Unidad 3: ESTRUCTURAS ALGEBRAICAS FINITAS

Estructuras Algebraicas.

Operaciones.

Propiedades de una Operación Binaria Cerrada.

Principales estructuras algebraicas:

Monoide,

Semigrupo,

Grupo,

Anillo,

Cuerpo,

Álgebra de Boole.

1.1 Introducción

Desde el nivel primario se conocen distintos conjuntos numéricos: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$, y en el nivel superior algunos nuevos como $M_{mxn}(\mathbb{R})$: conjunto de las matrices de números reales; $\mathbb{R}^n$: el conjunto de n-uplas ordenadas de números reales y C^n: conjunto de funciones continuas hasta la derivada de orden n . En ellos se definen operaciones que tienen propiedades en común, las cuales permiten clasificar a los conjuntos en "categorías". A dichas categorías se las llaman Estructuras Algebraicas. Estas estructuras (grupos, anillos, cuerpos, entre otros) permiten generalizar y abstraer conceptos matemáticos para resolver problemas complejos. Son fundamentales en matemáticas y tienen aplicaciones en diversas áreas como la física, la informática y la ingeniería.

En informática, las estructuras algebraicas son de gran importancia por varias razones:

- Permiten modelar estructuras de datos complejas y sus operaciones, lo que es fundamental para el diseño de software y bases de datos **(Modelado de Datos)**

- Son esenciales en criptografía para crear algoritmos de cifrados seguros. Por ejemplo, la teoría de grupos se utiliza en algoritmos como RSA **(Criptografía)**

- Ayudan a entender los fundamentos teóricos de la computación, como la complejidad computacional y la teoría de autómatas **(Teoría de la Computación)**

- Facilitan la creación y análisis de algoritmos eficientes, especialmente en la resolución de problemas combinatorios **(Optimización de Algoritmos)**

- Desde el punto de vista del Álgebra Universal son básicas en el desarrollo actual de la ciencia de la computación. Esto incluye monoides, semigrupos, grupos y anillos, que son estudiados en particular debido a su relevancia.

- Tienen aplicaciones prácticas en áreas como gráficos por computadora, encriptación de datos, procesamiento de señales, aprendizaje automático, robótica y automatización.

En resumen, las estructuras algebraicas proporcionan un marco teórico que apoya el desarrollo y la comprensión de muchos aspectos fundamentales de la informática.

1.2 Estructuras Algebraicas

Definición

Una Estructura Algebraica es un objeto matemático formado por un conjunto no vacío y una operación definida en él.

Notación:

(A, operación 1); (A,$*$)

Se lee estructura algebraica o sistema matemático del conjunto A $\neq\emptyset$ respecto de la operación 1.

En situaciones más complejas, puede suceder que:

- exista más de una operación en A, en ese caso se tiene: (A, operación 1, operación 2,…, operación n); (A, $*$, #)

- involucre más de un conjunto: (A, operación 1, B, operación 2) ; (A, $*$, B, #)

- Además del símbolo $*$ se puede usar cualquier símbolo a elección, por ejemplo: #, ♦, Δ, □, etc. inclusive los símbolos de las operaciones conocidas como + (adición), • (multiplicación), $\cup$ (unión), $\cap$ (intersección) , $\vee$ (disyunción), $\wedge$ (conjunción), etc.

Ejemplos

Las siguientes son estructuras ya conocidas por el estudiante:

i) $(\mathbb{N}, -)$, Números Naturales respecto de la operación diferencia usual
ii) $(\mathbb{Z}, +)$, Números Enteros respecto de la operación suma usual
iii) $(\mathbb{R}, +, \bullet)$, Números Reales respecto de la suma y producto usuales.
iv) $(\wp(X), \cup, \cap)$, Potencia de X respecto de la unión e intersección.
v) $(M_{nxn}(\mathbb{R}), +, \bullet)$, Matrices cuadradas de orden n de números reales con la suma y producto usual.
vi) (S , $\vee$, $\wedge$) , Conjunto de todas las proposiciones respecto de las operaciones disyunción y conjunción.
vii) ({0,1}, +, •), Conjunto de valores booleanos con las operaciones suma y producto lógico.

viii) $(V, +, \mathbb{R}, \bullet)$ espacio vectorial: es una estructura algebraica formada por un conjunto de vectores, donde se definen dos operaciones: la suma de vectores y la multiplicación de un vector por un escalar. Categoría que no se considerará en esta materia.

En particular, si el conjunto es finito se tiene una Estructura Algebraica Finita y son las estructuras en las que pondremos más énfasis en este capítulo.

1.3 Operación

Una operación es una función definida en un conjunto. Se clasifican en *binarias* y *unarias*.

Para la aplicación de una ley o enunciado, las operaciones pueden requerir un solo elemento, en cuyo caso se denominan unarias, o dos elementos, motivo por el cual suelen llamarse binarias.

Operación binaria

Definición

Sea un conjunto A ≠ ∅ se llama operación binaria sobre A, a toda función que tiene por dominio a AxA= A^2 e imagen en otro conjunto (que puede o no ser igual a A).

En particular, se dice que una operación binaria sobre A es cerrada (o **ley de composición interna**) si su imagen es A. Simbólicamente, se indica:

$$f\text{: AxA} \longrightarrow \text{A} \quad /$$

$$f\,(a,\, b) = \text{c}$$

Notación

Utilizaremos el símbolo $*$ en lugar de f, de la siguiente manera: $f(a, b) = a * b = \text{c}$

$$*\text{: AxA} \longrightarrow \text{A} \quad /$$

$$(a,\, b) \longrightarrow a * b$$

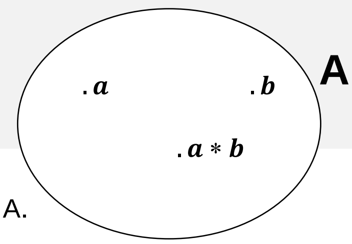

Fig.3.1. Conjunto A.

