Álgebra Lineal
Lectura 1: Operación Binaria y sus Propiedades

Ing. Aldo Jiménez Arteaga

Enero 2020, Rev. Agosto 2021

1. Operación Binaria

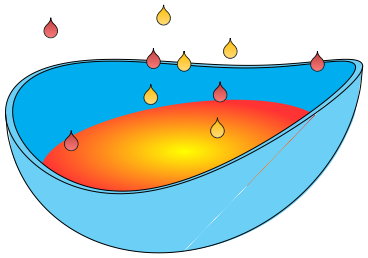

Figura 1. Un ejemplo de operación binaria es vertir dos sustancias en un recipiente; la mezcla es el resultado.

Los procesos de contar y medir se llevan a cabo mediante la interacción de elementos pertenecientes a un conjunto. Generalmente, dichos elementos son números (naturales, reales, entre otros), y la interacción es una relación entre dichos números; en algunas ocasiones los elementos que interactúan para llegar a un resultado pueden ser objetos físicos como se describe en la figura 1. El Álgebra Moderna se encarga de formalizar la teoría de las cantidades (conjuntos) y las relaciones entre ellas (operaciones).

Considerando las cantidades a y b, perteneciente a un conjunto V, se puede establecer una relación entre ellas al definir una regla de correspondencia:

$$f : V \times V \Rightarrow f(a,b) = c \qquad \forall\ a,b \in V \tag{1}$$

La regla mostrada en (1) establece la función multivariable $f(a,b)$, llamada operación, que tiene asignado un elemento c, llamado resultado, y puede o no pertenecer a V.

En el caso de los números, las operaciones definidas son la adición y el producto. Una característica importante es que solo pueden sumarse o multiplicarse dos cantidades a la vez, lo cual limita el accionar de dichas operaciones pero permite definir una serie de propiedades que agilizan la obtención de resultados. Con base en resultados y número de elementos a operar se define la operación binaria.

> Una operación binaria $*$, definida en un conjunto S, es una función $f : S \times S \to U$ que asigna a cada par de elementos $a, b \in S$ un resultado único $c \in U$, donde puede darse uno de dos casos: $U = S$, o bien $U \neq S$. Al par $(S, *)$ se le denominará estructura, si la operación definida cumple con ciertas propiedades.

Hay que resaltar los dos casos que se mencionan sobre la naturaleza del resultado. En el primero, $U = S$ quiere decir que el resultado de

la operación binaria pertenece al conjunto de los operandos; se conoce como *ley de composición interna*. En el segundo caso, $U \neq S$, se indica que el resultado no pertenece al conjunto de los operandos; ésta se llama *ley de composición externa*.

1.1. Propiedades de las Operaciones Binarias

Con una operación binaria $*$ definida en un conjunto S, se plantean las siguientes propiedades:

- ❑ Cerradura.
- ❑ Asociación.
- ❑ Elemento neutro.
- ❑ Elementos inversos.
- ❑ Conmutación.
- ❑ Distribución.

Como se mencionó, dichas propiedades permiten hacer eficiente la operación de elementos. Puesto que el resultado permanece inalterable al aplicar las propiedades, una operación compleja puede separarse en secciones simples que demandan menos esfuerzo para ser calculadas.

Cerradura. Si el resultado de aplicar la operación a dos elementos $a, b \in S$ está definido en S, entonces la operación es cerrada.

$$a * b \in S$$

Asociación. Si la operación es binaria, entonces no puede operar tres elementos $a, b, c \in S$ a la vez. La asociación permite trabajar dos cualesquiera de los elementos y el resultado de la operación se trabaja con el elemento restante.

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

Elemento neutro. Es el elemento $e \in S$ que al operarlo con cualquier otro, éste último no se ve afectado.

$$a * e = a$$

El elemento neutro es único.

Elementos inversos. Esta propiedad se relaciona directamente con el elemento neutro. Si al operar $a \in S$ con el elemento $a' \in S$ se obtiene el neutro, entonces a' es el inverso de a.

$$a * a' = e$$

Todo elemento del conjunto S posee su respectivo y único inverso.

