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

Leyes de composición interna

¿qué es una ley de composición interna?

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

+	0	1
0	0	1
1	1	0

+	0	1
0	2	0
1	0	1

+	0	1
0	0	0
1	0	1

¿Cuántas LCI pueden establecerse en el conjunto A ={0, 1}?

+	0	1
0	0	1
1	1	0

$$A_{4,r}^{2} = 2^{4} = 16$$

(0,0,0,0); (1,1,1,1)

(0,0,0,1); (0,0,1,0); (0,1,0,0); (1,0,0,0)

(1,1,1,0); (1,1,0,1); (1,0,1,1); (0,1,1,1)

(0,0,1,1); (0,1,1,0); (1,1,0,0); (1,0,0,1); (0,1,0,1); (1,0,1,0)

¿Cuántas LCI pueden establecerse en el conjunto A ={0, 1, 2}?

Propiedad Asociativa

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

Ejemplo:

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

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

Ejemplos

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 $t = 0$ $0 \in Z$

Proponga ejemplos de conjuntos y operaciones donde existe elemento neutro y donde no existe elemento neutro

Elemento simétrico (o inverso)

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

Ejemplo:

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

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

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

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

Proponga ejemplos de conjuntos y operaciones donde existe elemento inverso y donde no existe elemento inverso

Propiedad conmutativa

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

Diga en cada caso si se verifica la propiedad conmutativa para el par (A,+)

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

Si A = { x / x $\in$ N } ; + es el producto ordinario

Si A = { x / x $\in$ Z } ; + es el cociente

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

Resuelva las siguientes operacipnes de matrices

Sea M el conjunto de matrices de clase 2x3 donde sus elementos son 0 y/o 1, que representan valores de verdad del algebra proposicional; y sea + una operación proposicional determinada; diga si son monoides:

Ejemplos

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \quad B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

(M, +) ; +: disyunción

$$A \vee B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \vee \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 \vee 1 & 0 \vee 1 & 0 \vee 1 \\ 0 \vee 1 & 0 \vee 0 & 1 \vee 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

(M, +) ; +: conjunción

$$A \wedge B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \wedge \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 \wedge 1 & 0 \wedge 1 & 0 \wedge 1 \\ 0 \wedge 1 & 0 \wedge 0 & 1 \wedge 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Propiedades

Sea: A un conjunto no vacío

+: A x A → A una función

1) Si existe un neutro en A para +, éste es único

2) Sea +: A x A → A asociativa y e pertenece al conjunto A

Si $\boldsymbol{a}$ poseee inverso en A, este inverso es único

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 (G, +) donde:

G = R - {0}

$$+: \; a + b = \frac{a \cdot b}{2}$$

G = R

$$+: \; a + b = a + b + 2$$

G = R - { -1 }

$$+: \; a + b = a + b + a \cdot b$$

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...

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

$G = \{ e, a, b \}$

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

No se deben repetir elementos en las filas ni en las columnas porque no se cumpliría la unicidad del neutro

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

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

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

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

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

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

$a \in A$ Es **regular o simplificado** si:

$$a + a_1 = a + a_2 \rightarrow a_1 = a_2 \quad \forall a_1, a_2 \in A$$

y

$$a_1 + a = a_2 + a \rightarrow a_1 = a_2 \quad \forall a_1, a_2 \in A$$

Propiedades

Sea (G,+) grupo, entonces:

1) El neutro es único. El inverso de cada elemento es único

2) Los elementos de G son regulares

3) Las ecuaciones $x + a = b$ $\quad a + x = b$, $\quad \forall a, b, x \in G$

admiten solución única en G

4) $\forall x \in G: (x')' = x$

5) $\forall x, y \in G: (x + y)' = y' + x'$

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

3) Muestre algunos subgrupos posibles del Grupo $(\Sigma^3, +)$.

Si $\Sigma=\{0,1\}$; $\Sigma^3=\{000,001,010,100,011,101,110,111\}$

+ Se define: $(x_1x_2x_2)+(y_1y_2y_3) = (x_1+y_1, x_2+y_2, x_3+y_3)$

	000	001	010	100	011	101	110	111	
000	000	001	010	100	011	101	110	111	
001	001	000	011	101	010	100	111	110	
010	010	011	000	110	001	111	100	101	
100	100	101	110	000	111	001	010	011	
011	011	010	001	111	000	110	101	100	
101	101	100	111	001	110	000	011	010	
110	110	111	100	010	101	011	000	001	
111	111	110	101	011	100	010	001	000	

Los invito a programar para nxn

Los invito al mismo ejemplo pero cambiando el operador

Los invito a programar para nxn y para cualquier operador….

4) Consideremos en $\Sigma = \{0, 1\}$ las siguientes leyes de composición interna representadas con + y .

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

y una función inyectiva e: $\Sigma^2 \rightarrow \Sigma^5$ / e(x) = x M

x pertenece a Σ^2

x M es el producto matricial de x por la matriz M

$$M = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

		1	0	1	1	0
		0	1	0	1	1
0	0	0	0	0	0	0
0	1	0	1	0	1	1
1	0	1	0	1	1	0
1	1	1	1	1	0	1

$$
\begin{aligned}
00 &\rightarrow 00000 \\
01 &\rightarrow 01011 \\
10 &\rightarrow 10110 \\
11 &\rightarrow 11101
\end{aligned}
$$

+	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

+	00000	01011	10110	11101
00000	00000	01011	10110	11101
01011	01011	00000	11101	10110
10110	10110	11101	00000	01011
11101	11101	10110	01011	00000

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

(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

Anillos Finitos

G = { *e* }

(G, +, *)
Anillo

+	*e*
e	*e*

•	*e*
e	*e*

G = { *e*, *a* }

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

•	*e*	*a*
e	*e*	*e*
a	*e*	*e*

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

•	*e*	*a*
e	*e*	*e*
a	*e*	*a*

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

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

•	***e***	***a***	***b***
e	*e*	*e*	*e*
a	*e*	*e*	*e*
b	*e*	*e*	*e*

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

•	***e***	***a***	***b***
e	*e*	*e*	*e*
a	*e*	*a*	*b*
b	*e*	*b*	*a*

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

•	***e***	***a***	***b***
e	*e*	*e*	*e*
a	*e*	*b*	*a*
b	*e*	*a*	*a*

FIN