Es decir $a \in A \wedge b \in A \rightarrow a * b$

Observaciones

- La unicidad de $a * b$ está dada por la definición de función, así como $Dom(*)$ = A^2.

- En la expresión "$a * b$", a y b son los operandos izquierdo y derecho respectivamente de $*$.

OPERACIONES BINARIAS DEFINIDAS EN CONJUNTOS FINITOS

Si A es finito con n elementos, las operaciones binarias pueden definirse por medio de una tabla bidimensional (de doble entrada) de n filas por n columnas. Convenimos en disponer los elementos de A, en las columnas de izquierda a derecha y (con el mismo orden) en las filas de arriba hacia abajo, es decir:

Sea A = { x_1, x_2,…, x_n }, la operación binaria $*$: AxA → A puede definirse por

$*$	x_1	…	x_j	…	x_n
x_1					
⋮					
x_i			$x_i * x_j$		
⋮					
x_n					

elementos de A

La posición (i, j) corresponde al resultado de operar x_i con x_j.

Tabla 3.1

elementos de A

Si * es una operación binaria sobre un conjunto A, es común referirse a $*$ utilizando alguno de los siguientes enunciados (todos ellos equivalentes)

* es una operación cerrada sobre A

el conjunto A es cerrado bajo *

* es una ley de composición interna

* es una operación interna sobre A

🗒 Ejemplos

a) La adición o la multiplicación son cerradas en cada uno de los conjuntos numéricos: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$

Pues, cualquiera sea el par de números que se tomen de estos conjuntos siempre es posible sumarlos (o multiplicarlos) y el resultado que se obtiene es un único número que pertenece al mismo conjunto.

b) La adición usual en A = {1, 2, 3, 4, 5 } no es cerrada ya que 3 + 4 $\notin$ A.

c) En A = { a , b , c } y la operación $*$ definida por Tabla 3.2 es cerrada.

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

Tabla 3.2

Pues todos los elementos interiores a la tabla son elementos de A. Es decir:

a$*$a = a; a$*$b = c, a$*$c = b¸ b$*$a = b, b$*$b = a, b$*$c = c; c$*$a = c, c$*$b = b, c$*$c = a;

Actividad 3.1

Determinar si las siguientes son operaciones binarias cerradas (o leyes de composición interna) en el conjunto indicado:

a) Las operaciones sustracción y división en los conjuntos numéricos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{R} - \{0\}$

b) Las operaciones adición y multiplicación usual en el conjunto A donde

A = { x $\in$ $\mathbb{Z}$ / x es un entero impar}

a) La operación $*$: A x A → A donde A = {-1, 0, 1} y $*$ está dada por la Tabla 3.3

*	-1	0	1
-1	1	0	-1
0	0	1	0
1	-1	0	1

Tabla 3.3

Operación Unaria

Definición

Sea A $\neq \varnothing$, se dice que una operación es unaria sobre A si la función tiene dominio en A e imagen en cualquier conjunto.

En particular, se dice que una **operación unaria es cerrada** si su dominio e imagen es A.

$$f\text{: A} \longrightarrow \text{A} \quad /$$

$$f\ (a) = \text{c}$$

Notación

Utilizaremos el símbolo **'** en lugar de f, de la siguiente manera: $f(a) = a' = \text{c}$

$$' : \text{A} \longrightarrow \text{A} \quad /$$

$$a \longrightarrow a'$$

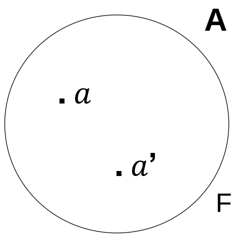

Fig. 4.2. Conjunto A.

Ejemplos

Son operadores unarios:

i) La negación de una proposición
ii) La operación complemento de un conjunto.
iii) La función valor absoluto de un número real.

Actividad 3.2

Determinar si cada uno de los siguientes operadores es cerrado:

a) En $\mathbb{R}^n$, la operación módulo de un vector
b) En $M_{2x3}(\mathbb{R})$, la operación transposición de una matriz
c) En $M_{3x3}(\mathbb{R})$, la operación transposición de una matriz

1.4 Propiedades de una Operación Binaria Cerrada

Propiedad Conmutativa

Definición

Sea (A , $*$) con $*$ una operación binaria cerrada.

Se dice que $*$ es conmutativa en A $\Leftrightarrow$ $\forall$ a, b $\in$ A, a $*$ b = b $*$ a

Ejemplos

a) La adición y la multiplicación son conmutativas en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$.

b) La potenciación en $\mathbb{Z}$ no es conmutativa ya que, por ejemplo: $2^3 \neq 3^2$.

c) Sea A = {a, 0, b} y $\otimes$ dada por la Tabla 3.4 .

$\otimes$	a	0	b
a	b	0	a
0	0	0	0
b	a	0	b

Tabla 3.4

Se tiene que $\otimes$ es conmutativa, pues a $\otimes$ 0 = 0 $\otimes$ a ; a $\otimes$ b = b $\otimes$ a ; 0 $\otimes$ b = b $\otimes$ 0

Observación

Se observa que, si la operación está dada por tabla, es conmutativa si hay simetría respecto de la diagonal.

Propiedad asociativa

Definición

Sea (A , $*$) con $*$ una operación binaria cerrada.

Se dice que $*$ es asociativa en A $\Leftrightarrow$ $\forall$ a, b, c $\in$ A, a$*$(b$*$c) = (a$*$b)$*$c

Observaciones

- Para la demostración de la propiedad asociativa se debe considerar todos los casos posibles. Si |A| = n, el número total de ternas a considerar es n^3.

- Los elementos a, b y c no necesariamente deben ser distintos, por lo que, para probar la asociatividad en conjuntos con menos de 3 elementos se deben tomar ternas repitiendo elementos.

