conjunto S donde para un par de subconjuntos V y W se define $a * b$ como $V \cup W$.

Operaciones binarias

En cada caso determinar si se trata de una operación binaria:

1. Sea $A = \mathbb{Z}$ se define $a * b$ como $a + b$. ✓
2. Sea $A = \mathbb{R}$ se define $a * b$ como $\frac{a}{b}$. ✗
3. Sea $A = \mathbb{Z}^+$ se define $a * b$ como $a - b$. ✗
4. Sea $A = \mathbb{Z}$ se define $a * b$ un número menor que a y b. ✗
5. Sea $A = \mathbb{R}$ se define $a * b =$máximo(a, b). ✓
6. Sea $A = P(S)$ para algún conjunto S donde para un par de subconjuntos V y W se define $a * b$ como $V \cup W$. ✓

Operaciones binarias

En cada caso determinar si se trata de una operación binaria:

1. Sea $A = \mathbb{Z}$ se define $a * b$ como $a + b$. ✓
2. Sea $A = \mathbb{R}$ se define $a * b$ como $\frac{a}{b}$. ✗
3. Sea $A = \mathbb{Z}^+$ se define $a * b$ como $a - b$. ✗
4. Sea $A = \mathbb{Z}$ se define $a * b$ un número menor que a y b. ✗
5. Sea $A = \mathbb{R}$ se define $a * b =$máximo(a, b). ✓
6. Sea $A = P(S)$ para algún conjunto S donde para un par de subconjuntos V y W se define $a * b$ como $V \cup W$. ✓
7. Sea $A = P(S)$ para algún conjunto S donde para un par de subconjuntos V y W se define $a * b$ como $V \cap W$.

Operaciones binarias

En cada caso determinar si se trata de una operación binaria:

1. Sea $A = \mathbb{Z}$ se define $a * b$ como $a + b$. ✓
2. Sea $A = \mathbb{R}$ se define $a * b$ como $\frac{a}{b}$. ✗
3. Sea $A = \mathbb{Z}^+$ se define $a * b$ como $a - b$. ✗
4. Sea $A = \mathbb{Z}$ se define $a * b$ un número menor que a y b. ✗
5. Sea $A = \mathbb{R}$ se define $a * b =$máximo(a, b). ✓
6. Sea $A = P(S)$ para algún conjunto S donde para un par de subconjuntos V y W se define $a * b$ como $V \cup W$. ✓
7. Sea $A = P(S)$ para algún conjunto S donde para un par de subconjuntos V y W se define $a * b$ como $V \cap W$. ✓

Operaciones binarias

Si $A = \{a_1, a_2, ..., a_n\}$ es un conjunto finito, se puede definir una operación binaria en A por medio de una tabla como se muestra a continuación:

Operaciones binarias

Si $A = \{a_1, a_2, ..., a_n\}$ es un conjunto finito, se puede definir una operación binaria en A por medio de una tabla como se muestra a continuación:

$*$	a_1	a_2	$\cdots$	a_j	$\cdots$	a_n
a_1						
a_2						
$\vdots$						
a_i				$a_i * a_j$		
$\vdots$						
a_n						

Cuadro 1: Tabla de Cayley

Operaciones binarias

Si $A = \{a_1, a_2, ..., a_n\}$ es un conjunto finito, se puede definir una operación binaria en A por medio de una tabla como se muestra a continuación:

$*$	a_1	a_2	$\cdots$	a_j	$\cdots$	a_n
a_1						
a_2						
$\vdots$						
a_i				$a_i * a_j$		
$\vdots$						
a_n						

Cuadro 1: Tabla de Cayley

Operaciones binarias

¿Cuántas operaciones se pueden definir en el conjunto $A = \{a, b\}$?

Operaciones binarias

¿Cuántas operaciones se pueden definir en el conjunto $A = \{a, b\}$?
Definir algunos ejemplos de operaciones para el conjunto $B = \{V, F\}$.

Operaciones binarias

¿Cuántas operaciones se pueden definir en el conjunto $A = \{a, b\}$?
Definir algunos ejemplos de operaciones para el conjunto $B = \{V, F\}$.

X	Y	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
F	F	F	F	F	F	F	F	F	F	V	V	V	V	V	V	V	V
F	V	F	F	F	F	V	V	V	V	F	F	F	F	V	V	V	V
V	F	F	F	V	V	F	F	V	V	F	F	V	V	F	F	V	V
V	V	F	V	F	V	F	V	F	V	F	V	F	V	F	V	F	V

Operaciones binarias

Disyunción lógica:

$\vee$	F	V
F	F	V
V	V	V

Conjunción lógica:

$\wedge$	V	F
V	V	F
F	F	F

Sea $a * b$ una operación binaria en un conjunto A entonces puede que se cumplan las siguientes propiedades:

Sea $a * b$ una operación binaria en un conjunto A entonces puede que se cumplan las siguientes propiedades:

1. **Conmutativa:** $a * b = b * a$

Sea $a * b$ una operación binaria en un conjunto A entonces puede que se cumplan las siguientes propiedades:

1. **Conmutativa:** $a * b = b * a$

2. **Asociativa:** $(a * b) * c = a * (b * c)$

Sea $a * b$ una operación binaria en un conjunto A entonces puede que se cumplan las siguientes propiedades:

1. **Conmutativa:** $a * b = b * a$
2. **Asociativa:** $(a * b) * c = a * (b * c)$
3. **Elemento Identidad:** $e * a = a$ y $a * e = a$ para cada elemento a de A.