Conmutación. Si en la operación binaria no hay orden para trabajar los elementos, se dice que la operación permite la conmutación.

$$a * b = b * a$$

Distribución. Al definirse una segunda operación $\circ$ dentro del conjunto, la distribución establece que la segunda operación se distribuye sobre la primera $(*)$.

$$a \circ (b * c) = (a \circ b) * (a \circ c)$$

En sentido estricto, las propiedades de elemento neutro, elementos inversos y distribución deben definirse por la izquierda y por la derecha. Por ejemplo, los elementos inversos deben existir tanto por izquierda

$$a' * a = e$$

como por derecha

$$a * a' = e$$

Por alcances del curso, éstas propiedades se definen por la derecha.

Juntas, las propiedades no solo facilitan las operaciones entre los elementos del conjunto involucrado; el planteamiento de ecuaciones de primer grado se facilita una vez que se confirma que la operación binaria involucrada satisface las primeras cinco propiedades.

Ejemplo. Sea el conjunto de los números racionales $\mathbb{Q}$, donde se define la operación binaria

$$a * b = a + b - \sqrt{2}ab \qquad \forall\ a, b \in \mathbb{Q}$$

Determine si la operación cumple con las propiedades de cerradura, elemento neutro y conmutación.

Cerradura. Para verificar la cerradura se requiere analizar la regla de asignación de la operación:

$$a * b = a + b - \sqrt{2}ab$$

Puesto que a y b son números racionales, entonces cualquier suma o producto entre ellos también será racional. En cambio $\sqrt{2}$ es irracional, lo que hace al producto $\sqrt{2}ab$ un número irracional. La operación no es cerrada.

Elemento neutro. El elemento neutro se descubre al aplicar la propiedad y despejando:

$$\begin{aligned} a * e &= a \\ a + e - \sqrt{2}ae &= a \\ e - \sqrt{2}ae &= 0 \\ e\left(1 - \sqrt{2}a\right) &= 0 \quad \therefore \quad e = 0 \in \mathbb{Q} \end{aligned}$$

En conclusión existe el elemento neutro para esta operación.

Conmutación. Se verifica una igualdad al aplicar la propiedad:

$$\begin{aligned} a * b &= b * a \\ a + b - \sqrt{2}ab &= b + a - \sqrt{2}ba \\ &= a + b - \sqrt{2}ab \end{aligned}$$

En este caso, la conmutación se cumple puesto que $*$ está definida con base en la suma y multiplicación usuales.

En todo conjunto se pueden definir diversas operaciones binarias. No es necesario que los elementos sean cantidades fijas, ya que cualquier relación de dos elementos con un resultado se considera una operación binaria; por ejemplo, el conjunto de funciones posee operaciones binarias como suma, multiplicación o composición que cumplen algunas de las propiedades mencionadas.

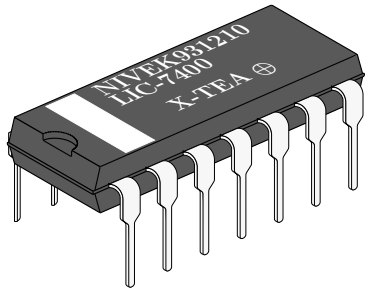

Figura 2. Las compuertas lógicas realizan las operaciones binarias AND, OR y XOR; los elementos que operan, como tal, no son numéricos: son voltajes altos y bajos.

En conjuntos que no poseen elementos matemáticos como tal, pueden definirse operaciones binarias que son cotidianas en la vida humana. Los colores son ejemplo de ello: la mezcla de dos colores arroja un resultado y esos tres elementos, en sí, no son matemáticos. Otro ejemplo son las operaciones lógicas, fundamentales en los circuitos electrónicos actuales. La figura 2 muestra compuertas lógicas que pueden encontrarse en cualquier dispositivo electrónico, y que utilizan voltajes como elementos de operaciones binarias.

Álgebra Lineal
Lectura 2: Grupo y Grupo Abeliano

Ing. Aldo Jiménez Arteaga

Enero 2020, Rev. Agosto 2021

1. Grupo

Los elementos de un conjunto junto con sus operaciones definen las llamadas estructuras algebraicas. Dependiendo del número de operaciones y las propiedades que cumplen, una estructura será más completa que otra y tendrá un uso más amplio.

La estructura más simple que se estudiará es el grupo:

Sea un conjunto no vacío G con una operación binaria $*$ definida. El sistema $(G, *)$ es un grupo si cumple con:

- ❑ Cerradura.
- ❑ Asociación.
- ❑ Elemento neutro.
- ❑ Elementos inversos.

No todos los conjuntos llegan a ser grupos, ya que con una propiedad que no se satisfaga el concepto no se cumple. Ejemplos de grupos son los números enteros, racionales, reales y complejos con la suma como operación binaria.

