Lógica y Matemática Computacional
Licenciatura en Sistemas de Información

Estructuras Algebraicas Finitas

Ing. JULIO C. ACOSTA

Facultad de Ciencias Exactas y Naturales y Agrimensura - UNNE

Unidad III. Estructuras algebraicas finitas. - Leyes de composición interna.

- Propiedades.
- Monoide.
- Semigrupo.
- Semigripo con unidad.
- Grupo.
- Grupo Abeliano.
- Subgrupo.
- Anillo.
- Anillo con unidad.
- Cuerpo.

Leyes de composición interna

Dado un conjunto A y una operación +
(+ no es necesariamente suma aditiva)

y el par (A,+)

+ es una ley de composición interna interna en A
si es una aplicación de la siguiente forma :

+: A x A −> A

(a, b) −> $c = a + b$

$\forall (a,b) \in A \times A, \qquad \exists!\, c \in A \ : \qquad c = a + b$

Sea K = { 0, 1 } y + definida según las siguientes tablas, diga en cada caso si (K, +) es LCI

+	0	1
0	0	1
1	1	0

(K, +) es L. C. I.

+	0	1
0	0	0
1	0	1

(K, +) es L. C. I.

+	0	1
0	2	0
1	0	1

(K, +) NO es L. C. I.

Propiedad Asociativa

Definida una LCI en el par (A, +) ; + es asociativo si

$$\forall a, b, c \in A : \ (a + b) + c = a + (b + c)$$

Si A = { x / x = 2^k, k $\in$ Z } ; + es el producto ordinario

$2^k + (2^t + 2^s) = 2^k \cdot (2^t \cdot 2^s) = 2^k \cdot 2^{(t+s)} = 2^{k+(t+s)}$

$= 2^{(k+t)+s} = 2^{(k+t)} \cdot 2^s = (2^k \cdot 2^t) \cdot 2^s = (2^k + 2^t) + 2^s$

$2^k + (2^t + 2^s) = (2^k + 2^t) + 2^s$

Elemento neutro

Definida una LCI en el par (A, +) ; A con +

tiene elemento neutro e si se cumple:

$$\exists e \in A \,/\, \forall a \in A : \; a + e = e + a = a$$

Si A = { x / x = 2^k, k $\in$ Z } ; + es el producto ordinario

Para cada 2^k debe existir $2^t = e$ con t $\in$ Z

$$2^k \cdot e = 2^k \cdot 2^t = 2^{(k+t)} = 2^k$$

$\Rightarrow$ k + t = k entonces t = 0 0 $\in$ Z

Si $A = \{ x / x = 3k , k \in N \}$; + es la adición

Si existe e (neutro) en A, tendrá la forma $e = 3t$; $t \in N$

$3k + 3t = 3k$ si $3t = e$

Entonces $3k + 3t = 3(k + t) = 3k$

Luego $(k+ t) = k \rightarrow t = 0$

pero $0 \notin N$ entonces . . .

NO Existe Elemento Neutro en A para +

Elemento simétrico (o inverso)

Definida una LCI en el par (A, +) ; A con +

tiene elemento simétrico $a`$ si se cumple:

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

Si A = { x / x $\in$ Z } ; + es la adición

Asumimos que existe $e = 0$ (neutro) en A,

$a + b = e$ si $b = -a$

$Si \quad a \in A \quad \rightarrow -a \in A$

Si A = { x / x $\in$ N } ; + es la adición

Asumimos que existe $e = 0$ (neutro) en A,

$a + b = e$ si $b = -a$

$Si \quad a \in A \quad \rightarrow \quad -a \notin A$

No se verifica la existencia de simétrico en A para la operación +

Propiedad conmutativa

Definida una LCI en el par (A, +) ; A con +

+ es operador conmutativo en A si se cumple:

$$\forall a, b \in A: \quad a + b = b + a$$

Si A = { x / x ∈ N } ; + es la suma ordinaria

$$a + b = b + a$$

Si A = { x / x ∈ N } ; + es el producto ordinario

$$a + b = b + a$$

Si A = { x / x ∈ Z } ; + es el cociente

$$a / b \neq b / a$$

NO es conmutativa

Monoide

Monoide es todo par (A,+)

A es un conjunto no vacío

+ es una ley de composición interna definida en A

(N, +) ; +: suma aditiva

(N, +) ; +: producto ordinario

(N, +) ; +: diferencia

(P(gr(n)), +) ; +: suma de polinomios

Semigrupo

(A, +) es semigrupo si:

1) Monoide (L.C.I.) $A^2 \rightarrow A$ + es una LCI

2) +: es Asociativo en A interna en A

$$\forall a,b,c : a, b, c \in A \Rightarrow (a + b) + c = a + (b + c)$$

(N, +) + es suma aditiva

(Z, +) + es suma aditiva

(P(x), +) + intersección de conjuntos

(P(x), +) + unión de conjuntos

Semigrupo con Unidad

(A, +) es semigrupo con unidad si:

1) Monoide (L.C.I.) $A^2 \rightarrow A$ + es una LCI

2) +: es Asociativo en A interna en A

$$\forall a,b,c : a, b, c \in A \Rightarrow (a + b) + c = a + (b + c)$$

3) Existe Elemento Neutro: Definida una operación + si en el conjunto A existe al menos un elemento "*e*", que al operarlo con cualquier otro elemento "*a*" de A resulta el mismo elemento "

$$\exists e \in A / \forall a : a \in A \Rightarrow a * e = e * a = a$$

$(N_0, +)$ + es suma aditiva

$A^2 \rightarrow A$ + es una LCI interna en A

$\forall a,b,c : a, b, c \in A \Rightarrow (a + b) + c = a + (b + c)$

$\exists e=0 \in A / \forall a : a \in A \Rightarrow a * e = e * a = a$

$(N_0, +)$ es Semigrupo con Unidad

$(N, +)$ + es suma aditiva

$A^2 \rightarrow A$ + es una LCI interna en A

$\forall a,b,c : a, b, c \in A \Rightarrow (a + b) + c = a + (b + c)$

$e=0$ NO pertenece al conjunto A – NO HAY NEUTRO

$(N, +)$ NO es Semigrupo con Unidad

Grupo

(A, +) es semigrupo con unidad si:

1) Monoide (L.C.I.) $A^2 \rightarrow A$ + es una LCI interna en A

2) +: es Asociativo en A

$$\forall a,b,c : a, b, c \in A \Rightarrow (a + b) + c = a + (b + c)$$

3) Existe Elemento Neutro

$$\exists e \in A / \forall a : a \in A \Rightarrow a * e = e * a = a$$

4) Existe Elemento Inverso: Definida + si para cada elemento de A existe al menos un elemento a' que al operar con a dá como resultado el neutro e

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

Grupo Abeliano

Grupo Abeliano es un Grupo conmutativo

1) Monoide (L.C.I.)

2) +: es Asociativo en A

$$\forall a,b,c : a, b, c \in A \Rightarrow (a + b) + c = a + (b + c)$$

3) Existe Elemento Neutro

$$\exists e \in A / \forall a : a \in A \Rightarrow a * e = e * a = a$$

4) Existe Elemento Inverso

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

5) Propiedad conmutativa

$$\forall a,b : a, b \in A \Rightarrow a * b = b * a$$

Si A = { 1; -1 } ; + es el producto ordinario

1)

$1 \cdot 1 = 1 \in A$ $-1 \cdot 1 = -1 \in A$

$-1 \cdot -1 = 1 \in A$ $1 \cdot -1 = -1 \in A$

Se verifica que + es L.C.I. en A

2) Podemos admitir que la Asociatividad "se hereda" de la asociatividad del producto entre elementos del conjunto de los números enteros

3) Sabemos que para el producto existe neutro en Z, pero debemos verificar que ese neutro $\in$ A

$-1 \cdot e = -1 \rightarrow e = 1$

$1 \cdot e = 1 \rightarrow e = 1$

$1 \in A$

Existe neutro

4) Analizamos si cada elemento de A admite inverso en A

$1 \cdot x = e = 1 \quad \rightarrow \quad x = 1$

$-1 \cdot x = e = 1 \quad \rightarrow \quad x = -1$

Los elementos de A admiten inverso

5) Podemos admitir que la Conmutatividad "se hereda" de la conmutatividad del producto entre elementos del conjunto de los números enteros

El par (A, +) ES grupo abeliano

Si A = { 1; -1 } ; + es el producto ordinario

Repaso

(A, +)

A es un conjunto no vacío

+ es un operador de una operación binaria definida en A

L.C.I en A

+ es Asociativo en A

Semi-grupo

Hay elemento neutro en A para +

Semigrupo con unidad

Hay elemento inverso en A para +

Grupo

+ es Conmutativa en A

Grupo Abeliano

Analice la Estructura algebraica del par (A,+) donde:

1) A es el conjunto de las matrices cuadradas de clase *n* x *n*
   + es la suma de matrices

   (K^{nxn}, +)

2) A es el conjunto de las matrices cuadradas de clase *2* x *2*
   + es la suma de matrices

   (K^{2x2}, +)

3) A es el conjunto de las matrices cuadradas de clase *2* x *2* del tipo:

$$M = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

   + es el producto ordinario de matrices

   (K^{2x2} - {$[0]^{2x2}$}, +)