Sea $a * b$ una operación binaria en un conjunto A entonces puede que se cumplan las siguientes propiedades:

1. **Conmutativa:** $a * b = b * a$
2. **Asociativa:** $(a * b) * c = a * (b * c)$
3. **Elemento Identidad:** $e * a = a$ y $a * e = a$ para cada elemento a de A.
4. **Elemento Inverso:** $a * a^{-1} = e$ y $a^1 * a = e$ para cada elemento a de A.

Sea $a * b$ una operación binaria en un conjunto A entonces puede que se cumplan las siguientes propiedades:

1. **Conmutativa:** $a * b = b * a$
2. **Asociativa:** $(a * b) * c = a * (b * c)$
3. **Elemento Identidad:** $e * a = a$ y $a * e = a$ para cada elemento a de A.
4. **Elemento Inverso:** $a * a^{-1} = e$ y $a^1 * a = e$ para cada elemento a de A.
5. **Distributiva:** $a * (b \oplus c) = a * b \oplus a * c$.

Sea $a * b$ una operación binaria en un conjunto A entonces puede que se cumplan las siguientes propiedades:

1. **Conmutativa:** $a * b = b * a$
2. **Asociativa:** $(a * b) * c = a * (b * c)$
3. **Elemento Identidad:** $e * a = a$ y $a * e = a$ para cada elemento a de A.
4. **Elemento Inverso:** $a * a^{-1} = e$ y $a^1 * a = e$ para cada elemento a de A.
5. **Distributiva:** $a * (b \oplus c) = a * b \oplus a * c$.

Observaciones: una operación binaria es conmutativa si su matriz es simétrica.

Operaciones binarias

En cada caso determinar si la operación binaria es conmutativa y asociativa:

Operaciones binarias

En cada caso determinar si la operación binaria es conmutativa y asociativa:

1. Sea $A = Z$ se define $a * b = a + b + 2$.

Operaciones binarias

En cada caso determinar si la operación binaria es conmutativa y asociativa:

1. Sea $A = Z$ se define $a * b = a + b + 2$.

2. Sea $A = R$ se define $a * b = mínimo(a, b)$.

Operaciones binarias

En cada caso determinar si la operación binaria es conmutativa y asociativa:

1. Sea $A = Z$ se define $a * b = a + b + 2$.

2. Sea $A = R$ se define $a * b = mínimo(a, b)$.

3. Sea $A = \{a, b, c, d\}$ se define $a * b$ según la siguiente tabla.

*	a	b	c	d
a	a	c	b	d
b	d	a	b	c
c	c	d	a	a
d	d	b	a	c

Es $(a * b) * c = a * (b * c)$?

Definición

Un sistema que consiste de un conjunto no vacío y una o más operaciones n-arias sobre el conjunto recibe el nombre de **estructura algebraica**. *Un sistema algebraico se denotará por medio de* $< S, f_1, f_2, ...f_n >$ *cuando* S *es un conjunto no vacío y* $f_1, f_2, ..., f_n$ *son operaciones n-arias sobre* S.

Clasificación de las estructuras algebraicas con una operación binaria representada por $< S, * >$.

Clasificación de las estructuras algebraicas con una operación binaria representada por $< S, * >$.

1. Semigrupo ✓

Clasificación de las estructuras algebraicas con una operación binaria representada por $< S, * >$.

1. Semigrupo ✓

2. Monoide ✓

Clasificación de las estructuras algebraicas con una operación binaria representada por $< S, * >$.

1. Semigrupo ✓
2. Monoide ✓
3. Grupo ✓

Clasificación de las estructuras algebraicas con una operación binaria representada por $< S, * >$.

1. Semigrupo ✓
2. Monoide ✓
3. Grupo ✓

Semigrupo

Definición

Sea S un conjunto no vacío y sea $*$ una operación binaria sobre S. Si se cumple que $*$ es una operación asociativa, entonces la dupla $< S, * >$ se denomina semigrupo donde:

$$(a * b) * c = a * (b * c), \text{ para todo } a, b, c \in S.$$

Monoide

Definición

Sea M un conjunto no vacío y sea $*$ una operación binaria en M, entonces $< M, * >$ es un monoide si es un semigrupo y tiene elemento identidad, es decir que:

1. $(a * b) * c = a * (b * c)$, *para todo* $a, b, c \in M$.
2. *Existe* $e \in M$ *tal que* $e * a = a = a * e$.