Ejemplo. Sea el conjunto $\mathbb{Z}$ donde se define la operación

$$a \,\Delta\, b = a + b - 3 \qquad \forall\ a, b \in \mathbb{Z}$$

Determine si el sistema $(\mathbb{Z}, \Delta)$ forma un grupo.

Cerradura. Por suma en los enteros $a + b \in \mathbb{Z}$ y al restar $-3 \in \mathbb{Z}$ se obtiene otro entero. Por lo tanto, la operación es cerrada.

Asociación. Se desarrollan ambos lados de la definición de la propiedad:

$$(a \,\Delta\, b) \,\Delta\, c = a \,\Delta\, (b \,\Delta\, c)$$
$$(a + b - 3) \,\Delta\, c = a \,\Delta\, (b + c - 3)$$
$$(a + b - 3) + c - 3 = a + (b + c - 3) - 3$$
$$a + b + c - 6 = a + b + c - 6$$

La igualdad al desarrollar ambos extremos se cumple; por lo tanto, la operación es asociativa. **Elemento neutro.** Se despeja el elemento neutro.

$$a \,\Delta\, e = a$$
$$a + e - 3 = a$$
$$e = a - a + 3 \quad \therefore \quad e = 3 \in \mathbb{Z}$$

Existe un único entero que aplica como neutro. Por lo tanto, la propiedad se cumple.

Elementos inversos. Se despejan los inversos con base en el neutro.

$$a \,\Delta\, a' = e$$
$$a + a' - 3 = 3$$
$$a' = 3 + 3 - a \quad \therefore \quad a' = 6 - a \in \mathbb{Z}$$

Cada elemento $a \in \mathbb{Z}$ tiene su propio inverso. Por lo tanto, la propiedad se cumple.

En conclusión, el sistema $(\mathbb{Z}, \Delta)$ es un grupo.

El grupo no es la estructura algebraica más simple; existen estructuras antecesoras del grupo como el magma, el semigrupo o el monoide. Estas estructuras no se estudiarán en este curso.

2. Grupo Abeliano

El concepto de grupo no es una estructura completa pues carece de la propiedad conmutativa. Niels Abel, uno de los pioneros del Álgebra Moderna definió en la teoría de grupos las propiedades que debe cumplir dicha estructura algebraica, incluyendo a la conmutación.

Sea un grupo $(G, *)$. G es un grupo abeliano si se cumple con la conmutación.

A finales del siglo XIX, se renombró al grupo conmutativo como abeliano a manera de homenaje póstumo a Abel.

Ejemplo. Sea el sistema $(\mathbb{Q}^+, \diamond)$ donde

$$a \diamond b = \frac{3}{2}ab \qquad \forall\ a, b \in \mathbb{Q}^+$$

Determine si el sistema es un grupo abeliano.

Cerradura. Por producto en los racionales $ab \in \mathbb{Q}$ y al multiplicar por $\frac{3}{2} \in \mathbb{Q}$ se obtiene otro racional; los tres números son positivos, entonces el resultado del producto siempre será positivo. Por lo tanto, se cumple la cerradura.

Asociación.

$$(a \diamond b) \diamond c = a \diamond (b \diamond c)$$
$$\left(\frac{3}{2}ab\right) \diamond c = a \diamond \left(\frac{3}{2}bc\right)$$
$$\frac{3}{2}\left(\frac{3}{2}ab\right)c = \frac{3}{2}a\left(\frac{3}{2}bc\right)$$
$$\frac{9}{4}abc = \frac{9}{4}abc$$

La igualdad se cumple. En consecuencia, la operación es asociativa.

Elemento neutro.

$$a = a \diamond e$$

$$a = \frac{3}{2}ae$$
$$1 = \frac{3}{2}e \quad \therefore \quad e = \frac{2}{3}$$

Existe un único racional positivo que aplica como neutro.

Elementos inversos.

$$e = a \diamond a'$$
$$\frac{2}{3} = \frac{3}{2}aa'$$
$$\frac{4}{9a} = a'$$

Cada elemento $a \in \mathbb{Q}^+$ tiene su propio inverso.

Conmutación.

$$a \diamond b = b \diamond a$$
$$\frac{3}{2}ab = \frac{3}{2}ba$$

Por conmutación en los racionales la propiedad se satisface.

