ESTRUCTURAS ALGEBRAICAS

Ing. Rubén Darío Estrella Sánchez, MBA
Cavaliere dell'ordine al Merito della Repubblica Italiana
Ingeniero de Sistemas, Administrador, Matemático, Teólogo y Maestro
ministerio@atalayadecristo.org / rubenestrella@atalayadecristo.org

www.atalayadecristo.org

INTRODUCCION

Muchos de los fenómenos que encontramos en la naturaleza tienen ciertas simetrías con las cuales podemos sacar conclusiones que nos permitan entender tal situación de una manera simple. Muchos casos corresponden a problemas de la física y biología. Por ejemplo en física, conceptos como momentos angulares, tensores, etc., aparecen como propiedades de la teoría de grupos. En biología podemos entender moléculas y cristales por sus grupos de simetrías.

Muchos temas se han propuesto como ejercicios para que el estudiante pueda poner en práctica los conceptos ya estudiados. Por supuesto, esto

podría tener la desventaja de producir una idea de aislamiento de los temarios tratados, lo cual no es nuestro propósito.

En esta unidad se introducen los conceptos básicos del álgebra abstracta: operaciones binarias y estructuras algebraicas y sus propiedades, para poder interpretar numerosas situaciones de la vida cotidiana. A manera de repaso se revisarán algunas simbologías de la teoría de conjuntos y sus operaciones.

OBJETIVOS

- Identificar y Reconocer las propiedades de las operaciones binarias.
- Reconocer y determinar elementos neutros y simétricos de diversas operaciones binarias.
- Comprender el concepto de estructura algebraica.
- Identificar los diferentes tipos de estructuras algebraicas a través de sus diferentes propiedades.
- Identificar en diferentes situaciones los diferentes tipos de estructuras algebraicas.
- Crear ejemplos de los diferentes tipos de estructuras algebraicas.
- Resolver problemas donde intervienen estructuras algebraicas.

ANTECEDENTES HISTORICOS

El matemático Evariste Galois (1811-1932) en víspera del duelo que lo llevaría a la muerte, entregó a un amigo notas de su último descubrimiento matemático para que fuesen vistas por los matemáticos Gauss y Jacobi con el objeto de que éstos sabios dieran su opinión sobre la importancia de sus descubrimientos. Los conceptos expuestos por Galois reciben hoy el nombre de Teoría de Grupos, aplicable a la física de partículas y la cristalografía. Justo es hacer notar que dicha teoría estaba esbozada en trabajos hechos por otros matemáticos Lagrange, Ruffini, Gauss y Nicolás Abel.

Estructuras Algebraicas

Operación Binaria.

Una operación binaria ***** en un conjunto, es una regla que asigna a cada par ordenado de elementos de un conjunto, algún elemento del conjunto.

Si **S** es un conjunto no vacío y ***** es una función. Entonces ***** es llamado una operación binaria sobre **S,** si y sólo si ***: S x S ➔ S.**

En otras palabras dado un conjunto no vacío **S** y el producto cartesiano de **S x S**, ***** es una función de modo que a cada par ordenado **(a,b)** le hace corresponder un único elemento de **S** simbolizado por **a*b**.

Toda operación interna en un conjunto se constituye en ley de composición en dicho conjunto. Por lo cual a las operaciones internas también se les llama ley de composición

Por ejemplo en el conjunto de los naturales **N**; la suma (*****) es una operación interna ya que todo par ordenado **(a,b)** se le asigna otro valor, el cual también pertenece a los naturales **N**.

Ejemplo: Si fuera la operación ***(4,6) ➔ 4 * 6 = 10**
lo mismo si se dijera ***(6,8) ➔ 6 * 8 = 14**

Veamos este ejemplo

Sea el conjunto **S = {1, 2, 3}** y la operación ***** definida como la suma de **a** mas **b** menos 1

*	1	2	3
1	1	2	3
2	2	3	
3	3		

*Hay algunos espacios vacío porque el resultado es un elemento que no pertenece al conjunto dado, por lo que se concluye que * no es una operación binaria en S.*
En base al concepto:
*Dado un conjunto no vacío **S** y el producto cartesiano de **S x S**, ***** es una función de modo que a cada par ordenado **(a,b)** le hace corresponder un único elemento de **S** simbolizado por **a*b**.*

Veamos otro ejemplo

Sea el conjunto **S = {A, B, C}** y la operación ***** definida como asociativa, es decir, (A * B) * C = A * (B * C)

*	A	B	C
A	A	B	C
B	B	C	A
C	C	A	B

(A * B) * C = A * (B * C)
B * C = A * A
A = A

(C * A) * B = C * (A * B)
C * B = C * B
A = A

***** es una operación binaria en **S**.*

En base al concepto:
*Dado un conjunto no vacío **S** y el producto cartesiano de **S x S**, ***** es una función de modo que a cada par ordenado **(a,b)** le hace corresponder un único elemento de **S** simbolizado por **a*b**.*

Propiedades de las Operaciones Binarias.