Monoide

Ejemplos:

Monoide

Ejemplos:

- Números enteros positivos con la operación producto.

Monoide

Ejemplos:

- Números enteros positivos con la operación producto. ✓

Monoide

Ejemplos:

- Números enteros positivos con la operación producto. ✓
- Números enteros positivos con la operación suma.

Monoide

Ejemplos:

- Números enteros positivos con la operación producto. ✓
- Números enteros positivos con la operación suma. ✓

Monoide

Ejemplos:

- Números enteros positivos con la operación producto. ✓
- Números enteros positivos con la operación suma. ✓
- Números racionales con la operación producto.

Monoide

Ejemplos:

- Números enteros positivos con la operación producto. ✓
- Números enteros positivos con la operación suma. ✓
- Números racionales con la operación producto. ✓

Monoide

Ejemplos:

- Números enteros positivos con la operación producto. ✓
- Números enteros positivos con la operación suma. ✓
- Números racionales con la operación producto. ✓

Definición

Sea G un conjunto no vacío y sea $*$ una operación binaria en G. Si $< G, * >$ es un monoide donde todo elemento tiene inverso, entonces $< G, * >$ se denomina grupo, esto significa que:

1. $(a * b) * c = a * (b * c)$, *para todo* $a, b, c \in M$.
2. *Existe* $e \in M$ *tal que* $e * a = a = a * e$.
3. *Para todo* $a \in G$ *existe* $a^{-1} \in G$ *tal que* $a * a^{-1} = e = a^{-1} * a$, *para todo* $a, b, c \in G$

Ejemplos

1. El conjunto de los números enteros positivos con la operación de suma.

Ejemplos

1. El conjunto de los números enteros positivos con la operación de suma. ✗

Ejemplos

1. El conjunto de los números enteros positivos con la operación de suma. ✗

2. El conjunto de los números enteros positivos con la operación de multiplicación.

Ejemplos

1. El conjunto de los números enteros positivos con la operación de suma. ✗

2. El conjunto de los números enteros positivos con la operación de multiplicación. ✗

Ejemplos

1. El conjunto de los números enteros positivos con la operación de suma. ✗
2. El conjunto de los números enteros positivos con la operación de multiplicación. ✗
3. El conjunto de los números racionales sin el cero con la operación producto.

Ejemplos

1. El conjunto de los números enteros positivos con la operación de suma. ✗
2. El conjunto de los números enteros positivos con la operación de multiplicación. ✗
3. El conjunto de los números racionales sin el cero con la operación producto. ✓

Ejemplos

1. El conjunto de los números enteros positivos con la operación de suma. ✗
2. El conjunto de los números enteros positivos con la operación de multiplicación. ✗
3. El conjunto de los números racionales sin el cero con la operación producto. ✓
4. El conjunto de matrices reales 2×2 inversibles con la operación producto.

Ejemplos

1. El conjunto de los números enteros positivos con la operación de suma. ✗
2. El conjunto de los números enteros positivos con la operación de multiplicación. ✗
3. El conjunto de los números racionales sin el cero con la operación producto. ✓
4. El conjunto de matrices reales 2×2 inversibles con la operación producto. ✓

Ejemplos

1. El conjunto de los números enteros positivos con la operación de suma. ✗
2. El conjunto de los números enteros positivos con la operación de multiplicación. ✗
3. El conjunto de los números racionales sin el cero con la operación producto. ✓
4. El conjunto de matrices reales 2×2 inversibles con la operación producto. ✓

Grupos

En cada caso explicar si las siguientes estructuras algebraicas son grupos:

En cada caso explicar si las siguientes estructuras algebraicas son grupos:

1. $< \mathbb{Z}, + >$

En cada caso explicar si las siguientes estructuras algebraicas son grupos:

1. $< \mathbb{Z}, + >$ ✓

En cada caso explicar si las siguientes estructuras algebraicas son grupos:

1. $< \mathbb{Z}, + >$ ✓
2. $< \mathbb{Z}, \times >$

Grupos

En cada caso explicar si las siguientes estructuras algebraicas son grupos:

1. $< \mathbb{Z}, + >$ ✓
2. $< \mathbb{Z}, \times >$ ✗

Grupos

En cada caso explicar si las siguientes estructuras algebraicas son grupos:

1. $< \mathbb{Z}, + >$ ✓
2. $< \mathbb{Z}, \times >$ ✗
3. $< \mathbb{Q}, \times >$

Grupos

En cada caso explicar si las siguientes estructuras algebraicas son grupos:

1. $< \mathbb{Z}, + >$ ✓
2. $< \mathbb{Z}, \times >$ ✗
3. $< \mathbb{Q}, \times >$ ✗

Grupos

En cada caso explicar si las siguientes estructuras algebraicas son grupos:

1. $< \mathbb{Z}, + >$ ✓
2. $< \mathbb{Z}, \times >$ ✗
3. $< \mathbb{Q}, \times >$ ✗

Ejemplo:

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Ejemplo:

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Si consideramos que $a = 4$ y $b = -2$ entonces:

$$\begin{aligned} 4 * (-2) &= 4 - 2 + 2 \cdot 4 \cdot (-2) \\ &= 4 - 2 - 16 \\ &= 4 - 18 \\ &= -14 \end{aligned}$$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Para verificar si $< \mathbb{R}, * >$ es un semigrupo debemos verificar si se cumple: $(a * b) * c = a * (b * c)$.