Al cumplir con las cinco propiedades, se concluye que el sistema $(\mathbb{Q}^+, \diamond)$ es un grupo abeliano.

3. Solución de Ecuaciones

Ahora que ya se tiene el concepto de grupo abeliano, se pueden enunciar varias propiedades de la estructura algebraica que son derivadas de la definición. Dichas propiedades adicionales son:

- ❑ Ley de cancelación:

$$a * b = c * b \quad \Rightarrow \quad a = c$$

- ❑ El elemento neutro e es único.
- ❑ El elemento inverso a' de cada a es único.
- ❑ El inverso de a' es $(a')' = a$.

Con estas propiedades pueden plantearse y resolverse ecuaciones de primer grado con una o varias incógnitas. Pero, si se extiende el concepto de grupo abeliano a una segunda operación se pueden plantear y resolver ecuaciones más complejas.

Ejemplo. Sea el grupo abeliano $(\mathbb{R}, \#)$ donde

$$a \# b = a + b - \sqrt{2} \qquad \forall\ a, b \in \mathbb{R}$$

Obtenga la solución de la ecuación $x \# 2\sqrt{2} = -3\sqrt{2}$.

Mediante propiedades del grupo abeliano, con $e = \sqrt{2}$ y $\left(2\sqrt{2}\right)' = 0$, la solución de la ecuación se desarrolla a continuación.

$$x \# 2\sqrt{2} = -3\sqrt{2}$$
$$x \# 2\sqrt{2} \# \left(2\sqrt{2}\right)' = -3\sqrt{2} \# \left(2\sqrt{2}\right)' \quad \text{operando con } \left(2\sqrt{2}\right)'$$
$$x \# \left[2\sqrt{2} \# \left(2\sqrt{2}\right)'\right] = -3\sqrt{2} \# \left(2\sqrt{2}\right)' \quad \text{por asociación}$$
$$x \# e = -3\sqrt{2} \# \left(2\sqrt{2}\right)' \quad \text{por inverso}$$
$$x = -3\sqrt{2} \# \left(2\sqrt{2}\right)' \quad \text{por neutro}$$

$$x = -3\sqrt{2} \# 0$$
$$x = -4\sqrt{2}$$

Así, la ecuación planteada en el grupo abealiano $(\mathbb{R}, \#)$ tiene como solución $x = -4\sqrt{2}$.

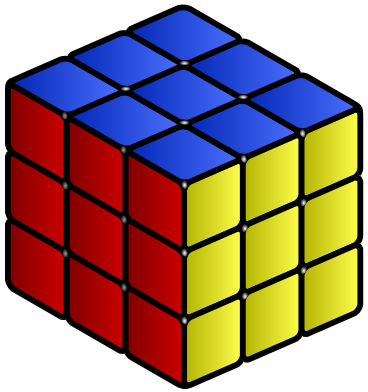

Figura 1. El cubo Rubik es un ejemplo de grupo abeliano.

Las aplicaciones del grupo abeliano son variadas: circuitos electrónicos, simetrías moleculares, cristalografía, entre otros. Una de ellas es el cubo Rubik (figura 1). Inventado por el arquitecto húngaro Erno Rubik, este rompecabezas mecánico puede modelarse a partir del grupo abeliano, donde los movimientos de las caras representan el conjunto de elementos, y la composición de movimientos (giro tras giro) es la operación binaria definida. La rama de la Matemática que estudia los conceptos analizados es la Teoría de Grupos. Esta teoría permite diseñar algoritmos que pueden resolver problemas lúdicos como la solución del cubo Rubik, o bien problemas más complejos como el acomodo de automóviles en un estacionamiento.

Álgebra Lineal
Lectura 3: Campo

Ing. Aldo Jiménez Arteaga

Enero 2020

Además del grupo abeliano, existen muchas otras estructuras algebraicas que se basan en la definición de una operación binaria. Pero las estructuras más completas se caracterizan por poseer dos operaciones binarias; entre ellas destacan el anillo, el pseudoanillo, el dominio entero o el campo. El campo es una de las bases del Álgebra Lineal, ya que es parte de la definición del espacio vectorial.

Sea K un conjunto no vacío, donde se definen las operaciones binarias $*$ y $\circ$. El sistema $(K, *, \circ)$ es un campo, si

- ❑ $(K, *)$ es un grupo abeliano.
- ❑ $(K, \circ)$ es una operación cerrada, asociativa, con elemento neutro.
- ❑ $(\circ)$ es una operación que se distribuye sobre $*$.
- ❑ existen elementos inversos para $(K, \circ)$, excepto para el neutro de la primera operación.