Ejemplos

Las siguientes operaciones son asociativas:

a) La adición y la multiplicación en $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ y $\mathbb{R}$

b) La intersección y unión en el conjunto potencia.

c) La disyunción y la conjunción en el con junto de todas las proposiciones.

Actividad 3.3

Determinar si las siguientes operaciones son conmutativas o asociativas en los conjuntos dados

a) En S = { p / p es una proposición} , las operaciones disyunción excluyente y condicional.

b) En A = {a, b} , la operación $*$: AxA ⟶ A dada por la Tabla 3.5

$*$	a	b
a	b	b
b	a	b

Tabla 3.5

Existencia del elemento neutro

Definición

Sea (A , $*$) con $*$ una operación binaria cerrada.

Se dice que A posee elemento neutro (o elemento identidad) respecto de $*$ ⟺

$$\exists\, e \in A ,\ \forall\, a \in A ,\ e * a = a * e = a$$

Es decir, al operar cualquier elemento del conjunto con el neutro el resultado que devuelve la operación es el elemento original.

Teorema: Unicidad del elemento neutro

Sea $(A , *)$ con $*$ una operación binaria cerrada . Si A posee neutro respecto de $*$, éste es único.

Ejemplos

i) En $\mathbb{Z}$, 0 es el neutro respecto de la operación suma pues

$$x + 0 = 0 + x = x \quad , \quad \forall x.$$

ii) En $\mathbb{Z}$, 1 es el neutro respecto de la operación multiplicación pues

$$x . 1 = 1 . x = x \quad , \quad \forall x.$$

iii) En el conjunto Potencia de X , $\wp(X)$, el neutro respecto de la operación unión es $\varnothing$ y el neutro respecto de la operación intersección es X, que sería en este caso el universo, ya que para cualquier conjunto $A \in \wp(X)$ se tendrá que

$$\varnothing \cup A = A \cup \varnothing = A \qquad y \qquad A \cap X = X \cap A = A$$

iv) La operación potenciación no posee neutro en ningún conjunto numérico dado que no existe un elemento e tal que a.e = e.a = a .

v) En A = {a, 0, b} existe el elemento neutro respecto de $\otimes$ dada por la Tabla 3.6

$\otimes$	a	0	b
a	b	0	a
0	0	b	0
b	a	0	b

Tabla 3.6

Dado que $b \otimes a = a \otimes b = a$, $b \otimes 0 = 0 \otimes b = 0$ y $b \otimes b = b$, entonces el neutro es b.

vi) La Tabla 3.7 define a la operación $\oplus$ la cual no posee elemento neutro en el conjunto A = { a , 0 , b }

$\oplus$	a	0	b
a	a	0	b
0	0	0	a
b	a	0	b

Tabla 3.7

Observación

Cuando el conjunto es finito y la operación se presenta por medio de una tabla, para hallar el elemento neutro se observa si existe un elemento tal que operando por izquierda (ver fila) y por derecha (ver columna) reproduce los encabezados de la tabla.

Existencia de elementos inversos

Definiciones

Sea (A , $*$) con $*$ una operación binaria cerrada con e como su elemento neutro.

- Se dice que a' es el inverso de a respecto de $* \Leftrightarrow$ a $*$ a' = a' $*$ a = e.

- Se dice que A cumple con la propiedad de existencia del inverso si y solo si

$$\forall a \in A , \exists a' \in A \ / \ a * a' = a' * a = e .$$

Ejemplos

i) En $\mathbb{Z}$ existe el inverso respecto de la +. Se le llama inverso aditivo (u opuesto). Simbólicamente:

$$\forall a \in \mathbb{Z} , \exists a'= -a \in \mathbb{Z} \ / \ a + (-a) = (-a) + a = 0$$

ii) En $\mathbb{R} - \{0\}$ existe el inverso respecto de la multiplicación, se le llama inverso multiplicativo (o recíproco). Simbólicamente:

$$\forall a \in \mathbb{R} - \{0\} , \exists a'= 1 / a \in \mathbb{R} - \{0\} \ / \ a . (1/a) = (1/a). a =1$$

iii) En A = { a , 0 , b } y la operación $\otimes$ definida por la Tabla 3.8 donde el elemento neutro es b se tiene que a' = a , 0' = 0 y b' = b, luego se puede decir que el conjunto A cumple con la propiedad de existencia del inverso respecto de $\otimes$.

⊗	a	0	b
a	b	0	a
0	0	b	0
b	a	0	b

Tabla 3.8

👁 **Observaciones**

- Cuando la operación está tabulada, para tener el inverso de cada elemento se detecta en cada fila al elemento neutro. La fila y la columna donde aparece el neutro están señalando a los elementos que son inversos mutuamente.
- Si A respecto de la operación $*$ no posee neutro, entonces tampoco posee elementos inversos.

Actividad 3.4

En cada apartado determinar si el conjunto cumple con la propiedad de existencia del elemento neutro respecto de la operación indicada. En los casos afirmativos investigar si el conjunto cumple con la propiedad de existencia del elemento inverso.

a) En $M_{nxn}(\mathbb{R})$, respecto de la suma y multiplicación usual de matrices

b) En A = {a, 0, b} y la operación binaria $\otimes : AxA \to A$, dada por la siguiente tabla:

⊗	a	0	b
a	a	0	b
0	0	0	a
b	b	a	b

Tabla 3.9

c) En A = { a, b, c } con la operación $*$ dada por la siguiente tabla:

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

Tabla 3.10

Hasta aquí se presentaron las propiedades que pueden cumplir las operaciones cerradas. En el siguiente ejemplo se mostrará que pueden definirse nuevas operaciones a partir de otras ya conocidas.