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Para verificar si $< \mathbb{R}, * >$ es un semigrupo debemos verificar si se cumple: $(a * b) * c = a * (b * c)$.

$$(a * b) * c \quad = \quad (a + b + 2ab) * c$$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Para verificar si $< \mathbb{R}, * >$ es un semigrupo debemos verificar si se cumple: $(a * b) * c = a * (b * c)$.

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

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Para verificar si $< \mathbb{R}, * >$ es un semigrupo debemos verificar si se cumple: $(a * b) * c = a * (b * c)$.

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

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Para verificar si $< \mathbb{R}, * >$ es un semigrupo debemos verificar si se cumple: $(a * b) * c = a * (b * c)$.

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

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Para verificar si $< \mathbb{R}, * >$ es un semigrupo debemos verificar si se cumple: $(a * b) * c = a * (b * c)$.

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

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Para verificar si $< \mathbb{R}, * >$ es un semigrupo debemos verificar si se cumple: $(a * b) * c = a * (b * c)$.

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

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Ahora hay que desarrollar la otra parte de la igualdad:

$$a * (b * c) \quad = \quad a * (b + c + 2bc)$$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Ahora hay que desarrollar la otra parte de la igualdad:

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

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Ahora hay que desarrollar la otra parte de la igualdad:

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

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Ahora hay que desarrollar la otra parte de la igualdad:

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

Grupo

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Verificar si la operación en $< \mathbb{R}, * >$ es conmutativa:

$$a * b \quad = \quad a + b + 2 \cdot a \cdot b$$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Verificar si la operación en $< \mathbb{R}, * >$ es conmutativa:

$$a * b = a + b + 2 \cdot a \cdot b$$

$$b * a = b + a + 2 \cdot b \cdot a$$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Verificar si la operación en $< \mathbb{R}, * >$ es conmutativa:

$$a * b = a + b + 2 \cdot a \cdot b$$

$$\begin{aligned} b * a &= b + a + 2 \cdot b \cdot a \\ &= a + b + 2 \cdot a \cdot b \end{aligned}$$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Verificar si la operación en $< \mathbb{R}, * >$ es conmutativa:

$$a * b = a + b + 2 \cdot a \cdot b$$

$$\begin{aligned} b * a &= b + a + 2 \cdot b \cdot a \\ &= a + b + 2 \cdot a \cdot b \end{aligned}$$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Ahora, hay que verificar si existe el elemento identidad en $< \mathbb{R}, * >$.
Recordar que se debe cumplir que $e * a = a = a * e$ para todo elemento a en $< \mathbb{R}, * >$.
Por un lado $a * e = a$ es decir que:

$$a + e + 2ae = a \quad \leftrightarrow \quad +a - a + e + 2ae$$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Ahora, hay que verificar si existe el elemento identidad en $< \mathbb{R}, * >$.
Recordar que se debe cumplir que $e * a = a = a * e$ para todo elemento a en $< \mathbb{R}, * >$.
Por un lado $a * e = a$ es decir que:

$$\begin{aligned} a + e + 2ae = a \quad &\leftrightarrow \quad +a - a + e + 2ae \\ &\leftrightarrow \quad e(1 + 2a) = 0 \end{aligned}$$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Ahora, hay que verificar si existe el elemento identidad en $< \mathbb{R}, * >$.
Recordar que se debe cumplir que $e * a = a = a * e$ para todo elemento a en $< \mathbb{R}, * >$.
Por un lado $a * e = a$ es decir que:

$$\begin{aligned} a + e + 2ae = a \quad &\leftrightarrow \quad +a - a + e + 2ae \\ &\leftrightarrow \quad e(1 + 2a) = 0 \\ &\leftrightarrow \quad e = \frac{0}{(1+2a)}, \text{ donde } a \neq \frac{-1}{2} \end{aligned}$$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Ahora, hay que verificar si existe el elemento identidad en $< \mathbb{R}, * >$.
Recordar que se debe cumplir que $e * a = a = a * e$ para todo elemento a en $< \mathbb{R}, * >$.
Por un lado $a * e = a$ es decir que:

$$\begin{aligned} a + e + 2ae = a \quad &\leftrightarrow \quad +a - a + e + 2ae \\ &\leftrightarrow \quad e(1 + 2a) = 0 \\ &\leftrightarrow \quad e = \tfrac{0}{(1+2a)}, \text{ donde } a \neq \tfrac{-1}{2} \\ &\leftrightarrow \quad e = 0, \text{ donde } a \neq \tfrac{-1}{2} \end{aligned}$$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Ahora, hay que verificar si existe el elemento identidad en $< \mathbb{R}, * >$.
Recordar que se debe cumplir que $e * a = a = a * e$ para todo elemento a en $< \mathbb{R}, * >$.
Por un lado $a * e = a$ es decir que:

$$\begin{aligned} a + e + 2ae = a \quad &\leftrightarrow \quad +a - a + e + 2ae \\ &\leftrightarrow \quad e(1 + 2a) = 0 \\ &\leftrightarrow \quad e = \tfrac{0}{(1+2a)}, \text{ donde } a \neq \tfrac{-1}{2} \\ &\leftrightarrow \quad e = 0, \text{ donde } a \neq \tfrac{-1}{2} \end{aligned}$$

Verificamos que:
$a * e = a * 0 = a + 0 + 2 \cdot a \cdot 0 = a$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Verificación de la existencia del elemento inverso a^{-1} en $< \mathbb{R}, * >$.
Recordar, el elemento inverso debe cumplir que $a * a^{-1} = e = a^{-1} * a$, es decir que:

$$a + a^{-1} + 2aa^{-1} = 0 \quad \leftrightarrow \quad a^{-1}(1 + 2a) = -a$$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Verificación de la existencia del elemento inverso a^{-1} en $< \mathbb{R}, * >$.
Recordar, el elemento inverso debe cumplir que $a * a^{-1} = e = a^{-1} * a$, es decir que:

$$\begin{aligned} a + a^{-1} + 2aa^{-1} = 0 \quad &\leftrightarrow \quad a^{-1}(1 + 2a) = -a \\ &\leftrightarrow \quad a^{-1} = -\frac{a}{1+2a}, \text{ donde } a \neq -\frac{1}{2} \end{aligned}$$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Verificación de la existencia del elemento inverso a^{-1} en $< \mathbb{R}, * >$.
Recordar, el elemento inverso debe cumplir que $a * a^{-1} = e = a^{-1} * a$, es decir que:

$$\begin{aligned} a + a^{-1} + 2aa^{-1} = 0 \quad &\leftrightarrow \quad a^{-1}(1 + 2a) = -a \\ &\leftrightarrow \quad a^{-1} = -\frac{a}{1+2a}, \text{ donde } a \neq -\frac{1}{2} \end{aligned}$$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

El elemento inverso a^{-1} en $< \mathbb{R}, * >$ es $a^{-1} = -\frac{a}{1+2a}$, donde $a \neq -\frac{1}{2}$.
Entonces podemos comprobar que:

$$a * a^{-1} \quad = \quad a * \left(-\frac{a}{1+2a}\right)$$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

El elemento inverso a^{-1} en $< \mathbb{R}, * >$ es $a^{-1} = -\frac{a}{1+2a}$, donde $a \neq -\frac{1}{2}$.
Entonces podemos comprobar que:

$$\begin{aligned} a * a^{-1} &= a * \left(-\tfrac{a}{1+2a}\right) \\ &= a + \left(-\tfrac{a}{1+2a}\right) + 2a\left(-\tfrac{a}{1+2a}\right) \end{aligned}$$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

El elemento inverso a^{-1} en $< \mathbb{R}, * >$ es $a^{-1} = -\frac{a}{1+2a}$, donde $a \neq -\frac{1}{2}$.
Entonces podemos comprobar que:

$$\begin{aligned} a * a^{-1} &= a * \left(-\tfrac{a}{1+2a}\right) \\ &= a + \left(-\tfrac{a}{1+2a}\right) + 2a\left(-\tfrac{a}{1+2a}\right) \\ &= \tfrac{a(1+2a)}{1+2a} - \tfrac{a}{1+2a} - \tfrac{2a^2}{1+2a} \end{aligned}$$

Sea $< \mathbb{R}, * >$ con la operación $*$ definida por $a * b = a + b + 2 \cdot a \cdot b$

El elemento inverso a^{-1} en $< \mathbb{R}, * >$ es $a^{-1} = -\frac{a}{1+2a}$, donde $a \neq -\frac{1}{2}$.
Entonces podemos comprobar que:

$$\begin{aligned} a * a^{-1} &= a * \left(-\tfrac{a}{1+2a}\right) \\ &= a + \left(-\tfrac{a}{1+2a}\right) + 2a\left(-\tfrac{a}{1+2a}\right) \\ &= \tfrac{a(1+2a)}{1+2a} - \tfrac{a}{1+2a} - \tfrac{2a^2}{1+2a} \\ &= \tfrac{a+2a^2-a-2a^2}{1+2a} = 0 \end{aligned}$$

Si consideramos $< \mathbb{R}, * >$ entonces no es un grupo ya que $-\frac{1}{2}$ no tiene inverso.

Si consideramos $< \mathbb{R}, * >$ entonces no es un grupo ya que $-\frac{1}{2}$ no tiene inverso.