Dos elementos trascendentes en el campo son el neutro de $*$, conocido como cero del campo, y el neutro de $\circ$, llamado unidad del campo. Estos nombres no se deben a que los elementos tengan un valor determinado, sino a que tradicionalmente los elementos neutro de la suma y la multiplicación son el cero y el uno, respectivamente. La notación que se utilizará es e para el cero y n para la unidad del campo.

Ejemplo. Sea el conjunto $H = \{0, 1, 2\}$ donde se definen las operaciones binarias $\oplus$ y $\otimes$ como

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\otimes$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Determine si el sistema $(H, \oplus, \otimes)$ forma un campo.

Puesto que las operaciones binarias están definidas con tablas (el conjunto de elementos es finito), el análisis de la estructura algebraica se realizará de manera conceptual en lugar de desarrollar cada propiedad.

Grupo abeliano $(H, \oplus)$

- ❑ **Cerradura**. Cualquier resultado de la operación pertenece al conjunto H, pues la tabla solo contiene a 0, 1 y 2.
- ❑ **Asociación**. Al probar todas las combinaciones sobre la asociación siempre se obtendrá el mismo resultado.
- ❑ **Conmutación**. La tabla es una matriz simétrica, entonces se cumple la conmutación para cualquier par de elementos.
- ❑ **Elemento neutro**. El cero del campo es $e = 0$, pues su renglón es el mismo que la cabecera de la columna.
- ❑ **Elementos inversos**. Son $0' = 0$, $1' = 2$ y $2' = 1$, pues el resultado de operarse con sus respectivos inversos es el neutro.

Propiedades para $(H, \otimes)$

- ❑ **Cerradura**. La tabla sólo contiene elementos del conjunto H; la operación es cerrada.
- ❑ **Asociación**. Al probar todas las combinaciones sobre la asociación siempre se obtendrá el mismo resultado.
- ❑ **Conmutación**. La tabla representa una matriz simétrica, entonces la operación es conmutativa.
- ❑ **Elemento neutro**. La unidad del campo es $n = 1$, cuyo renglón repite la cabecera de la tabla.
- ❑ **Elementos inversos**. Son $1' = 1$ y $2' = 2$; el único elemento carente de inverso es $e = 0$.

Distribución $(H, \oplus, \otimes)$ Al probar todas las posibles combinaciones la distribución se cumple.

Puesto que todas las propiedades de la definición se cumplen, la conclusión es que el sistema $(H, \oplus, \otimes)$ es, efectivamente, un campo.

Al igual que el grupo, el campo posee propiedades derivadas de la definición, las cuales son:

- ❑ Si $a * b = c * b \Rightarrow a = c$; si $a \circ b = c \circ b \Rightarrow a = c$.
- ❑ Los elementos neutros son únicos y diferentes entre sí.
- ❑ Para el cero del campo $a \circ e = e$.
- ❑ Los inversos de cada a son únicos en cada operación.

Los campos son muy comunes en la matemática. y la vida diaria en general. Los conjuntos numéricos de los racionales, los reales y los complejos son ejemplos de campos. Otro campo menos conocido fundamenta la electrónica digital moderna: el conjunto $B = \{0, 1\}$ de bits, es usado con las operaciones lógicas XOR y AND como la suma y la multiplicación en dispositivos digitales (véase la figura 1). La extensión de este campo a la computación se basa en la teoría que Evariste Galois fundamentó a principios del siglo XIX.

La teoría de campos de Galois definió por primera vez el concepto de campo y con ello extendió el concepto de grupo. El campo de Galois es una herramienta muy importante en la computación: permite modelar los bytes como elementos sobre los cuales se les puede aplicar las operaciones XOR y AND. El campo de Galois (*Galois Field*, GF) contiene un número finito de elementos; en computación se utiliza en potencias de dos, por ejemplo $GF(2^8)$.

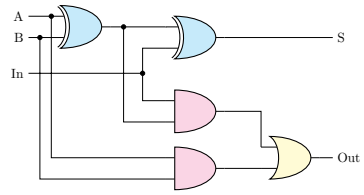

Figura 1. Los circuitos digitales actuales se basan en el uso de bits, los cuales son elementos de un campo con las operaciones XOR (cian) y AND (magenta).