Ejemplo

En $\mathbb{Z}$ se define la operación $*$ por medio de

$$a * b = a + b + 2 , \text{ donde } + \text{ es la suma usual}$$

¿Cuáles son las propiedades de $*$?

i) ¿Es $*$ una operación cerrada en $\mathbb{Z}$? ¿Se cumple que $\forall$ a, b $\in \mathbb{Z}$, $a * b \in \mathbb{Z}$?

Para la demostración, se toman dos elementos: sean $a \in \mathbb{Z} \wedge b \in \mathbb{Z} \Rightarrow a + b \in \mathbb{Z}$ por ser la suma cerrada en $\mathbb{Z}$. Luego como $2 \in \mathbb{Z} \Rightarrow a + b + 2 \in \mathbb{Z} \Rightarrow a * b \in \mathbb{Z}$. Por lo tanto, la respuesta es sí, la operación $*$ es cerrada en $\mathbb{Z}$.

ii) ¿Es $*$ asociativa en $\mathbb{Z}$?

¿Se cumple que $\forall$ a, b, c $\in \mathbb{Z}$, $a * (b * c) = (a * b) * c$?

Para la demostración, se desarrolla cada miembro de la igualdad a probar:

(I) $a * (b * c) = a * (b + c + 2) = a + (b + c + 2) + 2 = a + b + c + 4$

(II) $(a * b) * c = (a + b + 2) * c = (a + b + 2) + c + 2 = a + b + c + 4$

Las expresiones finales (I) y (II) son iguales. Por lo tanto, $*$ es asociativa en $\mathbb{Z}$.

iii) ¿Es $*$ conmutativa? Para ello se debe analizar si $\forall$ a, b $\in \mathbb{Z}$, $a * b = b * a$

Para la demostración, se desarrolla cada miembro de la igualdad a probar:

(I) $a * b = a + b + 2$

(II) $b * a = b + a + 2 = a + b + 2$ por la propiedad conmutativa de la + en $\mathbb{Z}$.

Las expresiones finales (I) y (II) son iguales. Por lo tanto, $*$ es conmutativa en $\mathbb{Z}$.

iv) ¿Posee $*$ elemento neutro en $\mathbb{Z}$? ¿ $\exists\, e \in Z$, $\forall\, a \in Z$, $e * a = a * e = a$?

Como se sabe que $*$ es conmutativa, se busca el neutro sólo a derecha y el mismo será neutro a izquierda.

$$a * e = a \Rightarrow a + e + 2 = a \Rightarrow e + 2 = 0 \Rightarrow e = -2 \in \mathbb{Z}$$

Por lo tanto – 2 es el elemento neutro respecto $*$ en $\mathbb{Z}$

v) ¿Existe el elemento inverso respecto de $*$ para cada elemento de $\mathbb{Z}$?

Se debe analizar si $\forall a \in \mathbb{Z}, \ \exists a' \in \mathbb{Z}, \ \ a * a' = a' * a = -2$

Como $*$ es conmutativa, se puede buscar el inverso sólo a derecha y el mismo será inverso a izquierda.

$$a * a' = -2 \Rightarrow a + a' + 2 = -2 \Rightarrow a' = -4 - a \in \mathbb{Z}$$

Por ejemplo, 5' = - 9.

La conclusión es que el conjunto $\mathbb{Z}$ posee inverso respecto de la operación $*$.

Observación

Se puede usar la notación $a' = a^{-1}$ para el elemento inverso.

Actividad 3.5

En el conjunto $\mathbb{Z}$ se definen las operaciones $\circ$ y $*$ por medio de

$a \circ b = a + b + a.b$ y $a * b = a + b + 1$ donde '+ ' y '**.**' son las operaciones sumas y productos usuales.

Determinar si

i) $\circ$ y $*$ son operaciones conmutativas y asociativas

ii) En $\mathbb{Z}$ existen elementos neutros y/o inverso respecto de $\circ$ y $*$

Distributividad

Definición

Sea $(A , * , \circ)$ con $*$ y $\circ$ dos operaciones cerradas en A .

Se dice que $\circ$ es distributiva respecto de $*$ en A $\Leftrightarrow$

$\forall$ a, b, c $\in$ A , se cumple que

$a \circ (b * c) = (a \circ b) * (a \circ c)$ (distributiva por izquierda) y

$(b * c) \circ a = (b \circ a) * (c \circ a)$ (distributiva por derecha) y, recíprocamente, se dice que $*$ es distributiva respecto de $\circ$ $\Leftrightarrow$

$a * (b \circ c) = (a * b) \circ (a * c)$ (distributiva por izquierda) y

$(b \circ c) * a = (b * a) \circ (c * a)$ (distributiva por derecha)

Si se cumple que $\circ$ es distributiva respecto de $*$ y que $*$ es distributiva respecto de $\circ$ se dice que $*$ y $\circ$ son mutuamente distributivas

Ejemplos

i) En $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ la multiplicación es distributiva respecto de la adición dado que:

$$x . (y + z) = x . y + x . z , \quad \forall x , y , z$$

$$(y + z) . x = y . x + z . x , \quad \forall x , y , z$$

ii) En el conjunto Potencia de X , $\wp(X)$, la unión y la intersección son distributivas mutuamente ya que:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad , \quad \forall A , B , C \in \wp(X)$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad , \quad \forall A , B , C \in \wp(X)$$

Actividad 3.6

a) En $\mathbb{Z}$ se definen las operaciones “ $\circ$ ” y “$*$” por medio de

$$a \circ b = a + b + a.b \qquad y \qquad a * b = a + b + 1$$

donde ‘+’ y ‘**.**’ son las operaciones sumas y productos usuales.

Determinar si $\circ$ y $*$ son distributivas mutuamente.

b) En A = { 0 , 1 } se definen las operaciones “$\circ$” y “$*$” definidas por las tablas 3.11 y 3.12. Determinar si ”$\circ$” y “$*$” son distributivas mutuamente.

