CAPITULO I

INTRODUCCION.

Al estudiar, separadamente, las relaciones entre los elementos de distintos conjuntos y operaciones definidas en ellos, se observó que muchas de las propiedades de los conjuntos con respecto a las operaciones, en los casos importantes, eran las mismas. Entonces se pensó en unificar todos estos criterios y en estudiar las relaciones entre los conjuntos y las operaciones de una forma general, definiendo estructuras algebraicas como grupo, campo, etc. Lo que se busca con esta generalización es utilizar toda la información que se posea de la estructura algebraica en casos particulares, ya que si se desea estudiar las características de un conjunto con respecto a una operación y este conjunto cumple con la definición de la estructura, todas sus propiedades quedarán completamente determinadas.

Notaciones.

$\mathbb{N}$ = Números Naturales
$\mathbb{Z}$ = Números Enteros
$\mathbb{Q}$ = Números Racionales
$\mathbb{R}$ = Números Reales
$\mathbb{C}$ = Números Complejos
$\mathbb{Z}^* = \mathbb{Z} - \{0\}$
$\mathbb{Q}^* = \mathbb{Q} - \{0\}$
$\mathbb{R}^* = \mathbb{R} - \{0\}$
$\mathbb{C}^* = \mathbb{C} - \{0\}$

Seccion 1. Leyes de Composición

Definición:

Sean A, B y C conjuntos, una función de A x B en C la llamaremos ley de composición u operación de A y B en C.

$$* \; A \times B \longrightarrow C$$
$$(a, b) \longrightarrow *((a, b)) = a * b$$

* Notación que representa la ley de composición.

En resumen, una operación es una regla que asigna a cada elemento de A x B un único elemento de C.

Ejemplos:

1-1) $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$
$(a, b) \longrightarrow +(a, b) = a + b$ Suma de reales (+)

1-2) $. : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$
$(a, b) \longrightarrow .((a, b)) = a.b$ Producto de reales (.)

1-3) $A = \{1, 2\}$ $B = \{-1, 4\}$
$* : A \times B \longrightarrow \mathbb{Z}$
$(a, b) \longrightarrow a * b = 3a + 2b$

1-4) $S = \mathbb{R} - \{-1\}$ $* : S \times S \longrightarrow S$
$(a, b) \longrightarrow a * b = a + b + a.b$

1-5) $- : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ No es ley de composición
$(a, b) \qquad a - b$

1-6) $- : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$
$(a, b) \longrightarrow a - b$

1-7) $\div \quad \mathbb{Q}^* \times \mathbb{Q}^* \longrightarrow \mathbb{Q}^*$
$(a, b) \longrightarrow a/b$

Definiciones:

1) Una ley de composición es interna o clausurativa en A si es de la forma:
$* : A \times A \longrightarrow A$ esto es si para todo $a, b \in A$ $a * b \in A$.
Las leyes de composición de los ejemplos 1-1, 1-2, 1-4, 1-6, 1-7 son clausurativas.

2) Una ley de composición interna en A se dice conmutativa si y solo si:
$\forall\, a, b \in A \qquad a * b = b * a$.
Los ejemplos 1-1, 1-2, 1-4 son conmutativos, los ejemplos 1-6, 1-7 no lo son ya que $a - b \neq b - a$ y $a/b \neq b/a$.

3) Una ley de composición interna en A se dice asociativa si y solo si:
$\forall\, a, b, c \in A \qquad (a * b) * c = a * (b * c)$.

Los ejemplos 1-1 y 1-2 son asociativos por su suma y producto de reales.

Veamos que la ley de composición del ejemplo 1-4 también es asociativa.

Sea: $a, b, c \in \mathbb{R} - \{-1\}$

$(a * b) * c = (a + b + ab) * c = (a + b + ab) + c + (a + b + ab)c$ def. de *

$= a + \underline{b} + ab + \underline{c} + ac + \underline{cb} + abc$ (1)

Además:

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

$= a + b + c + bc + ab + ac + abc$

$= a + b + ab + c + ac + cb$ (2)

(1) = (2) $\therefore$ $(a * b) * c = a * (b * c)$

La ley de composición del ejemplo 1-6 no es asociativa ya que:

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

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

$(a * b) * c \neq a * (b * c)$

La ley de composición 1-7 no es asociativa.