Subgrupos

Sea (A, +) Un conjunto no vacío S es subgrupo de A cuando S es grupo con el operador +

Sea (A, +) un Grupo, y S incluido en A, S no vacío

El Grupo (S, +) es SubGrupo de (A, +) si:

S contiene el elemento identidad de A $e \in S$

\+ es cerrada en S $\forall a, b \in S : \quad a + b \in S$

S contiene los simétricos

$$\forall a \in S, \exists a' \in S \; / \; a + a'' = a' + a = e$$

Propiedades de los Subgrupos

1) Todo Grupo A, tiene al menos dos sub grupos

$$S_1 = \{ e \}$$

$$S_2 = A$$

2) Transitividad de los subgrupos

Sean S_1 , S_2 y S_3 subgrupos de A

Si S_1 es subgrupo de S_2 y S_2 es subgrupo de S_3

entonces: S_1 es subgrupo de S_3

3) La intersección de dos subgrupos es un subgrupo

Sean S y S` dos subgrupos de A

$$e \in S \ \wedge \ e \in S` \ \rightarrow \ S \cap S` = \{e\}$$

Ejemplos

1) Sea el Grupo (A, +) donde A = Z ; + es la suma aditiva

Proponga subgrupos de A y analice como se cumplen las propiedades

2) Sea el Grupo (A, +)

Si $A = \{ x / x = 2^k, k \in Z \}$; + es el producto ordinario

Proponga subgrupos de A y analice como se cumplen las propiedades

Grupos Finitos

Sea (G, +) un grupo finito, G es un conjunto finito.

Orden de G es el número de elementos de G

G = { e }

+	e
e	e

G = { e, a }

Si llenamos el casillero con a, no se cumple la unicidad del neutro, por tanto debe ser llenado con e

+	e	a
e	e	a
a	a	e

No se deben repetir elementos en la misma línea para no perder la unicidad del neutro...

G = { *e*, *a*, *b* }

+	***e***	***a***	***b***
e	*e*	*a*	*b*
a	*a*	*b*	*e*
b	*b*	*e*	*a*

G = { *e*, *a*, *b*, *c* }

+	***e***	***a***	***b***	***c***
e	*e*	*a*	*b*	*c*
a	*a*	*e*	*b*	*c*
b	*b*	*c*	*e*	*a*
c	*c*	*b*	*a*	*e*

+	***e***	***a***	***b***	***c***
e	*e*	*a*	*b*	*c*
a	*a*	*e*	*b*	*c*
b	*b*	*c*	*a*	*e*
c	*c*	*b*	*e*	*a*

Anillo

Sea una estructura algebraica definida en un conjunto G con dos leyes de composición * y •

(A, + •) es Anillo

1) (A, +) es Grupo abeliano
2) (A, •) es semi Grupo
3) • es distributivo a izquierda y derecha respecto de *

$\forall a, \forall b, \forall c \in G$: $a \bullet (b + c) = (a \bullet b) + (a \bullet c)$

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

Si la segunda ley de composición es conmutativa,

(A, + •) es Anillo Conmutativo

Sea la estructura (A, +, •)

Donde A = Z

\+ es la suma aditiva

• es el producto ordinario

(A, +) es Grupo Abeliano

(A, •) es Grupo semigrupo

• es doblemente distributivo respecto de +

(A, +, •) es anillo conmutativo

(A, •) además es conmutativo

(A, +, •) es anillo conmutativo

Si $(A, +, \bullet)$ es Anillo

Y además posee elemento neutro respecto de $\bullet$

$(A, +, \bullet)$ es Anillo con Unidad

Un Anillo con unidad cuyos elementos no nulos son inversibles se llama **Anillo con división**

$(A, +)$ es Grupo Abeliano

$(A - \{0\}, \bullet)$ es Grupo

- es doblemente distributivo respecto de +

Ejercicio: Analice $(Z, + \bullet)$ donde + es la adición (suma) y $\bullet$ es el producto ordinario

Ejercicio: Analice el Anillo de las matrices cuadradas (A, +, •) con los operadores suma y producto respectivamente

Si un Anillo con división es conmutativo, se llama **Cuerpo**

1) (A, +) es Grupo abeliano

2) (A – {0}, •) es Grupo abeliano

3) • es distributivo respecto de +

Ejemplo: (Z, * •) donde * es la adición (suma) y • es el producto ordinario

No es cuerpo, pues los únicos elementos no nulos que admiten inverso multiplicativo son 1 y - 1

(R, * •) donde * es la adición y • es el producto ordinario

Es Cuerpo

FIN