Cerrada.

Si * es una operación binaria sobre S y A es subconjunto de S. Entonces el subconjunto A es cerrado con respecto a la operación binaria *, si y sólo si, para todo x, y que pertenece a A, x * y pertenece a A.

$$*: S \times S \rightarrow S$$

Si

*** es una operación binaria sobre S y $A \subseteq S$**

Entonces

A es cerrado con respecto a $* \Leftrightarrow \forall x, y \in A, x * y \in A$

Tomando en cuenta que el conjunto de los números enteros **Z** es un subconjunto de los números reales **R**.

Por ejemplo en el conjunto de los números enteros **Z**; la suma (*) es una operación interna ya que todo par ordenado **(a,b)** se le puede asignar otro valor, el cual también pertenece a los números enteros **Z**.

Ejemplo: Si fuera la operación ***(2,4) → 2 * 4 = 6**

lo mismo si se dijera ***(6,-5) → 6 * -5 = 1**

Tomando en cuenta que el conjunto de los números naturales **N** es un subconjunto de los números enteros **Z**.

Por ejemplo en el conjunto de los números naturales **N**; la resta (*) no es una operación interna ya que todo par ordenado **(a,b)** no se le puede asignar otro valor, el cual también pertenece a los números naturales **N**.

Ejemplo: Si fuera la operación ***(4,2) → 4 * 2 = 2**

si se dijera ***(6,8) → 6 * 8 = -2**

- 2 no pertenece a **N**. Por tanto la resta **(*)** no es una operación interna del conjunto de los números naturales **N**.

Propiedades de las Operaciones Binarias.

Conmutativa.

Si * es una operación binaria sobre S. Entonces * es conmutativa, si y sólo si, para todo x, y que pertenece a S, **x * y = y * x**.

$$*: S \times S \rightarrow S$$

Si

*** es una operación binaria sobre S**

Entonces

*** es conmutativa $\Leftrightarrow \forall x, y \in S, x * y = y * x$**

Sea el conjunto **S = {A, B, C}** y la operación ***** definida como conmutativa, es decir, x * y = y * x.

*	A	B	C
A	A	B	C
B	B	A	B
C	C	B	A

A * B = B * A

B = B

C * A = A * C

C = C

Por ejemplo si $x * y = x^2 + y^2$ $\forall x, y \in R, x * y = y * x$

$$x * y = y * x$$
$$x^2 + y^2 = y^2 + x^2$$

Si tomamos el par ordenado (-3,2)

$$-3^2 + 2^2 = 2^2 + -3^2$$
$$9 + 4 = 4 + 9$$
$$13 = 13$$

Propiedades de las Operaciones Binarias.

Asociativa.

Si * es una operación binaria sobre S. Entonces * es asociativa, si y sólo si, para todo x, y, z que pertenece a S, **x * (y * z) = (x * y) * z**.

$$*: S \times S \rightarrow S$$

Si

*** es una operación binaria sobre S**

Entonces

*** es asociativa** $\Leftrightarrow \forall$ **x, y, z** $\in$ **S,** $x * (y * z) = (x * y) * z$

Sea el conjunto **S = {A, B, C}** y la operación ***** definida como asociativa, es decir, (A * B) * C = A * (B * C)

*	A	B	C
A	A	B	C
B	B	C	A
C	C	A	B

(A * B) * C = A * (B * C)

B * C = A * A

A = A

(C * A) * B = C * (A * B)

C * B = C * B

A = A

Propiedades de las Operaciones Binarias.

Elemento Identidad.

Si * es una operación binaria sobre S y **e** pertenece a S. Entonces **e** es llamado elemento identidad con respecto a *, si y sólo si, para todo x que pertenece a S, **x * e = e * x = x**.

$$*: S \times S \rightarrow S$$

Si

*** es una operación binaria sobre S**

Entonces

e es el elemento identidad con respecto a $* \Leftrightarrow \forall x \in S, x * e = e * x = x$

$$x + 0 = 0 + x = x$$
$$a \times 0 = 0 \times a = a$$

Para todo número real x. Los números 0 y 1 son llamados elementos identidad para las operaciones de la suma y la multiplicación respectivamente.