Si consideramos $< \mathbb{R} - \frac{1}{2}, * >$ entonces si es un grupo ya que todo elemento tiene inverso.

Definición

Sea $\mathbb{Z}_n$ el conjunto de enteros módulo n que en forma general está dado por: $\mathbb{Z}_n = [0], [1], \cdots, [n-2], [n-1]$.

Definición

Sea $\mathbb{Z}_n$ el conjunto de enteros módulo n que en forma general está dado por: $\mathbb{Z}_n = [0], [1], \cdots, [n-2], [n-1]$.

Ejemplos:

$\mathbb{Z}_2 = [0], [1]$

Definición

Sea $\mathbb{Z}_n$ el conjunto de enteros módulo n que en forma general está dado por: $\mathbb{Z}_n = [0], [1], \cdots, [n-2], [n-1]$.

Ejemplos:

$\mathbb{Z}_2 = [0], [1]$

$\mathbb{Z}_3 = [0], [1], [2]$

Definición

Sea $\mathbb{Z}_n$ el conjunto de enteros módulo n que en forma general está dado por: $\mathbb{Z}_n = [0], [1], \cdots, [n-2], [n-1]$.

Ejemplos:

$\mathbb{Z}_2 = [0], [1]$

$\mathbb{Z}_3 = [0], [1], [2]$

$\mathbb{Z}_4 = [0], [1], [2], [3]$

Definición

Sea $\mathbb{Z}_n$ el conjunto de enteros módulo n que en forma general está dado por: $\mathbb{Z}_n = [0], [1], \cdots, [n-2], [n-1]$.

Ejemplos:

$\mathbb{Z}_2 = [0], [1]$

$\mathbb{Z}_3 = [0], [1], [2]$

$\mathbb{Z}_4 = [0], [1], [2], [3]$

$\mathbb{Z}_5 = [0], [1], [2], [3], [4]$

Definición

Sea $\mathbb{Z}_n$ el conjunto de enteros módulo n que en forma general está dado por: $\mathbb{Z}_n = [0], [1], \cdots, [n-2], [n-1]$.

Ejemplos:

$\mathbb{Z}_2 = [0], [1]$

$\mathbb{Z}_3 = [0], [1], [2]$

$\mathbb{Z}_4 = [0], [1], [2], [3]$

$\mathbb{Z}_5 = [0], [1], [2], [3], [4]$

$\mathbb{Z}_6 = [0], [1], [2], [3], [4], [5]$

Definición

Sea $\mathbb{Z}_n$ el conjunto de enteros módulo n que en forma general está dado por: $\mathbb{Z}_n = [0], [1], \cdots, [n-2], [n-1]$.

Ejemplos:

$\mathbb{Z}_2 = [0], [1]$

$\mathbb{Z}_3 = [0], [1], [2]$

$\mathbb{Z}_4 = [0], [1], [2], [3]$

$\mathbb{Z}_5 = [0], [1], [2], [3], [4]$

$\mathbb{Z}_6 = [0], [1], [2], [3], [4], [5]$

Es posible definir las operaciones de suma y producto en $\mathbb{Z}_n$.

Podemos definir el producto en $\mathbb{Z}_n$ utilizando las tablas de Cayley:

Podemos definir el producto en $\mathbb{Z}_n$ utilizando las tablas de Cayley:

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

Podemos definir el producto en $\mathbb{Z}_n$ utilizando las tablas de Cayley:

Podemos definir el producto en $\mathbb{Z}_n$ utilizando las tablas de Cayley:

$\times$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[6]	[8]	[10]
[3]	[0]	[3]	[6]			
[4]	[0]	[4]	[8]			
[5]	[0]	[5]	[10]			

Podemos definir el producto en $\mathbb{Z}_n$ utilizando las tablas de Cayley:

Podemos definir el producto en $\mathbb{Z}_n$ utilizando las tablas de Cayley:

$\times$	[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]			
[4]	[0]	[4]	[2]			
[5]	[0]	[5]	[4]			

Podemos definir el producto en $\mathbb{Z}_n$ utilizando las tablas de Cayley:

Podemos definir el producto en $\mathbb{Z}_n$ utilizando las tablas de Cayley:

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

Podemos definir el producto en $\mathbb{Z}_n$ utilizando las tablas de Cayley:

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

Es posible demostrar que $\times$ es asociativa en $\mathbb{Z}_6$, por lo tanto $< \mathbb{Z}_6, \times >$ es un semigrupo.

Podemos definir el producto en $\mathbb{Z}_n$ utilizando las tablas de Cayley:

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

Es posible demostrar que $\times$ es asociativa en $\mathbb{Z}_6$, por lo tanto $< \mathbb{Z}_6, \times >$ es un semigrupo.

$< \mathbb{Z}_6, \times >$ no es un grupo ya que por ejemplo [2] no tiene inverso.

