Tema 1

Estructuras algebraicas

1.1 Álgebras binarias

Sea A un conjunto no vacío, una ***operación binaria*** (u operación interna) en A es una aplicación

$$*: A \times A \longrightarrow A$$
$$(x, y) \longrightarrow x * y$$

es decir, una regla que a cada par de elementos x, y de A les asocia un único elemento de A, denotado por $x * y$.

Un conjunto con una o más operaciones internas se llama álgebra binaria, ***estructura algebraica*** o sistema algebraico, y se denota (A, *, #, ...). El tipo o clase de estructura se caracterizará atendiendo a las propiedades que verifiquen las operaciones definidas en el conjunto.

Ejemplos

1. La suma y producto usuales en N, Z, Q, R y C son operaciones internas y, de hecho, son el modelo en el que se apoya la noción de operación interna.

2. La unión y la intersección son operaciones internas en $\mathbf{P}(X)$.

3. La composición es una operación interna en X^X, siendo

$$X^X = \{f: X \to X / \ f \text{ aplicación}\}$$

4. En $R^* = R - \{0\}$, $x * y = x/y$ es una operación interna, mientras que en $Z^* = Z - \{0\}$, $x * y = x/y$ no lo es.

5. En N, $x * y =$ (un número natural menor que x, y) no es una operación, pues * no es aplicación.

Si el conjunto A es finito, $A = \{a_1, a_2, \dots, a_n\}$ una operación binaria en A puede definirse mediante una tabla:

$*$	a_1	...	a_j	...	a_n
a_1	$a_1 * a_1$	...	$a_1 * a_j$	...	$a_n * a_j$
:	:		:		:
a_i	$a_i * a_1$	...	$a_i * a_j$	...	$a_i * a_n$
:	:		:		:
a_n	$a_n * a_1$	...	$a_n * a_j$	...	$a_n * a_n$

Ejemplo

Si se considera el conjunto de las permutaciones de orden 3, $S_3 = \{1, \alpha, \beta, \gamma, \delta, \varepsilon\}$, con la operación composición, que está reflejada en la tabla:

$$1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} \quad \alpha = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$$

$$\beta = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \quad \gamma = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

$$\delta = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} \quad \varepsilon = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$$

Nota: $\delta = \alpha \circ \beta$

$\circ$	1	α	β	γ	δ	ε
1	1	α	β	γ	δ	ε
α	α	1	δ	ε	β	γ
β	β	γ	1	α	ε	δ
γ	γ	β	ε	δ	1	α
δ	δ	ε	α	1	γ	β
ε	ε	δ	γ	β	α	1

1.2 Propiedades de las operaciones binarias

Sea $*$ una operación interna en A. Se dice que:

1. $*$ es ***asociativa*** si $(a * b) * c = a * (b * c)$, $\forall a, b, c \in A$

2. $*$ es ***conmutativa*** si $a * b = b * a$, $\forall a, b \in A$

3. $*$ tiene elemento ***neutro*** si $\exists\ e \in A$ tal que $a * e = a = e * a$, $\forall a \in A$

- ♦ Si $*$ tiene elemento neutro (o identidad), es único. Pues si e, e' son neutros de $*$, entonces $e = e * e' = e'$.

4. supuesto que exista elemento neutro e, un elemento $a \in A$ tiene ***inverso*** (o simétrico) si $\exists\ a' \in A$ tal que $a * a' = e = a' * a$

♦ Si $*$ es asociativa y a tiene inverso, éste es único. Pues si a' y a'' son inversos de a, $a' = a'*e = a'*(a*a'') = (a'*a)*a'' = e*a'' = a''$.

El inverso de a se representa por a^{-1}

5. un elemento $a \in A$ es regular o ***simplificable*** si $\forall$ b, c $\in$ A

$(a * b = a * c \Rightarrow b = c) \quad \wedge \quad (b * a = c * a \Rightarrow b = c)$

♦ Si $*$ es asociativa y a tiene inverso, a es simplificable

6. un elemento $a \in A$ es idempotente si $a * a = a$

7. $*$ es distributiva respecto a otra operación interna # en A si, $\forall a, b, c \in A$

$a * (b \# c) = (a * b) \# (a * c) \quad \wedge \quad (b \# c) * a = (b * a) \# (c * a)$

Notas

1. Si $*$ es asociativa, se puede escribir $a * b * c$ en lugar de $a * (b * c)$, pues $(a * b) * c = a * (b * c)$ y no crea confusión. En general, escribiremos $a_1 * a_2 * ... * a_n$ pues se operan agrupándolos de dos en dos de cualquier forma (manteniendo el orden de los elementos).

2. El elemento $a * a * ... * a$ (n veces) se escribe a^n

3. Con notación aditiva, el simétrico de un elemento a se llama opuesto y se representa por $-a$, y $a + a + ... + a$ (n veces) puede denotarse na.

Ejemplos

1. En (N, +), (N, ·), (Z, +), (Z, ·), (Q, +), (Q, ·), (R, +), (R, ·) las operaciones indicadas son asociativas, conmutativas y · es distributiva respecto a +

2. En P(X) la unión y la intersección son operaciones internas asociativas, conmutativas, tienen elemento neutro (Ø y X, respectivamente), y ese elemento es el único simplificable e inversible con la operación correspondiente.

3. En $X^X = \{ f: X \to X / f \text{ aplicación}\}$ la composición es una operación interna asociativa, no conmutativa, donde el elemento neutro es la aplicación identidad de X y sólo tienen inverso las aplicaciones biyectivas.

