VII. Estructuras Algebraicas

Objetivo

Se analizarán las operaciones binarias y sus propiedades dentro de una estructura algebraica.

Definición de operación binaria

Operaciones como la suma, resta, multiplicación o división de números son consideradas operaciones binarias, ya que asocian a un par de números con un resultado. En general, una operación binaria tiene dos características esenciales:

- Se aplica a un par de elementos con una naturaleza determinada.
- Asocia a dicho par con otro único elemento de la misma naturaleza determinada; la asociación se realiza por medio de un criterio definido.

En forma general, una operación binaria definida en un conjunto S no vacío es una función $S \times S$ que relaciona un par de elementos $(a, b)\ \forall\ a, b \in S$ con una imagen $c \in S$.

Ejemplo 7.1. Si se considera al conjunto de los números racionales y la suma, se tendrá que dicha operación asocia a un par de números racionales otro único número racional; es decir, para el par de números racionales $\left(\frac{a}{b}, \frac{c}{d}\right)$, existe un único número denotado como $\frac{a}{b} + \frac{c}{d}$ que se conoce como la suma de $\frac{a}{b}$ y $\frac{c}{d}$. El criterio para obtener la suma de dos números racionales es

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

Además de las operaciones tradicionales, es posible expresar otras operaciones binarias.

Ejemplo 7.2. La tabla 7.1 especifica la operación binaria AND, que establece una operación lógica utilizada en la electrónica y la computación

·	***0***	***1***
0	0	0
1	0	1

Tabla 7.1. Operación AND.

En este caso, el criterio que se establece para realizar la operación es la misma tabla, y el conjunto sobre el cual se aplica es $\{0, 1\}$; en este caso se tendría:

$$0 \cdot 1 = 0 \qquad 1 \cdot 0 = 0$$

$$1 \cdot 1 = 1 \qquad 0 \cdot 0 = 0$$

Que son los resultados que la operación puede asignar.

Las operaciones binarias también pueden definirse por medio de reglas de correspondencia, y haciendo uso de las operaciones binarias tradicionales.

Ejemplo 7.3. Sea la siguiente operación binaria

$$x \ddagger y = x^y \ \forall \ x, y \in \mathbb{Z}$$

Se puede obtener un resultado para la pareja $(-1, 6)$:

$$-1 \ddagger 6 = (-1)^6$$

Cuyo resultado es 1.

Propiedades de las operaciones binarias

Cuando un conjunto tiene definida una operación binaria se puede formar un sistema algebraico que posee una estructura definida, la cual está ligada a las diferentes propiedades que posea la operación binaria.

Los niveles y diferentes tipos de estructuras algebraicas están sujetos a la naturaleza de las propiedades que se cumplen para una operación en un conjunto dado. Así, las estructuras de **grupo**, **anillo** y **campo** se diferencian por el número de operaciones y las propiedades que éstas cumplen en un conjunto numérico dado.

La primera de estas propiedades es inherente al concepto de operación binaria: a cada par de elementos de cierta naturaleza se le asigna un resultado de ésa misma naturaleza.

Ejemplo 7.4. Si se aplica la suma a los números naturales, el resultado será otro número natural:

$$m + n = p \quad \forall \ m, n, p \in \mathbb{N}$$

Si se tuviesen los números naturales 3 y 4, el resultado de su suma es 7, otro número natural.

Esto quiere decir que una operación binaria es cerrada; o sea, una operación definida en un conjunto S da como resultado un elemento de ese conjunto S.

Cerradura

Si el resultado de aplicar una operación binaria $(*)$ está definido en un conjunto S, entonces se dice que S es cerrado con respecto a dicha operación binaria; es decir,

$$a * b \in S, \quad \forall \ a, b \in S$$

Ejemplo 7.5. Sea la operación binaria $x \ddagger y = x^y \ \forall \ x, y \in \mathbb{Z}$. Se obtiene un resultado que puede o no pertenecer a los números enteros. Si el operando y fuese mayor a cero, el resultado es un número entero; por ejemplo, $(-2,3)$ arrojaría el siguiente resultado:

$$-2 \ddagger 3 = (-2)^{-3}$$

Que es $-8 \in \mathbb{Z}$. En cambio si la pareja a operar fuese $(3, -2)$, el resultado sería

$$3 \ddagger -2 = (-3)^{-2}$$

Que es el número fraccionario $\frac{1}{9} \notin \mathbb{Z}$, ya que es un número racional; por lo tanto, la operación $(\ddagger)$ no es cerrada para el conjunto de los números enteros.