Podemos definir el producto en $\mathbb{Z}_n$ utilizando las tablas de Cayley:

Podemos definir el producto en $\mathbb{Z}_n$ utilizando las tablas de Cayley:

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

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

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

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

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

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[3]$	$[3]$	$[4]$	$[5]$		
$[4]$	$[4]$	$[0]$	$[6]$		

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

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

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

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

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

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

Es posible demostrar que $+$ es asociativa en $\mathbb{Z}_5$, por lo tanto $< \mathbb{Z}_5, + >$ es un semigrupo.

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

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

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

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

Es posible demostrar que $+$ es asociativa en $\mathbb{Z}_5$, por lo tanto $< \mathbb{Z}_5, + >$ es un semigrupo.

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

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

Es posible demostrar que $+$ es asociativa en $\mathbb{Z}_5$, por lo tanto $< \mathbb{Z}_5, + >$ es un semigrupo.

Es posible observar que $[0]$ es el elemento identidad $\mathbb{Z}_5$, por lo tanto $< \mathbb{Z}_5, + >$ es un monoide.

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

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

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

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

Es posible demostrar que $+$ es asociativa en $\mathbb{Z}_5$, por lo tanto $< \mathbb{Z}_5, + >$ es un semigrupo.

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

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

Es posible demostrar que $+$ es asociativa en $\mathbb{Z}_5$, por lo tanto $< \mathbb{Z}_5, + >$ es un semigrupo.

Es posible observar que $[0]$ es el elemento identidad $\mathbb{Z}_5$, por lo tanto $< \mathbb{Z}_5, + >$ es un monoide.

Podemos definir la suma en $\mathbb{Z}_5$ utilizando la tabla de Cayley:

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

Es posible demostrar que $+$ es asociativa en $\mathbb{Z}_5$, por lo tanto $< \mathbb{Z}_5, + >$ es un semigrupo.

Es posible observar que $[0]$ es el elemento identidad $\mathbb{Z}_5$, por lo tanto $< \mathbb{Z}_5, + >$ es un monoide.

Existe un inverso para cada elemento de $\mathbb{Z}_5$, por lo tanto $< \mathbb{Z}_5, + >$ es un grupo. ¿Cuáles son los inversos?

Sea $< G, \times >$ un grupo, en donde la operación $\times$ es identificada como un producto, y sea e el elemento neutro de G. Entonces escribimos $a^0 := e$ para todo $a \in G$.

Sea $< G, \times >$ un grupo, en donde la operación $\times$ es identificada como un producto, y sea e el elemento neutro de G. Entonces, si $n = 1, 2, 3, \cdots$ escribimos $a^n := a \times a \times a \cdots \times a$ (n veces) para todo $a \in G$.

Sea $< G, \times >$ un grupo, en donde la operación $\times$ es identificada como un producto, y sea e el elemento neutro de G. Entonces, si $n = 1, 2, 3, \cdots$ escribimos $a^{-n} := a^{-1} \times a^{-1} \times a^{-1} \cdots \times a^{-1}$ (n veces) para todo $a \in G$.

Sea $< G, + >$ un grupo, en donde la operación $+$ es identificada como una suma, y sea e el elemento neutro de G. Entonces escribimos $0 \cdot a = e$ para todo $a \in G$.

Sea $< G, + >$ un grupo, en donde la operación $+$ es identificada como una suma, y sea e el elemento neutro de G. Entonces si $n = 1, 2, 3, \cdots$, escribimos $n \cdot a = a + a + \cdots + a$ (n veces), para todo $a \in G$.

Sea $< G, + >$ un grupo, en donde la operación $+$ es identificada como una suma, y sea e el elemento neutro de G. Entonces si $n = 1, 2, 3, \cdots$, escribimos $(-n) \cdot a = (-a) + (-a) + \cdots + (-a)$ (n veces), para todo $a \in G$. Observar que $-a$ representa el elemento inverso aditivo u opuesto.

Definición

Sea $< G, * >$ un grupo, entonces el **orden del grupo** *G, denotado por $O(G)$, es el cardinal del conjunto G, es decir, la cantidad de elementos del conjunto G.*

Definición

Se dice que un **semigrupo**, *un* **monoide** *o un* **grupo** *es* **conmutativo** *o* **abeliano** *si se cumple que:*

Definición

Se dice que un **semigrupo**, *un* **monoide** *o un* **grupo** *es* **conmutativo** *o* **abeliano** *si se cumple que:*

$$a * b = b * a$$

para todo a, b *en la estructura algebraica correspondiente.*

Resumen clasificación estructuras algebraicas con una operación

	Asociativa	Identidad	Inverso	Conmutativa
Semigrupo	✓			
Monoide	✓	✓		
Grupo	✓	✓	✓	
Grupo Abeliano	✓	✓	✓	✓

Theorem

Sea $< G, * >$ un grupo, entonces se cumplen las siguientes propiedades:

Theorem

Sea $< G, * >$ un grupo, entonces se cumplen las siguientes propiedades:

1. *El elemento identidad de $< G, * >$ es único.*

Theorem

Sea $< G, * >$ un grupo, entonces se cumplen las siguientes propiedades:

1. *El elemento identidad de $< G, * >$ es único.*
2. *El elemento inverso de cada elemento de $< G, * >$ es único.*

Theorem

Sea $< G, * >$ un grupo, entonces se cumplen las siguientes propiedades:

1. *El elemento identidad de $< G, * >$ es único.*
2. *El elemento inverso de cada elemento de $< G, * >$ es único.*
3. *Las leyes de cancelación son verdaderas en un grupo, es decir, para todo $a, b, c \in G$.*

Theorem

Sea $< G, * >$ un grupo, entonces se cumplen las siguientes propiedades:

1. *El elemento identidad de $< G, * >$ es único.*
2. *El elemento inverso de cada elemento de $< G, * >$ es único.*
3. *Las leyes de cancelación son verdaderas en un grupo, es decir, para todo $a, b, c \in G$.*

$$a * b = a * c \rightarrow b = c$$
$$b * a = c * a \rightarrow b = c$$

4. *Si $a, b \in G$ la ecuación $a * x = b$ tiene solución única $x = a^{-1} * b$. Similarmente, la ecuación $y * a = b$ tiene solución única $y = b * a^{-1}$.*

Theorem

Sea $< G, * >$ un grupo, entonces se cumplen las siguientes propiedades:

1. *El elemento identidad de $< G, * >$ es único.*
2. *El elemento inverso de cada elemento de $< G, * >$ es único.*
3. *Las leyes de cancelación son verdaderas en un grupo, es decir, para todo $a, b, c \in G$.*

$$a * b = a * c \rightarrow b = c$$
$$b * a = c * a \rightarrow b = c$$

4. *Si $a, b \in G$ la ecuación $a * x = b$ tiene solución única $x = a^{-1} * b$. Similarmente, la ecuación $y * a = b$ tiene solución única $y = b * a^{-1}$.*
5. *El único elemento* **idempotencia** *de $< G, * >$ es el elemento identidad e, es decir: $a * a = a \rightarrow a = e$.*

Ejercicios

Operaciones binarias

Considere los siguientes incisos, y para cada uno indique si la operación es cerrada en el dominio:

1. La suma $(+)$ en el conjunto de los números enteros $(\mathbb{Z})$.
2. La suma $(+)$ en el conjunto de los números enteros pares.
3. La suma $(+)$ en el conjunto de los números enteros impares.
4. La disyunción $(\vee)$ en el conjunto de los valores lógicos $(\{\text{Verdadero,Falso}\})$.
5. La resta (-) en el conjunto de los números enteros $(\mathbb{Z})$.
6. La resta (-) en el conjunto de los números naturales $(\mathbb{N})$.
7. El condicional $(\rightarrow)$ en el conjunto de los valores lógicos $(\{\text{Verdadero,Falso}\})$.
8. La multiplicación (.) en el conjunto de los números reales $(\mathbb{R})$.
9. La división $(/)$ en el conjunto de los números enteros $(\mathbb{Z})$.

Operaciones binarias

En caso de no estar bien denida la operación, proporcionar las condiciones necesarias para que su denifición sea adecuada.

1. $\mathbb{Z}$ con a*b=a+b
2. $\mathbb{R}$ con $a \triangle b = \frac{a}{b}$
3. $\mathbb{Z}$ con $a \otimes b = \frac{a}{b}$
4. $\mathbb{Z}^+$ con $a \star b = a - b$
5. $\mathbb{Z}$ con $a \oplus b$ =menor(a,b)
6. $P(\mathbb{S})$ con $a : b = W \cup V$, suponiendo que la operación binaria es asociativa.

Clasificación Estructuras Algebraicas

Determinar, en cada caso, si los conjuntos con las operaciones dadas son semigrupos, monoides o grupos. Indicar si son abelianos.

1. El conjunto $\mathbb{Z}$ con la operación de adición.
2. $\mathbb{Q}$ donde $(a \triangle b) = a + b$.
3. $\mathbb{Q}$ con el producto usual.
4. $\mathbb{R}$ donde $(a \oslash b) = a + b + 2$
5. $G = \{x | x \in \mathbb{R} \wedge x \neq -1\}$ donde $(a \otimes b) = a + b + ab$

Determinar, en cada caso, si los conjuntos con las operaciones dadas son semigrupos, monoides o grupos. Indicar si son abelianos.

6. La operación binaria sobre el conjunto $\mathbb{R}$ de números reales definida por $(a * b) = a + b + 2ab$

7. El conjunto de los números racionales $G = \{\mathbb{Q} - \{0\} \times \mathbb{Q}\}$ con la operación $(a, b) * (c, d) = (ac, bc + d)$ donde las operaciones son la suma y productos habituales de $\mathbb{Q}$. Determinar si $< G, * >$ es un monoide, un semigrupo y/o un grupo, es abeliano?

Fin