Seccion 2. Grupos

Definición:

Sea G un conjunto, * una ley de composición interna. El sistema (G, *) es un grupo, si y solo si cumple las siguientes condiciones:

1) La ley de composición interna es asociativa.

2) Existe $e \in G$ tal que para toda $a \in G$ $a * e = e * a = a$
a $\underline{e}$ lo llamaremos elemento neutro.

3) Para cada $a \in G$ existe $a' \in G$ tal que $a * a' = a' * a = e$
el elemento a' lo llamamos inverso u opuesto de a.

Definición:

Un grupo se dice abeliano si y solo si la ley de composición interna es conmutativa.

Notación: $(G, *)$ G es un grupo con respecto a $*$.

Ejemplos:

2-1) De los ejemplos anteriormente dados, veamos cuáles son grupos.

a) $(\mathbb{N}, +) = ?$ "+" es ley de composición interna asociativa $a + e = a$

$e = 0$ $0 \notin \mathbb{N}$ luego $(\mathbb{N}, +)$: no es un grupo.

b) $(\mathbb{N}, \cdot)$. $\cdot$ es ley de composición interna

$\cdot$ es ley de composición interna asociativa

$1 \in \mathbb{N}$ $a.1 = 1.a = a$ $1 \in \mathbb{N}$

$a.a' = 1$ $a' = -1/a$ pero $-1/a \notin \mathbb{N}$

luego $(\mathbb{N}, \cdot)$ no es un grupo.

c) En el ejemplo 1-3 la ley de composición no es interna.

d) $(S, *)$. Ya vimos que $*$ es una ley de composición interna asociativa. Busquemos elemento neutro de esta operación.

Sea $a \in S$ $a \neq -1$. Sea $\underline{e}$ el elemento neutro, entonces por definición $a * e = e * a = a$

$a + e + ae = a$ $e + ae = 0$ como $a \neq -1$

$e(a + 1) = 0$ como $a \neq -1$ $a + 1 \neq 0$ $\therefore$ $e = 0$

$0 \in S$ luego cumple la segunda condición

$a * 0 = 0 * a = a$

Dado $a \in S$ hallemos su inverso a'

Por definición $a * a' = a' * a = 0$

$a * a' = 0$ $a + a' + aa' = 0$ $a'(1 + a) = -a$

Como $1 + a \neq 0$ entonces

$$a' = \frac{-a}{1+a}$$

luego todo elemento de S tiene inverso.

$\therefore$ $(S, *)$ es un grupo, como $*$ es conmutativa.

$(S, *)$ es un grupo abeliano.

2-2) Sea $G = \{1, -1\}$ "$*$" el producto de reales

$(G, \cdot)$ es un grupo

$(G, +)$ no es un grupo "+" la suma de reales.

2-3) $(\mathbb{Z}, +)$ es un grupo abeliano

$(\mathbb{Z}, \cdot)$ no es un grupo

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

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

$(\mathbb{Q}^*, \cdot)$ es un grupo abeliano

$(\mathbb{R}^*, \cdot)$ es un grupo abeliano

2-4) Sea $\mathbb{R}^2 = \{(x, y)/x \in \mathbb{R} \wedge y \in \mathbb{R}\}$

Igualdad en $\mathbb{R}^2$ $(x_1, y_1) = (x_2, y_2) \iff x_1 = x_2 \wedge y_1 = y_2$

$+ : \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

$(x_1 + x_2, y_1 + y_2) \in \mathbb{R}^2$ luego "+" es ley de composición interna

$$[(x_1, y_1) + (x_2, y_2)] + (x_3, y_3) = (x_1 + x_2, y_1 + y_2) + (x_3\ y_3) \quad (1)$$

$$= ((x_1 + x_2) + x_3, (y_1 + y_2) + y_3) \quad (2)$$

$$= (x_1 + (x_2 + x_3), y_1 + (y_2 + y_3)) \quad (3)$$

$$= (x_1, y_1) + (x_2 + x_3, y_2 + y_3) \quad (4)$$

$$= (x_1, y_1) + [(x_2, y_2) + (x_3, y_3)] \quad (5)$$

(1), (2), (4) y (5) por definición de la ley de composición.