Estructuras Algebraicas

Una estructura algebraica es un conjunto no vacío con por lo menos una operación binaria.

*Si **S** es un conjunto no vacío y ***** es una función. Entonces ***** es llamado una operación binaria sobre **S,** si y sólo si ***: S x S ➔ S.***

*En otras palabras dado un conjunto no vacío **S** y el producto cartesiano de **S x S**, ***** es una función de modo que a cada par ordenado **(a,b)** le hace corresponder un único elemento de **S** simbolizado por **a*b**.*

Nosotros podemos decir que (R, +) y (R, ·) son sistemas algebraicos o estructuras algebraicas porque la suma y la multiplicación de números reales son operaciones binarias sobre dicho conjunto. Además como el conjunto de los números enteros **Z** es un subconjunto de los números reales **R.** Podemos decir que los números enteros **Z** son cerrados con respecto a la suma y la multiplicación, es decir, que también (Z, +) y (Z, ·) son sistemas algebraicos o estructuras algebraicas.

Por ejemplo la operación suma con el conjunto de los números naturales **N**, forma una estructura algebraica puesto que cualquiera que sean los números naturales **N** siempre que se sumen dos naturales el resultado será otro número natural **N**. En pocas palabras **N** es un conjunto no vacío y **+** es una operación interna en N. Por tanto (N, +) constituye una estructura algebraica.

Sea el conjunto **A = {-1, 0, 1}** y la operación ***** una operación interna definida como el producto de **"a" por "b",** los resultados se pueden observar en la siguiente tabla:

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

Siempre que se realice la operación a*b resultará un elemento del mismo conjunto por lo cual **(A, *)** forman una estructura algebraica.

Estructura Algebraica – Semigrupo

Semigrupo.

La estructura algebraica o sistema algebraico **(S, *)** es llamado semigrupo, si y sólo si, la operación binaria ***** es asociativa.

(S, *) es semigrupo $\Leftrightarrow$ ***** es asociativa

*** es asociativa** $\Leftrightarrow \forall$ **x, y, z** $\in$ **S,** $x * (y * z) = (x * y) * z$

Sea el conjunto **S = {A, B, C}** y la operación ***** definida como asociativa, es decir, (A * B) * C = A * (B * C)

*	A	B	C
A	A	B	C
B	B	C	A
C	C	A	B

(A * B) * C = A * (B * C)
B * C = A * A
A = A

(C * A) * B = C * (A * B)
C * B = C * B
A = A

Por tanto **(S, *)** es semigrupo.

Dada la operación binaria *, definida por a*b es el máximo de a , b, para todo a, b y c que pertenecen a R.

R es el conjunto de los números reales

***** es la **operación binaria** definida por a*b es el máximo de a y b

(R, *) es semigrupo $\Leftrightarrow$ ***** es asociativa

*** es asociativa** $\Leftrightarrow \forall$ **x, y, z** $\in$ **S,** x * (y * z) = (x * y) * z

$\forall$ a, b, c $\in$ R, a *** (b * c) = (a * b) * c**

Máx {máx {a,b}, c} = Máx {a, máx {b,c}}

Para la solución de esta operación hay 6 posibles casos:

Caso 1: $a \geq b \geq c$
Caso 2: $a \geq c \geq b$
Caso 3: $b \geq a \geq c$
Caso 4: $b \geq c \geq a$
Caso 5: $c \geq a \geq b$
Caso 6: $c \geq b \geq a$

(R, *) es semigrupo

Si S está formada por todas las matrices 2 x 2 de números reales R, y "+" "•" son operaciones binarias definidas por la suma y a la multiplicación de matrices, y como ambas operaciones son asociativas; por tanto (S, +) y (S, •) son semigrupos.

<u>Ejemplos de semigrupos</u>

(N , +) es un semigrupo conmutativo sin elemento neutro.

(N_0 , +) es un semigrupo conmutativo con elemento neutro, el 0.

(N , •) es un semigrupo conmutativo con elemento neutro ó identidad igual a 1.

Teorema 1:

Si (S, *) es un semigrupo y $x_i \in S$, entonces $x_1 * x_2 * x_3 * ... * x_n$ es un miembro único de S $\forall$ n $\in$ N.

Teorema 2:

Si (S, *) es un semigrupo conmutativo, entonces $(x*y)^n = x^n * y^n$
$\forall$ x $\in$ S y $\forall$ n $\in$ N.

Estructura Algebraica – Monoide

Monoide.

Si (S, *) es un semigrupo con un elemento identidad, entonces lo llamamos Monoide, es decir:

*** es asociativa $\Leftrightarrow \forall$ x, y, z $\in$ S,** x * (y * z) = (x * y) * z

e es el elemento identidad con respecto a *** $\Leftrightarrow \forall$ x $\in$ S, x * e = e * x = x**

Semigrupo.