4. En N, la operación $n * m = n(n + m)$ no es asociativa, ni conmutativa.

5. En el conjunto de cadenas finitas de 0's y 1's la concatenación es una operación interna asociativa con elemento neutro la secuencia vacía.

1.3 Subestructuras

Si (A, $*$) es una estructura algebraica y B un subconjunto no vacío de A, se dice que B es cerrado para $*$ si:

$$\forall x, y \in B,\ x * y \in B$$

En este caso, (B, $*$) es una estructura algebraica, que se llama ***subestructura*** de (A, $*$).

Ejemplos

1. El conjunto P de los enteros pares es una subestructura de (Z, +), pero P' no lo es.

2. En (Z, $\cdot$), P y P' son subestructuras.

3. El conjunto $\{x \in R \ / \ x \geq 0\}$ es subestructura de (R, $\cdot$), pero no lo es $\{x \in R \ / \ x < 0\}$

4. En (X^X, $\circ$), la operación composición es interna en los subconjuntos $B_1 = \{f \ / \ f \text{ inyectiva}\}$, $B_2 = \{f \ / \ f \text{ sobreyectiva}\}$ y $B_3 = \{f \ / \ f \text{ biyectiva}\}$.

1.4 Relaciones de congruencia y estructura cociente

En el conjunto Z se ha visto cómo la relación "ser congruente módulo m", para un entero $m \geq 1$, es compatible con la operación suma. Esto ha permito definir en el conjunto cociente Z_m la operación suma módulo m

$$[a] + [b] = [a + b]$$

sin que dependa del representante elegido.

En general, si $\sim$ es una relación de equivalencia en un conjunto A con una operación interna $*$, se dice que $\sim$ es compatible con la operación $*$ (o que $\sim$ es una congruencia) si

$$\forall x, x', y, y' \in A, \quad x \sim x' \wedge y \sim y' \Rightarrow x * y \sim x' * y'$$

Asimismo se dice que $\sim$ es una relación de congruencia en la estructura algebraica (A,$*$). En este caso, $[a] * [b] = [a * b]$ define una operación interna en

el conjunto cociente A/~ (está bien definida, es decir, el resultado no depende del representante elegido) y (A/~, *****) es una estructura algebraica que "hereda" las propiedades de (A, *):

a. Si * es asociativa (o conmutativa) en A, ***** también lo es en A/~

b. Si e es elemento neutro en A, [e] es el elemento neutro en A/~

c. Si a' es inverso de a en A, [a'] es el inverso de [a] en en A/~

Ejemplos

1. En (Z, +) consideramos la relación "ser congruentes módulo 6", que es compatible con la suma, la tabla de la suma en el conjunto cociente Z/<6> es

+	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

[1] + [5] = [1 + 5] = [6] = [0],
[3] + [5] = [3 + 5] = [8] = [2]

2. En (A = {n ∈ Z/n ≥ 2}, +) se considera la relación de equivalencia definida por

a ~ b ⇔ a y b son números primos o números compuestos

da lugar a dos clases de equivalencia

[2] = {n ∈ A/ n es primo}

[4] = {n ∈ A/ n es compuesto}

Sin embargo, ~ no es compatible con la operación +, pues 2 ~ 2 , 2 ~ 3, y 2 + 2 ¬~ 2 + 3. Es decir, [2] = [2] y [2] = [3], pero [2 + 2] ≠ [2 + 3]. Por este motivo, la suma en A no puede "trasladarse" a A/~.

1.5 Morfismos

Para señalar que dos estructuras algebraicas son esencialmente análogas se dice que son "homomorfas" (semejantes en las formas). La idea se concreta

recurriendo a una aplicación entre los conjuntos que "conserve" la operación.

Sean (A, $*$), (B, #) estructuras algebraicas. Una aplicación f: A $\rightarrow$ B se denomina ***morfismo*** si $f(a_1 * a_2) = f(a_1) \# f(a_2)$, $\forall a_1, a_2 \in A$;

Si f es inyectiva, se llama monomorfismo; si es sobreyectiva, epimorfimo, y si f es biyectiva, isomorfismo. En este caso, Se dice que (A, $*$) y (B, #) son estructuras isomorfas.

Ejemplos

1. f: (N, +) $\rightarrow$ (Z, +), con f(x) = – x es un monomorfismo

2. f: (Z, +) $\rightarrow$ (Z_m, +), con f(x) = [x] es un epimorfismo

3. f: (R, +) $\rightarrow$ (R^+, $\cdot$), con f(x) = exp (x) es un isomorfismo y $f^{-1}(x) = Ln(x)$

4. f: (**P**(X), $\cup$) $\rightarrow$ (**P**(X), $\cap$) con f(Y) = Y′ (complementario de Y en X) es un isomorfismo y $f^{-1} = f$.

Propiedades

1. Si A′ es una subestructura de A, $f(A') = \{f(a') / a' \in A'\}$ es una subestructura de B. En particular, Im (f) = f(A′) es subestructura de B.
2. Si B′ es una subestructura de B y $f^{-1}(B') \neq \varnothing$, $f^{-1}(B') = \{a \in A / f(a) \in B'\}$ es una subestructura de A.
3. Si f es un isomorfismo, entonces f^{-1} es un (iso)morfismo.
4. La composición de morfismos es un morfismo.