(3) por asociatividad de $\mathbb{R}$.

$\therefore$ "+" es ley de composición interna asociativa.

Hallemos el neutro de esta operación. Sea (e_1, e_2) el neutro de "+". Luego:

$$(x, y) + (e_1, e_2) = (x, y)$$

$$(x + e_1, y + e_2) = (x, y) \iff x + e_1 = x \wedge y_1 + e_2 = y$$

$$\therefore \quad e_1 = 0 \qquad e_2 = 0 \qquad 0 \in \mathbb{R} \text{ neutro de los reales}$$

luego $(0, 0)$ es el neutro $\quad (0, 0) \in \mathbb{R}^2$

$$(0, 0) + (x, y) = (0 + x, 0 + y) = (x, y)$$

Hallemos el inverso de (x, y). Sea (x', y') el inverso de (x, y), entonces por definición:

$$(x, y) + (x', y') = (0, 0)$$

$$(x + x', y + y') = (0, 0) \iff x + x' = 0 \wedge y + y' = 0$$

$$\therefore \quad x' = -x \wedge y' = -y'$$

$$\therefore \quad (-x, -y) + (x, y) = (x, y) + (-x, -y) = (0, 0)$$

$(-x, -y) \in \mathbb{R}^2$ ya que $(x, y) \in \mathbb{R}^2 \Rightarrow x \in \mathbb{R}, \; y \in \mathbb{R} \; \therefore$

$$-x \in \mathbb{R} \; y \; -y \in \mathbb{R}.$$

"+" es conmutativa ya que:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) = (x_2 + x_1, y_2 + y_1)$$

$$= (x_2, y_2) + (x_1, y_1)$$

$\therefore$ $(\mathbb{R}^2, +)$ es un grupo abeliano.

De estos ejemplos podemos ver que la estructura de grupo depende tanto del conjunto como de la operación definida.

Teorema. Propiedades de un Grupo

1) El elemento neutro de un grupo $(G, *)$ es único.

2) El inverso de un elemento de un grupo es único.

dm:

1) Supongamos que hay en en G dos elementos diferentes $e \neq e'$. Sea e y e' neutros de $(G, *)$, entonces

$e * e' = e * e' = e'$ por ser e neutro y

$e * e' = e$ por ser e' neutro luego

$e * e' = e = e'$ $\therefore$ $e = e'$ $\longrightarrow\!\leftarrow$ luego e es único.

2) Supongamos que a G tiene dos inversos diferentes $a' \neq a_1'$

$a * a' = e$ por ser a' inverso de a.

$a_1' * (a \times a') = a_1' * e$ por ser e neutro y por estar en un grupo

$(a_1' * a) * a' = a_1'$ por ser a_1' inverso de a tenemos que:

$e * a' = a_1'$ o sea que

$a' = a_1'$ $\longrightarrow\!\leftarrow$ luego a' es único.

Nota: Cuando la operación definida sea una suma el inverso de un elemento lo llamaremos opuesto.

Ejercicios:

1. Responda las siguientes preguntas: justifícándolas.

   a) Puede formarse con el conjunto vacío un grupo?

   b) Puede existir un grupo con un solo elemento?
   Cuál sería este elemento si existe el grupo?

   c) Sean a, b elementos de un grupo. Es $(a * b)' = a' * b'$?

   d) Sean a, b elementos de un grupo abeliano. Es $(a * b)' = a' * b'$?

   e) Es $\{1, -1, i, -i\}$ "un" grupo respecto al producto de complejos?

   f) En un grupo son válidas las leyes cancelativas?
   $a, b, c \in G \quad a * b = a * c \Longrightarrow b = c$

2. Sea $\mathbb{R}^2 = \{(x, y)/x, y \in \mathbb{R}\}$ en $\mathbb{R}^2$ definimos la siguiente operación:

   "$*$" $(x_1, y_1) * (x_2, y_2) = (x_1 + x_2, 0)$

   Es $(\mathbb{R}^2, *)$ un grupo?