La estructura algebraica o sistema algebraico **(S, *)** es llamado semigrupo, si y sólo si, la operación binaria ***** es asociativa.

(S, *) es semigrupo $\Leftrightarrow$ ***** es asociativa

*** es asociativa $\Leftrightarrow \forall$ x, y, z $\in$ S,** x * (y * z) = (x * y) * z

Elemento Identidad.

Si * es una operación binaria sobre S y **e** pertenece a S. Entonces **e** es llamado elemento identidad con respecto a *, si y sólo si, para todo x que pertenece a S, **x * e = e * x = x**.

***: S x S ➔ S**

Si

*** es una operación binaria sobre S**

Entonces

e es el elemento identidad con respecto a *** $\Leftrightarrow \forall$ x $\in$ S, x * e = e * x = x**

Todo Monoide es Semigrupo, pero no todo Semigrupo es Monoide.

Sea el conjunto **S = {A, B, C}** y la operación ***** definida como asociativa, es decir, (A * B) * C = A * (B * C)

*	A	B	C
A	A	B	C
B	B	C	A
C	C	A	B

(A * B) * C = A * (B * C)
B * C = A * A
A = A

(C * A) * B = C * (A * B)
C * B = C * B
A = A
***** es Asociativa.

A * A = A
B * A = A * B = B
C * A = A * C = C

A es el elemento identidad.

Por tanto (S, *) es un Monoide.

Si S está formada por todas las matrices 2 x 2 de números reales R, y "•" es una operación binaria definida por multiplicación de matrices, y como $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ es el elemento identidad de la multiplicación de matrices 2 x 2, y "•" es asociativa; por tanto (S, •) es un monoide.

Teorema 3:
Si (S, *) es una estructura algebraica con un elemento identidad, entonces la identidad es única.

Ejemplos de Monoide

(N , +) , **(Z , +)** , **(Q , +) ,** son monoides.

(N , -) no es un monoide porque la sustracción no es ley de composición interna en **N.**

(N , $*$) donde $*$ está definido como a $*$ b = máx.{a , b} es un monoide.

Estructura Algebraica - Invertible e Inversa

Invertible.

Si **(S, *)** es una estructura algebraica con un elemento identidad **e** y **x ∈ S**, entonces **x** es invertible, si y sólo si, existe **y ∈ S** tal que:

$$x * y = y * x = e$$

es decir:

(S, *) es una estructura algebraica

e es el elemento identidad con respecto a * $\Leftrightarrow \forall x \in S, x * e = e * x = x$

$\forall x \in S$ es invertible $\Leftrightarrow \exists y \in S: x * y = y * x = e$

Teorema 4:

Si **(S, *)** es un Monoide con un elemento identidad **e**, entonces **e** es invertible, es decir, **e * x = x * e = e**.

Teorema 5:

Si **(S, *)** es un Monoide con un elemento identidad **e** y $X \in S$,

if $x * y = y * x = e, \exists! y \in S$, entonces y es único.

Inversa.

Si **(S, *)** es un Monoide con un elemento identidad **e** y **x, y ∈ S**, entonces **y** es llamado inversa de **x**, denotado por $y = x^{-1}$, si y sólo si:

$$y * x = x * y = e$$

es decir:

(S, *) es una estructura algebraica

e es el elemento identidad con respecto a *** ⇔ ∀ x ∈ S, x * e = e * x = x**

∀ x ∈ S ∃! y ∈ S es inversa $\mathbf{y = x^{-1}} \Leftrightarrow \mathbf{y * x = x * y = e}$

Teorema 6:

Si **(S, *)** es un Monoide con un elemento identidad **e** y X, y ∈ S, if **x** es invertible in **(S, *)** y **x * y = e** or **y * x = e,** entonces $\mathbf{y = x^{-1}}$.

Teorema 7:

Si **(S, *)** es un Monoide con un elemento identidad **e** y X ∈ S, if **x** es invertible in **(S, *),** entonces $\mathbf{y = x^{-1}}$ es invertible $(\mathbf{x^{-1}})^{-1} = \mathbf{x}$.

Teorema 8:

Si **(S, *)** es un Monoide con un elemento identidad **e** y X, y ∈ S, if **x** y **y** son invertibles in **(S, *),** entonces **x * y** es invertible y $(\mathbf{x * y})^{-1} = \mathbf{y^{-1} * x^{-1}}$.

Estructura Algebraica – Grupo

Grupo.