Ejemplo 7.6. Sea el conjunto $X = \{ä, ö, ü\}$ y la operación definida por la tabla 7.2.

ß	**ä**	**ö**	**ü**
ä	ä	ö	ü
ö	ö	ö	ä
ü	ä	ö	ü

Tabla 7.2. Operación Eszett definida para X.

Al aplicar la operación a una pareja de elementos, se puede observar que la operación es cerrada, ya que siempre se obtendrá como resultado un elemento del conjunto X.

$$ä \, ß \, ö = ö \qquad ü \, ß \, ü = ü \qquad ö \, ß \, ü = ä$$

Asociatividad

Al momento de definir una operación binaria se precisó que sólo podía realizarse con dos elementos de un solo conjunto; es decir, al tratar de operar tres elementos, primero se debe realizar la operación con dos de ellos, y después trabajar con el resultado y el tercer elemento. Este proceso de asociar elementos para operarlos se define como propiedad asociativa.

Para una operación binaria $(*)$ definida en el conjunto S, la asociación de elementos especifica que:

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

Ejemplo 7.7. En la suma de números enteros se tiene la asociación cumplida.

$$(a + b) + c = a + (b + c) \quad \forall \, a, b, c \in \mathbb{Z}$$

Que a su vez es extensión de la suma en los números naturales.

Ejemplo 7.8. Para el conjunto X y la operación de la tabla 7.2, la asociación no puede cumplirse ya que

$$ö \, ß \, (ö \, ß \, ü) = ö \, ß \, ä \Rightarrow ö$$

$$(ö \, ß \, ö) \, ß \, ü = ö \, ß \, ü \Rightarrow ä$$

Que son dos resultados completamente diferentes.

Ejemplo 7.9. Para las matrices de orden $m \times n$ y la operación de suma, es posible asociar los elementos que se operarán:

$$(A_{m\times n} + B_{m\times n}) + C_{m\times n} = A_{m\times n} + (B_{m\times n} + C_{m\times n})$$

Y el resultado no se verá alterado.

Existencia del elemento neutro

Si existe un elemento e dentro de un conjunto, que tiene la propiedad de no alterar a otro elemento a cuando se les aplica una operación binaria, entonces se habla de un elemento neutro.

Si se define la operación binaria $(*)$ dentro del conjunto S, y existe un elemento $e \in S$ tal que

- $a * e = a, \forall\, a \in S$, entonces e es un elemento neutro por la derecha.
- $e * a = a, \forall\, a \in S$, entonces e es un elemento neutro por la izquierda.
- $a * e = e * a \Rightarrow a, \forall\, a \in S$, entonces e es un elemento neutro para $(*)$.

Esto quiere decir que un conjunto dado tendrá, al menos, un elemento neutro si éste es neutro por la izquierda y por la derecha.

Ejemplo 7.10. Si se considera al conjunto de las matrices de orden $m \times n$ y la operación de multiplicación, se verifica que el elemento neutro sería la matriz identidad:

$$I_m A_{m\times n} = A_{m\times n}$$

Donde I_m es la matriz identidad de orden m, la cual es un elemento neutro por la izquierda.

$$I_n A_{n\times m} = A_{n\times m}$$

Donde I_n es la matriz identidad de orden n, la cual es un elemento neutro por la derecha.

Estas son las propiedades que cumple la matriz identidad y que se estudiaron en el tema de matrices y determinantes.

Ejemplo 7.11. El elemento neutro para la operación de suma en los números complejos sería el número $0 + 0i$, ya que

$$(x + yi) + (0 + 0i) = x + yi \quad \forall\, x + yi \in \mathbb{C}$$

Por medio de la conmutación en $\mathbb{C}$, se verifica que $0 + 0i$ es neutro por la izquierda y por la derecha.