$\circ$	0	1
0	0	1
1	1	1

Tabla 3.11

$*$	0	1
0	0	0
1	0	1

Tabla 3.12

1.5 Principales Estructuras Algebraicas

Las estructuras algebraicas se clasifican según las propiedades que cumplen las operaciones sobre el conjunto donde están definidas. Las principales son:

Monoide

📚 **Definición**

Sea $A \neq \emptyset$. Se dice que $M = (A , *)$ es un monoide si y sólo sí "$*$" es una operación cerrada o ley de composición interna, esto es $* : A \times A \longrightarrow A$

👁 **Observación**

No existe un criterio uniforme en cuanto a la definición de monoide. Claude Chevalley (1909-1984), en *Fundamental Concepts of Algebra* (Conceptos Fundamentales del Algebra-1956), lo introduce como un conjunto en el que se define una ley de composición interna (LCI), asociativa y con elemento neutro. En este curso, adoptamos la definición que expone Enzo R. Gentile, en Estructuras algebraicas (Monografía N° 3 de la O.E.A.-1967) en la que se exigen menos condiciones.

🗒 **Ejemplos**

1) $(\mathbb{N} , +)$ es un monoide mientras que $(\mathbb{N} , -)$ no lo es.

2) $(\mathbb{N} , *)$ donde "$*$" está definida como $a * b = \text{máx} \{a , b\}$ es un monoide.

3) Concatenación de cadenas alfanuméricas: Si consideramos un conjunto (A) de caracteres alfanuméricos, la concatenación de cadenas del alfabeto (A) forma un monoide.

Semigrupo

Definición

Sea A ≠ ∅ y sea ∗ una operación binaria cerrada definida en A.

Se dice que S = (A , ∗) es un Semigrupo si y sólo sí "∗" cumple la siguiente condición:

$$a * (b * c) = (a * b) * c \quad , \ \forall\, a, b, c \in A \ \text{(asociativa)}$$

Observaciones

- Si además "∗" es conmutativa, entonces S = (A, ∗) se dice Semigrupo Conmutativo.
- Si existe el elemento neutro en A respecto de "∗", S = (A, ∗) se dice que es un Semigrupo con Unidad

Ejemplos

i) (ℕ, +) es un Semigrupo Conmutativo.

ii) ($\mathbb{N}_0$, +) es un Semigrupo Conmutativo con Unidad.

iii) (ℕ, .) es un Semigrupo Conmutativo con Unidad.

iv) ($M_{mxn}(\mathbb{R})$, +) , ($\wp(X)$, ∩) y ($\wp(X)$, ∪) son Semigrupos Conmutativos con Unidad.

Actividad 3.7

Determinar en cada caso a que estructura corresponde cada apartado:

a) (P_n, +) donde P_n es el conjunto de polinomios de grado menor o igual que n, con coeficientes reales y + es la operación suma usual de polinomios

b) (A , ∗) siendo A = {1 ,2 , 3 } y "∗" definida por medio de la Tabla 3.13

∗	1	2	3
1	3	2	1
2	2	3	1
3	1	1	1

Tabla 3.13

Grupo

Definición

Sea $A \neq \emptyset$ y sea $*$ una operación binaria cerrada definida en A.

Se dice que $G = (A , *)$ es Grupo si y sólo sí "$*$" cumple las siguientes condiciones:

i) $a * (b * c) = (a * b) * c, \ \forall a, b, c \in A,$ (asociativa)

ii) $\exists e \in A / \ e * a = a * e = a \ , \forall a \in A$ (existencia elemento neutro)

iii) $\forall a \in A , \exists a^{-1} \in A \ / \ a * a^{-1} = a^{-1} * a = e$ (existencia elemento inverso)

Observaciones

- Si además "$*$" es conmutativa entonces $(A; *)$ se dice grupo abeliano (en honor al matemático N. Henrik Abel,1802-1829).
- Si $G = (A, *)$ es un grupo, se dice que es un grupo finito cuando el conjunto A es finito, y su cardinal se dice orden del grupo.

Ejemplos

i) $(\mathbb{Q} - \{0\}, \bullet)$ y $(\mathbb{R} - \{0\}, \bullet)$ son grupos, donde "$\bullet$" es el producto usual.

ii) $(\mathbb{R}, +)$ es un grupo abeliano

iii) $(\mathbb{R} - \{0\}, \bullet)$ es un grupo abeliano

iv) $(\mathbb{N} , +)$ no es grupo, no tiene elemento neutro y por lo tanto tampoco inverso.

v) $(\mathbb{N}_0 , +)$ no es grupo, aunque tiene neutro, pero no tiene inverso aditivo.

Actividad 3.8

¿Es $(M_{2x3}(\mathbb{R}) , +)$ grupo abeliano, donde $M_{2x3}(\mathbb{R})$ es el conjunto de todas las matrices de números reales de orden 2x3 y + es la suma usual? Justificar la respuesta dada.

Propiedades de los grupos

Sea $(A , *)$ un grupo. Entonces se cumple que:

a) Si $*$ posee elemento identidad e, éste es único (Unicidad del elemento identidad)

b) Si $a \in G$ tiene elemento inverso a^{-1}, éste es único (Unicidad del elemento inverso)

c) Propiedad cancelativa:

i) $a * b = a * c \Rightarrow b = c$ (propiedad cancelativa por izquierda)

ii) $b * a = c * a \Rightarrow b = c$ (propiedad cancelativa por derecha)

d) Propiedades del inverso:

i) $(a^{-1})^{-1} = a$

ii) $(a * b)^{-1} = b^{-1} * a^{-1}$

e) Si $a, b \in A$ entonces las ecuaciones del tipo $x * a = b$ y $a * x = b$ admiten solución única en A, y es $x = b * a^{-1}$ (unicidad de la solución de una ecuación)

Ejemplo

Sea el conjunto: $M = \{A \in M^{2x2} |A| \neq 0\}$ y la operación binaria "**.**" (producto habitual de matrices), luego $(M, .)$ es un grupo por lo que son válidas las leyes cancelativas, esto nos permite resolver problemas como el siguiente:

Sean $A, B \in M$ calcular $X \in M$ tal que: $A \,.\, X = B$

Como $(M, .)$ es un grupo existe A^{-1} : $A \,.\, X = B \Longrightarrow A^{-1} \,.\, A \,.\, X = A^{-1} \,.\, B \Longrightarrow X = A^{-1} \,.\, B$

Cómo la matriz A^{-1} es única, la solución de la ecuación, $X = A^{-1} \,.\, B$ es única.