La estructura algebraica (G, *) es llamada Grupo, si y sólo si,

1. * es Asociativa

   *** es asociativa ⇔ ∀ x, y, z ∈ S,** x * (y * z) = (x * y) * z

2. (G, *) tiene un elemento identidad.

   e es el elemento identidad con respecto a *** ⇔ ∀ x ∈ S, x * e = e * x = x**

3. cada elemeto de G es invertible.

$\forall$ x $\in$ G es invertible $\Leftrightarrow \exists$ y $\in$ G: **x * y = y * x = e**

En otras palabras un Grupo es un Monoide en el cual todos sus elementos son invertibles.

Sea * la operación binaria definida sobre el conjunto **G = {1, a, b}** a través de la siguiente tabla de operación:

*	1	a	b
1	1	a	b
a	A	b	1
b	B	1	a

Entonces (G,*) es un grupo de orden 3. Usando la notación convencional para grupo, nosotros podemos decir a^2 = b y ba = 1, es decir, a*a = a^2 = b y b*a = 1 = a*a*a.

Todo los Grupos son Monoides, pero no todos los Monoides son Grupos.

Si la operación binaria * además es conmutativa el Grupo (G, *) es llamado Grupo Abeliano.

<u>Grupo Abeliano.</u>

La estructura algebraica (G, *) es llamada Grupo Abeliano, si y sólo si,

1. * es Asociativa
   *** es asociativa $\Leftrightarrow \forall$ x, y, z $\in$ G,** x * (y * z) = (x * y) * z

2. (G, *) tiene un elemento identidad.
e es el elemento identidad con respecto a *** $\Leftrightarrow \forall$ x $\in$ S, x * e = e * x = x**

3. cada elemeto de G es invertible.
   $\forall$ x $\in$ G es invertible $\Leftrightarrow \exists$ y $\in$ G: **x * y = y * x = e**

4. * es Conmutativa
   *** es conmutativa $\Leftrightarrow \forall$ x, y $\in$ G,** x * y = y * x

Teorema 9:

Si $(G, *)$ es un Grupo y $a, b, x \in G$, entonces $ax = b$, si sólo si, $x = a^{-1}b$ y $xa = b$, si y sólo si $x = ba^{-1}$.

Teorema 10:

$(G, *)$ es un Grupo y $a, b, c \in G$, si $ab = ac$ o $ba = ca$, entonces $b = c$. Llamada Ley de Cancelación.

Teorema 11:

$(G, *)$ es un Grupo finito y $a \in G$, entonces $a^n = 1$ para algún $n \in G$.

Ejemplos de Grupos:

1) $(Z, +)$; $(Q, +)$; $(R, +)$ y $(C, +)$ Son grupos abelianos. También se llaman grupos aditivos debido a la operación aditiva.

2) $(N, +)$ No es grupo. No tiene neutro ni inverso de cada elemento.

3) $(N_0, +)$ No es grupo. Tiene neutro, el 0 , pero no tiene inverso aditivo.

4) $(Q, \bullet)$ No es grupo, el 0 no tiene inverso multiplicativo.

5) $(R, \bullet)$ No es grupo, el 0 no tiene inverso multiplicativo.

6) $(Q - \{0\}, \bullet)$ y $(R - \{0\}, \bullet)$ Son grupos.

Estructura Algebraica – Subgrupo

Subgrupo.

(G, *) es un grupo y **H ⊆ G**, entonces **(H, *)** es llamado Subgrupo de **(G, *), si y sólo si (H, *) es un grupo**.

La estructura algebraica (G, *) es llamada Grupo, si y sólo si,

1. * es Asociativa
   *** es asociativa ⇔ ∀ x, y, z ∈ S,** x * (y * z) = (x * y) * z

2. (G, *) tiene un elemento identidad.
e es el elemento identidad con respecto a *** ⇔ ∀ x ∈ S, x * e = e * x = x**

3. cada elemeto de G es invertible.
   ∀ x ∈ G es invertible ⇔ ∃ y ∈ G: **x * y = y * x = e**

Por ejemplo los sistemas o estructuras algebraicas (R, +) y (Z, +), ambos son modelos de grupos; y Z ⊆ R, podemos decir entonces que (Z, +) es un subgrupo de (R, +).

Sea * la operación binaria definida sobre el conjunto **G = {1, a, b, c}** a través de la siguiente tabla de operación:

*	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	c	b	1	a
c	c	b	a	1

Entonces **(G, *)** es un grupo y el orden de cada elemento de a, b y c es 2. Por ejemplo $a^2 = 1$, el conjunto **{1, a}** junto a la operación binaria * es un grupo. **({1, a}, *)** es un subgrupo de **(G, *)**.
Similarmente, **({1, b},*) y ({1, c}, *)** ambos son subgrupos de **(G,*)**.