Ejemplo 7.12. En el conjunto X del ejemplo 7.6 y la operación de la tabla 7.2, se puede verificar que existen dos elementos neutros por la izquierda: $\ddot{a}$ y $\ddot{u}$.

$$\ddot{a}\ \text{ß}\ \ddot{a} = \ddot{a} \qquad \ddot{a}\ \text{ß}\ \ddot{o} = \ddot{o} \qquad \ddot{a}\ \text{ß}\ \ddot{u} = \ddot{u}$$

$$\ddot{u}\ \text{ß}\ \ddot{a} = \ddot{a} \qquad \ddot{u}\ \text{ß}\ \ddot{o} = \ddot{o} \qquad \ddot{u}\ \text{ß}\ \ddot{u} = \ddot{u}$$

En cambio, estos elementos no son neutros por la derecha.

$$\ddot{a}\ ß\ \ddot{a} = \ddot{a} \qquad \ddot{o}\ ß\ \ddot{a} = \ddot{o} \qquad \ddot{u}\ ß\ \ddot{a} = \ddot{a}$$

$$\ddot{a}\ ß\ \ddot{u} = \ddot{u} \qquad \ddot{o}\ ß\ \ddot{u} = \ddot{a} \qquad \ddot{u}\ ß\ \ddot{u} = \ddot{u}$$

Y por lo tanto, la operación ß no posee elementos neutros.

Existencia de elementos inversos

Los elementos inversos se relacionan directamente con el elemento neutro. En este caso, si el resultado de la operación binaria es el elemento neutro, entonces los dos elementos que intervinieron en la operación son inversos uno del otro.

Al definir la operación binaria $(*)$ dentro del conjunto S, y tomando en cuenta la existencia del elemento neutro $e \in S$, se dice que

- $a * \breve{a} = e, \forall\ a \in S$, entonces $\breve{a}$ es el elemento inverso de a por la derecha.
- $\breve{a} * a = e, \forall\ a \in S$, entonces $\breve{a}$ es el elemento inverso de a por la izquierda.
- $a * \breve{a} = \breve{a} * a \Rightarrow e, \forall\ a \in S$, entonces $\breve{a}$ es el elemento inverso de a para $(*)$.

Por lo tanto, si el inverso por la izquierda y por la derecha es el mismo, entonces es un elemento inverso único para a. Además, un conjunto tendrá para cada elemento su correspondiente inverso en una operación binaria.

Ejemplo 7.13. En la multiplicación de matrices de orden n, y que son no-singulares, se tiene que

$$I_n A_n = A_n I_n \Rightarrow A_n$$

Donde I_n define al elemento neutro. En consecuencia, el elemento inverso de A por la izquierda será el mismo que el inverso por la derecha:

Ejemplo 7.14. Cada elemento del conjunto de los números reales tiene un solo inverso definido para la operación de multiplicación:

$$x \cdot x^{-1} \quad \forall\ x \neq 0 \in \mathbb{R}$$

Sabiendo que 1 es el elemento neutro en $\mathbb{R}$ para la multiplicación, y que el cero es el único elemento que no posee inverso.

Conmutatividad

Cuando una operación binaria permite que el orden de los elementos no influya en el resultado que se obtendrá, se dice que la operación permite la conmutación.

Para una operación binaria $(*)$ definida en el conjunto S, la conmutación especifica que:

$$a * b = b * a \quad \forall\ a, b \in S$$

Ejemplo 7.15. Para la multiplicación de matrices de orden 2 no siempre se cumple la conmutación:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

En cambio, el producto

$$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} b_{11}a_{11} + b_{12}a_{21} & b_{11}a_{12} + b_{12}a_{22} \\ b_{21}a_{11} + b_{22}a_{21} & b_{21}a_{12} + b_{22}a_{22} \end{pmatrix}$$

Que son dos matrices completamente diferentes.

Ejemplo 7.16. Para el conjunto X y la operación de la tabla 7.2, la conmutación no puede consumarse en los casos

$$ä \text{ ß } ü = ü$$

$$ü \text{ ß } ä = ä$$

Por lo tanto, no existe la conmutación para esta operación.

Ejemplo 7.17. Para las matrices diagonales de orden 3 y la multiplicación se tiene que:

$$\begin{pmatrix} a_{11} & & \\ & a_{22} & \\ & & a_{33} \end{pmatrix}\begin{pmatrix} c_{11} & & \\ & c_{22} & \\ & & c_{33} \end{pmatrix} = \begin{pmatrix} c_{11} & & \\ & c_{22} & \\ & & c_{33} \end{pmatrix}\begin{pmatrix} a_{11} & & \\ & a_{22} & \\ & & a_{33} \end{pmatrix}$$

Cuyo resultado será el mismo en ambos casos:

$$\begin{pmatrix} a_{11}c_{11} & & \\ & a_{22}c_{22} & \\ & & a_{33}c_{33} \end{pmatrix}$$

Estas cinco propiedades permiten establecer una jerarquía de estructuras, que se vuelven más completas según la naturaleza de sus elementos, el número de operaciones binarias que se define en ellos, y las propiedades que cumplen estas operaciones.