Actividad 3.9

a) Demostrar que $(\mathbb{Z}, *)$ es grupo abeliano, donde "$*$" es la operación definida como $a * b = a + b + 3$

b) Sea $A = \{a, b, c\}$ y las operaciones $*_1$ y $*_2$

$*_1$	a	b	c
a			
b			
c			

Tabla 3.14

$*_2$	a	b	c
a			
b			
c			

Tabla 3.15

i) Completar la Tabla 3.14 de tal modo que A tenga estructura de Grupo respecto de $*_1$ con elemento neutro b y a' = c .

ii) Completar la Tabla 3.15 para que A sea de grupo abeliano respecto de $*_2$ y además las ecuaciones a $*_2$ x = b y c $*_2$ x = a se satisfacen para x = a.

En síntesis:

Dado un conjunto $A \neq \emptyset$ en el que se ha definido una operación binaria $*$, el par $(A,*)$ constituye una estructura algebraica, cuyo nombre depende de las propiedades que deba satisfacer $*$.

- (A, $*$) es un monoide si $*$ es una operación binaria asociativa.
- (A, $*$) es un semigrupo si $*$ es una operación binaria asociativa que posee elemento identidad e.
- (A, $*$) es un grupo si $*$ es una operación binaria asociativa que posee elemento identidad e y además cada elemento a en A tiene inverso a^{-1} en A.
- Si la operación $*$ verifica la propiedad conmutativa se dice que el sistema matemático es abeliano (monoide abeliano, semigrupo abeliano, grupo abeliano)
- De las definiciones de monoide, semigrupo y grupo se desprende que:

  - Todo grupo es también monoide y semigrupo

  - Todo semigrupo es también monoide.

Subgrupo

Definición

Sea (A , $*$) un Grupo y sea B $\subseteq$ A , tal que B $\neq \emptyset$. Se dice que (B ,$*$) es subgrupo de (A , $*$) si y solo sí (B , $*$) es un grupo por sí mismo respecto de la misma operación $*$.

Ejemplos

1) ($\mathbb{Z}$,+) es un subgrupo de ($\mathbb{Q}$, +) , donde + es la suma usual.

2) ($\mathbb{Q}$, +) es subgrupo de ($\mathbb{R}$,+) , donde + es la suma usual.

3) ($\mathbb{Q} - \{0\}$, $\bullet$) es subgrupo de ($\mathbb{R} - \{0\}$, $\bullet$), donde $\bullet$ es la multiplicación usual.

4) Sea H el conjunto de las matrices cuadradas simétricas, (H, +) es un subgrupo de ($\mathbb{R}^{n\,x\,n}, +$) grupo abeliano de las matrices cuadradas $n\ x\ n$, con la adicción usual de matrices.

5) B = {(x, y) $\in$ $\mathbb{R}^2$ / y = 2x}, (B, +) es un subgrupo del grupo abeliano ($\mathbb{R}^2, +$).

Propiedad de los Subgrupos

Sea (A , $*$) un grupo y sea B $\neq \varnothing$ tal que B $\subseteq$ A , entonces B es subgrupo de A si y solo si se verifican:

i) a $*$ b $\in$ B , $\forall$a , b $\in$ B.

ii) a^{-1} $\in$ B , $\forall$a $\in$ B.

Observación

La condición "B $\neq \varnothing$" puede sustituirse por otra condición necesaria, como es que "e $\in$ B", con e: elemento neutro.

Actividad 3.10

Dado el grupo (A , $*$) , donde A = { a , b , c , d } y

"$*$" definida por la Tabla 3.16

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

Tabla 3.16

Demostrar que:

a) B = { a , b } es subgrupo de A.

b) B = { a , b , c } no es subgrupo de A.

Anillo

Definición

Sea $A \neq \emptyset$ y dos leyes de composición interna "$*$" y "$\bullet$" definidas en A.

Sean a , b , c elementos cualesquiera de A. Se dice que $(A , *, \bullet)$ tiene estructura de Anillo si y solo si

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

b) $\exists\, e \in A \,/\, a * e = e * a = a \quad , \forall a$

c) $\forall a , \exists\, a^{-1} \in A \,/\, a * a^{-1} = a^{-1} * a = e$

d) $a * b = b * a$

e) $(a \bullet b) \bullet c = a \bullet (b \bullet c)$

f) $a \bullet (b * c) = (a \bullet b) * (a \bullet c)$ y $(b * c) \bullet a = (b \bullet a) * (c \bullet a)$

Es decir, $(A , *, \bullet)$ es un Anillo si y solo si

i) $(A , *)$ es un Grupo Abeliano ;
ii) $(A , \bullet)$ es un Semigrupo y

iii) La segunda operación "$\bullet$" es distributiva respecto de la primera "$*$".

Si en el anillo $(A , *, \bullet)$ se cumple además que:

- La operación "$\bullet$" es conmutativa entonces $(A , *, \bullet)$ es un anillo conmutativo.

- La operación "$\bullet$" posee elemento neutro en A, entonces $(A , *, \bullet)$ es un anillo con Identidad o anillo con unidad.

Sea A un Anillo con Identidad. Si todo elemento de A distinto de cero es invertible en A respecto de "$*$" entonces $(A , *, \bullet)$ se llama Anillo de División.