Estructura Algebraica – Grupo Cíclico

Grupo Cíclico.

Un Grupo **(G, *)** es cíclico si todo miembro de G puede ser expresado como una potencia de un número entero positivo en un simple elemento de G.

$$a^m a^n = a^{m+n} \quad (a^m)^n = a^{mn}$$

Sea * la operación binaria definida sobre el conjunto **G={1, a, a^2, a^3 }** y $a^4 = 1$, a través de la siguiente tabla de operación:

*	1	a	a^2	a^3
1	1	a	a^2	a^3
a	a	a^2	a^3	1
a^2	a^2	a^3	1	a
a^3	a^3	1	a	a^2

La estructura algebraica (G, *) es llamada Grupo Cíclico de orden 4.

$a^4 = 1$, el orden de a es 4 y $(a^2)^2 = a^4$.

Estructura Algebraica – Campo

Campo.

F es un conjunto y + y • son operaciones binarias sobre F. Entonces la estructura algebraica (F, +, •) es llamada campo, si y sólo si,

1. $\forall$ x, y, z $\in$ F, **x + (y + z) = (x + y) + z** ➔ **Asociativa con respecto a +**
2. $\forall$ x, y $\in$ F, **x + y = y + x** ➔ **Conmutativa con respecto a +**
3. $\exists$ 0 $\in$ F, **x + 0 = x** ➔ **Identidad con respecto a +**
4. $\forall$ x $\in$ F, $\exists$ -x $\in$ F, **x + (-x) = 0** ➔ **inverso con respecto a +**
5. $\forall$ x, y, z $\in$ F, **x • (y • z) = (x • y) • z** ➔ **Asociativa con respecto a •**
6. $\forall$ x, y $\in$ F, **x • y = y • x** ➔ **Conmutativa con respecto a •**
7. $\exists$ 1 $\in$ F, **x • 1 = x** ➔ **Identidad con respecto a •**
8. $\forall$x $\in$ F–{0}, $\exists$ x^{-1} $\in$ F–{0}, **x•** x^{-1} **= 1** ➔ **inverso con respecto a •**
9. $\forall$ x, y, z $\in$ F, **x • (y + z) = x•y + x•z** ➔ **Distributiva con respecto a +**
10. $0 \neq 1$.

(R, +, •) el conjunto de los números reales y las operaciones de la suma y la multiplicación son un ejemplo de Campo.

Sea $\bar{x}$ y $\bar{y}$ son elemento de Z_3, y la suma y el producto de $\bar{x}$ y $\bar{y}$ son definidas por:

$$\bar{x} + \bar{y} = \overline{x + y} \qquad \bar{x} \bullet \bar{y} = \overline{xy}$$

Las tablas de las operaciones de la adición y la multiplicación en (Z3, +, •) son las siguientes:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

•	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Estructura Algebraica – Anillo

Dados, un conjunto no vacío A y dos leyes de composición interna $*$ y $\bullet$, la terna ordenada **(A , $*$, $\bullet$)** tiene estructura de ***Anillo*** si y solo si

a) $*$ es asociativa. Es decir $\forall a$, $\forall b$, $\forall c$: a, b, c $\in$ A $\Rightarrow$ $(a * b) * c = a * (b * c)$

b) $*$ posee elemento neutro en A. Es decir $\exists e \in A$ / $\forall a$, si $a \in A \Rightarrow a * e = e * a = a$

c) Todo elemento de A es invertible en A respecto de $*$.
Es decir $\forall a \in A$, $\exists a' \in A$ / $a * a' = a' * a = e$

d) $*$ es conmutativa. Es decir $\forall a$, $\forall b$: a, b $\in$ A $\Rightarrow a * b = b * a$

Estas 4 propiedades muestran que **(A , $*$)** es un ***grupo abeliano***.

e) $\bullet$ es asociativa. Es decir $\forall a$, $\forall b$, $\forall c$: a, b, c $\in$ A $\Rightarrow$ (a $\bullet$ b) $\bullet$ c = a $\bullet$ (b $\bullet$ c)

Esta propiedad muestra que **(A , $\bullet$)** es un semigrupo.

f) $\bullet$ distribuye doblemente sobre $*$. Es decir, $\forall a$, $\forall b$, $\forall c$: a, b, c $\in$ A
$\Rightarrow$ a $\bullet$ (b $*$ c) = (a $\bullet$ b) $*$ (a $\bullet$ c) y (b $*$ c) $\bullet$ a = (b $\bullet$ a) $*$ (c $\bullet$ a)

Resumiendo podemos decir que:

(A , $*$, $\bullet$) es un ***Anillo*** sii **(A , $*$)** es un ***grupo abeliano*** ; **(A , $\bullet$)** es un ***semigrupo*** y la segunda operación ***distribuye*** sobre la primera.