Definición de grupo

La estructura algebraica más simple que se estudiará será el grupo. Este define a un conjunto que posee una operación binaria y se cumplen tres propiedades: asociación, elemento neutro y elemento inverso.

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

1. $(a * b) * c = a * (b * c)$
2. $\exists\, e \in G, a * e = e * a \Rightarrow a$
3. $\exists\, ă \in G, a * ă = ă * a \Rightarrow e$

Para cualquier $a, b, c \in G$.

Ejemplo 7.18. De los conjuntos numéricos conocidos, el primero que posee una estructura de grupo es el conjunto de los números enteros estableciendo a la suma como su operación binaria:

1. $(a+b)+c=a+(b+c)$
2. $\exists\, 0 \in \mathbb{Z}, a+0=0+a \Rightarrow a$
3. $\exists -a \in \mathbb{Z}, a+(-a)=(-a)+a \Rightarrow 0$

Los números naturales no poseen este tipo de estructura, ya que no está definido un elemento neutro para la suma ni mucho menos los elementos inversos.

Ejemplo 7.19. Para el conjunto de los números complejos y la operación definida como

$$z_1 \text{ ю } z_2 = \overline{z_1 z_2}$$

Se satisface que la operación es cerrada, ya que la multiplicación de números complejos arroja un resultado en $\mathbb{C}$; además, el conjugado de un número complejo es otro complejo.

$$\overline{z_1 z_2} \in \mathbb{C}$$

Para comprobar si existe la asociación se debe verificar que

$$(z_1 \text{ ю } z_2) \text{ ю } z_3 = z_1 \text{ ю } (z_2 \text{ ю } z_3)$$

Entonces,

$$\begin{aligned}(z_1 \text{ ю } z_2) \text{ ю } z_3 &= \overline{z_1 z_2} \text{ ю } z_3 \\ &= \overline{\overline{(z_1 z_2)} z_3} \\ &= z_1 z_2 \overline{z_3} \ldots (1)\end{aligned}$$

Por otra parte,

$$z_1 \text{ ю } (z_2 \text{ ю } z_3) = z_1 \text{ ю } \overline{z_2 z_3}$$

$$= \overline{\overline{z_1 (\overline{z_2 z_3})}}$$

$$= \overline{z_1} z_2 z_3 \ldots (2)$$

Se constata que (1) y (2) no son iguales; por lo tanto, $\mathbb{C}$ bajo la operación ю no es un grupo.

Ejemplo 7.20. Sea el sistema dado por $(\mathbb{R}-\{0\}, \sim)$ donde

$$x \sim y = 2xy \quad \forall\, x, y \neq 0 \in \mathbb{R}$$

Se verifica que el resultado de la operación será un número real. Además, se observa que

$$\begin{aligned}(x \sim y) \sim z &= x \sim (y \sim z) \\ 2xy \sim z &= x \sim 2yz \\ 2(2xy)z &= 2x(2yz) \\ 4xyz &= 4xyz\end{aligned}$$

Y la propiedad asociativa se cumple.

Por otro lado,

$$\begin{aligned} e{\sim}x &= x \\ 2ex &= \\ 2e &= 1 \\ e &= \frac{1}{2} \end{aligned}$$

Como el elemento neutro e está definido, implica que se cumple esta propiedad.

Finalmente,

$$\begin{aligned} \check{x}{\sim}x &= e \\ 2\check{x}x &= \frac{1}{2} \\ \check{x} &= \frac{1}{2x} \end{aligned}$$

Y existe un elemento inverso para cada x que pertenezca al conjunto dado. Por lo tanto, los números reales diferentes de cero forman un grupo con respecto a la operación definida.

Subgrupo

De un grupo G se pueden tomar subconjuntos, que posiblemente puedan formar un grupo tomando la operación definida para G.

Sea $(G,*)$ un grupo. Un subconjunto H de G es un subgrupo si él mismo es un grupo para la operación $(*)$; es decir, $(H,*)$ es un grupo.