Si además se cumple que elementos no nulos de A dan producto no nulo se dice que $(A , *, \bullet)$ es un Anillo sin divisores de cero.

🗒 Ejemplos

Sean los conjuntos numéricos $\mathbb{N}$, $\mathbb{N}_0$ y $\mathbb{Z}$, y sean + y • las operaciones de adición y multiplicación usuales. Se tiene que:

i) ($\mathbb{N}$, + , •) no es un Anillo, pues en $\mathbb{N}$ no existe neutro para la adición.
ii) ($\mathbb{N}_0$, + , •) no es un Anillo, pues $\mathbb{N}_0$ carece de inversos aditivos
iii) ($\mathbb{Z}$, + , •) es un Anillo Conmutativo con Unidad y sin divisores de cero.

👁 Observaciones

- Es usual escribir (A, + , •) para representar a cualquier Anillo, pero "+" y "•" no son forzosamente las operaciones suma y producto usual, salvo que ello esté expresamente indicado.
- El elemento neutro de la operación "+" se representa con el símbolo 0 (cero) y el neutro de la operación "•" con el símbolo 1 (uno) sin que ellos sean necesariamente los números reales 0 y 1.

Actividad 3.11

Sea X = { a , b } y sea A = $\wp(X)$ = { ∅ , {a} , {b} , {a,b} } .

Demostrar que ($\wp(X)$, ⊕ , ∩) es un anillo, donde ⊕, la operación diferencia simétrica y ∩ , la operación intersección están dadas por las tablas 3.17 y 3.18

⊕	∅	{a}	{b}	{a,b}
∅	∅	{a}	{b}	{a,b}
{a}	{a}	∅	{a,b}	{b}
{b}	{b}	{a,b}	∅	{a}
{a,b}	{a,b}	{b}	{a}	∅

Tabla 3.17

∩	∅	{a}	{b}	{a,b}
∅	∅	∅	∅	∅
{a}	∅	{a}	∅	{a}
{b}	∅	∅	{b}	{b}
{a,b}	∅	{a}	{b}	{a,b}

Tabla 3.18

Cuerpo

Definición

Sea $A \neq \emptyset$ y sean dos operaciones binarias cerradas "$*$" y "$\bullet$" definidas en A. Se dice que $(A, *, \bullet)$ es un cuerpo si y solo si

i) $(A, *)$ es un grupo abeliano.

ii) $(A - \{0\}, \bullet)$ es un grupo abeliano, donde 0 es el neutro respecto de "$*$"

iii) "$\bullet$" se distribuye respecto de "$*$".

Es decir, $(A, *, \bullet)$ es un cuerpo si y solo si $(A, *, \bullet)$ es un Anillo Conmutativo, con Unidad y cuyos elementos no nulos admiten inverso multiplicativo.

Ejemplos

i) $(\mathbb{Q}, +, \bullet)$, $(\mathbb{R}, +, \bullet)$ y $(\mathbb{C}, +, \bullet)$ con las operaciones suma y producto usual son cuerpos.

ii) $(\mathbb{Z}, +, \bullet)$ con las operaciones suma y producto usual no es cuerpo, pues $\mathbb{Z}$ carece de inversos multiplicativos.

Actividad 3.12

Determinar si cada uno de los siguientes conjuntos tiene estructura de Cuerpo

a) A es el conjunto de los enteros pares respecto de la suma y producto usuales.

b) A = {0 ,1} y las operaciones "+" y "$\bullet$" definidas por las siguientes tablas:

+	0	1
0	0	1
1	1	0

Tabla 3.19

$\bullet$	0	1
0	0	0
1	0	1

Tabla 3.20

Algebra de Boole

Definición

Un Álgebra Booleana es una estructura matemática conformada por un conjunto B que contiene por lo menos dos elementos que indicamos con 0 y 1, en donde se han definido dos operaciones binarias cerradas, simbolizadas como • y + (que se leen por y más) y una operación unaria ‘ (que se lee como complemento). Simbólicamente la sextupla (B, +, •, ‘, 0, 1) es un algebra de boole (en honor a George Boole 1813-1864) si tomando elementos cualesquiera a, b y c del conjunto B, se cumplen las siguientes propiedades o axiomas:

1) Leyes asociativas	
$x + (y + z) = (x + y) + z$	$x \bullet (y \bullet z) = (x \bullet y) \bullet z$
2) Leyes conmutativas	
$x + y = y + x$	$x \bullet y = y \bullet x$
3) Leyes distributivas	
$x + y \bullet z = (x + y) \bullet (x + z)$	$x \bullet (y + z) = x \bullet y + x \bullet z$
4) Leyes de identidad (o de elemento neutro)	
$\exists\, 0 \in B \,/\, \forall x \in B \quad , \quad x + 0 = 0 + x = x$	$\exists\, 1 \in B \,/\, \forall x \in B \quad , \quad x \bullet 1 = 1 \bullet x = x$
5) Leyes de complementariedad	
$\forall x \in B, \exists\, x' \in B \;\;/\;\; x + x' = x' + x = 1$	$\forall x \in B, \exists\, x' \in B \;\;/\;\; x \bullet x' = x' \bullet x = 0$

Observaciones

- Por convención habitual (si no existen paréntesis), la operación unaria tiene prioridad sobre •, y • tiene prioridad sobre **+**. Por ejemplo: $x + y \bullet z = x + (y \bullet z)$ y $x \bullet y' = x \bullet (y')$.

- El uso del “0” y del “1” es simplemente simbólico (no necesariamente tienen que ver con los números cero y uno. Comentario análogo para los símbolos “+” y “•”

Ejemplos

a) Sea $X \neq \varnothing$ Y finito y sea $\wp(X)$ el conjunto potencia de X. Entonces ($\wp(X)$, $\cup$, $\cap$) constituye un Álgebra Booleana.