Una aclaración oportuna

Como la operación $*$ es aditiva y la operación $\bullet$ es multiplicativa, es común representarlas con los conocidos signos de la suma y el producto, pero en todos los casos deberá respetarse la definición que corresponde a cada operación.

Con esta aclaración debe quedar claro que **(A , + , •)** representa una estructura algebraica, talvez un anillo, pero que la operación + y la operación • no representan la suma y el producto conocido, salvo ello esté expresamente indicado.
Con igual margen de tolerancia en la interpretación de este tema, debemos decir que el elemento neutro de la operación aditiva se representa con 0 (cero) y el neutro de la operación multiplicativa con 1 (uno) sin que ellos sean necesariamente el 0 y 1 conocidos.

Si además

g) • conmutativa. Es decir $\forall a , \forall b : a, b \in A \Rightarrow a \bullet b = b \bullet a$

entonces tenemos un ***Anillo conmutativo***.

h) • posee elemento neutro en A. Es decir $\exists e \in A / \forall a$, si $a \in A \Rightarrow a g e = e g a = a$

entonces tenemos un ***Anillo con identidad*** ó ***Anillo con unidad***.

i) Todo elemento de A distinto de cero es invertible en A respecto de • .

Es decir $\forall a \in A , a \neq 0 , \exists a' \in A / a \bullet a' = a' \bullet a = e$ entonces se llama

Anillo de división.

Ejemplos

1.- **(N , + , •)** con las operaciones conocidas **no es un anillo**, pues en **N** no existe neutro para la adición.

2.- **(N_0 , + , •)** con las operaciones conocidas **no es anillo**, pues N_0 carece de inversos aditivos.

3.- **(Z , + , •)** con las operaciones conocidas, **es un anillo conmutativo con unidad.**

Anillos sin divisores de cero

Un anillo **(A , $*$, $\bullet$)** se dice ***sin divisores de cero*** si y solo sí elementos **no nulos** de **A** dan producto **no nulo**.

En símbolos:

(A , $*$, $\bullet$) carece de divisores de cero si y solo sí $\forall a$, $\forall b$: a, b $\in$ A si $a \neq 0$ y $b \neq 0$
entonces $a \bullet b \neq 0$

Anillo de integridad

(A , $*$, $\bullet$) es un ***Anillo de integridad*** si y solo sí **(A , $*$, $\bullet$)** es un anillo y 0 es su único divisor de cero

Dominio de integridad

La terna **(A , $*$, $\bullet$)** se llama ***Dominio de integridad*** si y solo sí **(A , $*$, $\bullet$)** es un ***Anillo conmutativo con unidad y sin divisores de cero***.

Dicho de otra manera, un ***Dominio de integridad*** es un ***Anillo conmutativo con identidad y de integridad.***

Ejemplos

1.- **(Z , + , $\bullet$)** con las operaciones conocidas es un **dominio de integridad**.

2.- **(Q , + , $\bullet$) ; (R , + , $\bullet$) y (C , + , $\bullet$)** con las operaciones conocidas
son **dominio de integridad**.

3.- Los polinomios en una indeterminada (o más) con coeficientes en **Q** , **R** ó
C forman **dominio de integridad** con las operaciones conocidas.

Evariste Galois

born Oct. 25, 1811, Bourg-la-Reine, near Paris
died May 31, 1832, Paris

French mathematician famous for his contributions to the part of higher algebra known as group theory. His theory solved many long-standing unanswered questions, including the impossibility of trisecting the angle and squaring the circle.

Galois was the son of Nicolas-Gabriel Galois, an important citizen in the Paris suburb of Bourg-la-Reine. In 1815, during the Hundred Days regime that followed Napoleon's escapefrom Elba, his father was elected mayor. Galois's mother, Adelaïde-Marie Demante, was of a distinguished family of jurists. She educated Galois at home until 1823, when he entered the Collège Royal de Louis-le-Grand. There his education languished at the hands of mediocre and uninspiring teachers. But his mathematical ability suddenly appeared when he was able to master quickly the works of Adrien-Marie Legendre on geometry and Joseph-Louis Lagrange on algebra.