3. $X \neq \emptyset$ un conjunto cualquiera ($\emptyset$ = el conjunto vacío)

   $\mathbb{F} = \{f: X \longrightarrow X/f \text{ es biyectiva}\}$ $\mathbb{F}$ conjunto de todas las permutaciones de X.

   "o" Composición de funciones que está definida así:

   $$f, g \in \mathbb{F} \quad (fog)x = f(g(x))$$

   Mostrar que $(\mathbb{F}, o)$ es un grupo no abeliano.

4. $P = \{2n/n \in \mathbb{Z}\}$ Conjunto de los pares

   $I = \{2n+1/n \in \mathbb{Z}\}$ Conjunto de los impares

   Considere: $(P, +)$, $(P, \cdot)$, $(I, +)$, $(I, \cdot)$. Cuáles son grupos con la suma y el producto tradicional?

Sección 3. Campo

Definición:

Sea $K \neq \emptyset$ un conjunto en el cual hay definidas dos leyes de composición internas que llamaremos suma y producto respectivamente. Diremos que K es un campo con respecto a estas dos operaciones y lo notaremos $(K, +, \cdot)$ si y solo si se cumplen las siguientes condiciones:

1) $(K, +)$ es un grupo abeliano

2) $(K^*, \cdot)$ es un grupo abeliano

   $K^* = K - \{e\}$ e elemento neutro respecto a la suma (primera operación)

3) Que para todo $a, b, c \in K$

   $$(a + b).c = ac + bc$$

   esto es que las dos operaciones cumplen las leyes distributivas, esta última condición establece una relación entre las dos operaciones.

Ejemplos:

3-1) $(\mathbb{N}, +, \cdot)$ No forman un campo ya que ni $(\mathbb{N}, +)$ ni $(\mathbb{N}^*, \cdot)$ son grupos.

3-2) $(\mathbb{Z}, +, \cdot)$ No es un campo ya que $(\mathbb{Z}^*, \cdot)$ no es un grupo.

3-3) $(\mathbb{Q}, +, \cdot)$ Es un campo ya que $(\mathbb{Q}, +)$, $(\mathbb{Q}^*, \cdot)$ son grupos abelianos. Además sabemos que la suma y el producto de racionales es distributivo.

3-4) $(\mathbb{R}, +, \cdot)$ es un campo.

3-5) Sea $K = \{a + b\sqrt{2} / a, b \quad \mathbb{Q}\}$

$$(+): (a_1 + b_1\sqrt{2}) \ (+) \ (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$

$$(\cdot): (a_1 + b_1\sqrt{2}) \ (\cdot) \ (a_2 + b_2\sqrt{2}) = (a_1 a_2 + 2 b_1 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{2}$$

$(K, (+), (\cdot))$ es un campo.

Ejercicios:

1) Responda las siguientes preguntas, justificándolas:

   a) Puede existir un campo con un solo elemento?

   b) Puede existir un campo con dos elementos? Cuáles serían estos dos elementos?

   c) $G = \{1, -1\}$ es $(G, +, \cdot)$ Con la suma y producto tradicionales un campo?

   d) Sea $(K, +, \cdot)$ un campo $a \in K$, e elemento neutro con respecto a la suma. Es $ae = e$ para todo $a \in K$?

2) Demostrar ejemplo 3-5.

3) Demostrar que $(\mathbb{C}, (+), (\cdot))$ es un campo. Conduce a $\mathbb{C}$ como:

$$\mathbb{C} = \{a + bi / a, b \in \mathbb{R}\}$$

$$(+): \quad (a_1 + b_1 i) \ (+) \ (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2) i$$

$$(\cdot): \quad (a_1 + b_1 i) \ (\cdot) \ (a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) i$$