Como caso particular si $X = \{a,\ b,\ c\}$, $\wp(X) = \{\emptyset\ ,\{a\},\ \{b\},\ \{c\},\ \{a,b\},\ \{a,c\},\ \{b,c\},\ X\}$ entonces ($\wp(X)$, $\cup$, $\cap$) es un Álgebra de Boole donde $\emptyset$ y X son los neutros respecto de la unión e intersección respectivamente, y los complementos son:

$\emptyset' = X$ y $X' = \emptyset$ pues: $\emptyset \cup X = X$ y $\emptyset \cap X = \emptyset$

$\{a\}' = \{b,c\}$ y $\{b,c\}' = \{a\}$ ya que $\{a\} \cup \{b,c\} = X$ y $\{a\} \cap \{b,c\} = \emptyset$

$\{b\}' = \{a,c\}$ y $\{a,c\}' = \{b\}$ ya que $\{b\} \cup \{a,c\} = X$ y $\{b\} \cap \{a,c\} = \emptyset$

$\{c\}' = \{a,b\}$ y $\{a,b\}' = \{c\}$ ya que $\{c\} \cup \{a,b\} = X$ y $\{c\} \cap \{a,b\} = \emptyset$

b) Sea D_{30} = {1,2,3,5,6,10,15,30}, el conjunto de los divisores positivos de 30 donde definimos las leyes de composición interna, adición y multiplicación como:

$x + y = mcm\{x, y\};\quad x * y = mcd\{x, y\}.$

Las tablas de las operaciones “+” y “$*$” serían las siguientes:

+	**1**	**2**	**3**	**5**	**6**	**10**	**15**	**30**
1	1	2	3	5	6	10	15	30
2	2	2	6	10	6	10	30	30
3	3	6	3	15	6	30	15	30
5	5	10	15	5	30	10	15	30
6	6	6	6	30	6	30	30	30
10	10	10	30	10	30	10	30	30
15	15	30	15	15	30	30	15	30
30	30	30	30	30	30	30	30	30

Tabla 3.21

$*$	**1**	**2**	**3**	**5**	**6**	**10**	**15**	**30**
1	1	1	1	1	1	1	1	1
2	1	2	1	1	2	2	1	2
3	1	1	3	1	3	1	3	3
5	1	1	1	5	1	10	5	5
6	1	2	3	1	6	2	3	6
10	1	2	1	10	2	10	5	10
15	1	1	3	5	3	5	15	15
30	1	2	3	5	6	10	15	30

Tabla 3.22

Observemos que los neutros son: 1 para la operación “+” y 30 para la operación “$*$”.

Los complementos de: 1´ = 30 y 30´=1 pues: 1 + 30 = 30 y 1 $*$ 30 = 1,

2´ = 15 y 15´ = 2 pues: 2 + 15 = 30 y 2 $*$ 15 = 1, 3´ = 10 y 10´ = 3 pues: 3 + 10 = 30 y 3 $*$ 10 = 1,

5´ = 6 y 6´ = 5 pues: 5 + 6 = 30 y 5 $*$ 6 = 1.

c) Sea B^n el conjunto de las sucesiones de n-bits. B^n es un álgebra de Boole definiendo la suma de dos elementos a y b como el elemento a+b que contiene un 1 en una cierta posición si a o b tienen un 1 en esa misma posición, y el producto de a y b como el elemento a•b que tiene un 1 en una cierta posición si ambos, a y b, tienen un 1 en esa misma posición. El complemento de a, denotado por a', contiene un 1 si a contiene un 0.

(B^n, +, •) es el álgebra de Boole de las secuencias de n bits, definiendo 0 como la secuencia de n bits iguales a cero y 1 como la secuencia de n bits iguales a 1.

Observaciones

En general nos referiremos a $\mathrm{D}_n = \{\, \mathrm{x} \in \mathbb{N}\,,\ \ \mathrm{x}\,|n\}$ como el conjunto de los divisores positivos de $n \in \mathbb{N}$. Definiendo las operaciones "+" y "$*$" como:

$x + y = mcm\{x, y\}$; $x * y = mcd\{x, y\}$ se genera la estructura (D_n , + , $*$).

De aquí surge la pregunta ¿Para qué valores de n, D_n es un álgebra de Boole?

Teorema

D_n es un Álgebra Booleana si y solo sí $n = p_1 . p_2 \ldots\ldots p_k$ donde $p_1, p_2, \ldots\ldots, p_k$ son números primos distintos.

Ejemplos

i) D_6 es algebra booleana pues 6 = 2.3
ii) D_{20} no es algebra booleana pues 20 = 2.2.5
iii) D_{30} es algebra booleana pues 30 = 2.3.5
iv) D_{1848} no es algebra booleana pues 1848 = 2^3 .3 . 7.11

Teorema

En un Álgebra de Boole B, se cumplen las siguientes propiedades para todos sus elementos a y b cualesquiera:

1) Leyes idempotencia	
$(a + a) = a$	$(a \bullet a) = a$
2) Leyes de acotación	
$a + 1 = 1$	$a \bullet 0 = 0$
3) Leyes de absorción	
$a + (a \bullet b) = a$	$a \bullet (a + b) = a$
4) Leyes de complementos de los neutros	
$0' = 1$	$1' = 0$
Leyes de De Morgan	
$(a + b)' = a' \bullet b'$	$(a \bullet b)' = a' + b'$
Ley de involución	
$(a')' = a$	

Actividad 3.13

a) Sea $B = \{0, 1\}$ y las operaciones "+" y "•" definidas por las tablas 3.23 y 3.24 Demostrar que $(B, +, \bullet)$ tiene estructura de Algebra de Boole.

+	0	1
0	0	1
1	1	1

Tabla 3.23

•	0	1
0	0	0
1	0	1

Tabla 3.24

b) Determinar si los siguientes conjuntos son Algebras de Boole: D_{21}, D_{25}, D_{40}, D_{60}, D_{105}