Under the guidance of Louis Richard, one of his teachers at Louis-le-Grand, Galois's further study of algebra soon led him to take up a major challenge. Mathematicians for a long time had used explicit formulas, involving only rational operations and extractions of roots, for the solution of equations up to degree four. (For example, $3x2 + 5 = 17$ is an equation of the second degree, since it contains the exponent 2; solving an equation of this type is called a solution by radicals, because it involves extracting the square root of an expression composed of one or more terms whose coefficients appear in the equation.) The solution of quadratic, or second degree, equations goes back to ancient times. Formulas for the cubic and quartic were published in 1545 by Gerolamo Cardano, Italian mathematician and physician, after their discovery a few years earlier by the mathematicians Niccolo Tartaglia and Ludovico Ferrari. The equation of the fifth degree then defeated mathematicians until Paolo Ruffini in 1796 attempted to prove the impossibility of solving the general quintic equation by radicals. Ruffini's effort was not wholly successful,but the Norwegian mathematician Niels Abel in 1824 gave an essentially correct proof.

Galois was unaware of Abel's work in the first stages of his investigation, although he did learn of it later. This was perhaps fortunate because Galois actually had launched himself on a much more ambitious study; while yet a student, at about age 16, he sought, by what is now called the “Galois theory,” a deeper understanding of the essential conditions that an equation must satisfy in order for it to be solvable by radicals. His method was to analyze the “admissible” permutations (a change in an ordered arrangement) of the roots of the equation. That is, in today's terminology, he formed the “group” of automorphisms (a particular kind of transformation) of the “field,” obtained by adjoining the roots of the equation. His key discovery, brilliant and highly imaginative, was that solvability by radicals ispossible if and only if the group of automorphisms is solvable, which means

essentially that the group can be broken down into prime-order constituents (prime numbers are positive numbers greater than 1 divisible only by themselves and 1) that always have an easily understood structure. The term solvable is used because of this connection with solvability by radicals. Thus Galois perceived that solving equations of the quintic and beyond required a wholly different kind of treatment than that required for the quadratic, cubic, and quartic.

While still at Louis-le-Grand he published several minor papers. Soon disappointments and tragedy filled his life withbitterness. Three memoirs that he submitted to the Academy of Sciences were lost or rejected by the academicians, who as mathematicians were authorized to act as editors. The first was lost in 1829 by Augustin-Louis Cauchy. In each of two attempts (1827 and 1829) to enter the École Polytechnique, the leading school of French mathematics, he had a disastrous encounter with an oral examiner and failed. Then his father, after bitter clashes with conservative elements in his hometown, committed suicide in 1829. The same year, realizing that his career possibilities as a professional mathematician had ended, Galois enrolled as a teacher candidate in the less prestigious École Normale Supérieure and turned to political activism. But he continued his research.

A second memoir, on algebraic functions, which he submitted in 1830 to the Academy of Sciences, was lost by Jean-Baptiste-Joseph Fourier. The revolution of 1830 sent the last Bourbon monarch, Charles X, into exile. But republicans were deeply disappointed when yet another king, Louis-Philippe, ascended the throne—even though he was a citizen king who wore the tricolour of the Revolution. When Galois wrote a vigorous article expressing these views, he was promptly expelled from the École Normale Supérieure. Subsequently he was arrested twice for republican activities; he was acquitted the first time but spent six months in prison on the second charge. His third memoir in 1831 was returned by Siméon-Denis Poisson with a note that it was virtually incomprehensible and shouldbe expanded and clarified.

The circumstances that led to Galois's death in a duel in Paris have never been fully explained. It has been variously suggested that it resulted from a quarrel over a woman, that he was challenged by royalists who detested his republican views, or that an agent provocateur of the police was involved. Alexandre Dumas, in his autobiography MesMémoirs (1863–65), implicated Pécheux d'Herbinville as the man who shot Galois. In any case, anticipating his deathin the coming duel, Galois in feverish haste wrote a scientific last testament addressed to his friend and former schoolmate Auguste Chevalier. In his distracted notes, there are hints that Galois had begun to develop the theory of algebraic functions, the full development of which was achieved 40 years later by the German mathematician Bernhard Riemann.

Galois's manuscripts, with annotations by Joseph Liouville, were published in 1846 in the Journal de Mathématiques Pures et Appliquées. In 1870 the French mathematician Camille Jordan published the full-length treatment of Galois's theory, Traité des Substitutions. These works rendered his discoveries fully accessible and his place secure in the history of mathematics. On June 13, 1909, a plaque was placed on Galois's modest

birthplace at Bourg-la-Reine, and the mathematician Jules Tannery made an eloquent speech of dedication, which was publishedthe same year in the Bulletin des Sciences Mathématiques.