Para poder identificar si $H \subset G$ es un subgrupo para la operación $(*)$, basta con verificar si se cumple que

$$a * b \in H, \forall\, a, b \in H$$

$$\check{a} \in H, \forall\, a \in H$$

Ejemplo 7.21. Se sabe que $(\mathbb{Z}, +)$ es un grupo; sin embargo, los subconjuntos de los números naturales y los números negativos no pueden ser subgrupos.

Para la cerradura de la suma se sabe que

$$m + n \in \mathbb{N}, \forall\, m, n \in \mathbb{N}$$

Análogamente,

$$a + b \in \mathbb{Z}^-, \forall\, a, b \in \mathbb{Z}^-$$

Sin embargo, al tratar de determinar el elemento inverso para suma, se sabe que los inversos aditivos para los números naturales se encuentran en el conjunto de los números negativos, y viceversa. Esto quiere decir, que aunque $\mathbb{Z}$ es un grupo, sus subconjuntos no necesariamente lo son.

Ejemplo 7.22. Sea el grupo $(\mathbb{R}, +)$. Si $\mathbb{Q} \subset \mathbb{R}$, entonces se cumple que

$$\frac{a}{b} + \frac{c}{d} \in \mathbb{Q}$$

Y además, el inverso aditivo

$$-\frac{a}{b} \in \mathbb{Q}$$

Por lo tanto, $\mathbb{Q}$ forma un subgrupo del grupo $\mathbb{R}$ para la suma.

Grupo abeliano

El grupo abeliano añade la propiedad conmutativa a la definición de grupo.

Se dice que $(G,*)$ es un grupo abeliano (o conmutativo) si la operación $(*)$ cumple con

$$a * b = b * a \quad \forall\, a, b \in G$$

Ejemplo 7.23. Sea M el siguiente conjunto:

$$M = \left\{ \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \middle| m_{11}, m_{12}, m_{21}, m_{22} \in \mathbb{R} \right\}$$

Y la operación suma de matrices tradicional. Para determinar si $(M, +)$ es un grupo abeliano se deben demostrar las propiedades de asociación, existencia de elemento neutro, existencia de elementos inversos y conmutación. De las propiedades del grupo se sabe que $E = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ es el elemento neutro de la suma, y $\check{A} = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$ representa a los elementos inversos; la asociación y conmutación en la suma se cumplen como una extensión de las propiedades de la suma en los números reales. En consecuencia, el sistema $(M, +)$ es un grupo abeliano.

Ejemplo 7.24. Sea el conjunto $A = \{a, b\}$ y la operación definida en la tabla 7.3.

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

Tabla 7.3. Operación binaria en A.

Para verificar si $(A, +)$ es un grupo abeliano se tiene:

Asociación:

$$a+(a+b)=(a+a)+b$$
$$a+b=b+a$$
$$b=b$$

$$b+(a+a)=(b+a)+a$$
$$b+a=b+a$$
$$b=b$$

$$a+(b+a)=(a+b)+a$$
$$a+b=b+a$$
$$b=b$$

$$b+(a+b)=(b+a)+b$$
$$b+b=b+b$$
$$a=a$$

$$a+(b+b)=(a+b)+b$$
$$a+a=b+b$$
$$a=a$$

$$b+(b+a)=(b+b)+a$$
$$b+b=a+a$$
$$a=a$$

Además, para los casos en los cuales todos los operandos son iguales, se cumple la propiedad. Por lo tanto existe la asociación para $(A,+)$.

Elemento neutro:

$$e+a=a \quad \Rightarrow \quad e=a$$

$$e+b=b \quad \Rightarrow \quad e=a$$

Por lo tanto, existe un único elemento neutro (a); y así, se cumple la propiedad.

Elementos inversos:

$$\breve{a}+a=a \quad \Rightarrow \quad \breve{a}=a$$

$$\breve{b}+b=a \quad \Rightarrow \quad \breve{b}=a$$

Para este ejemplo, los elementos inversos existen; por lo tanto, la propiedad se cumple.

Finalmente, la propiedad conmutativa queda como:

$$a+b=b+a$$
$$b=b$$

Y la conmutación también es válida para la operación. Por lo tanto, se concluye que el sistema $(A,+)$ tiene estructura de grupo abeliano.

Definición de anillo

Conocido el grupo, se puede ampliar esta estructura a una más completa; que pueda abarcar no sólo nuevas propiedades para una operación binaria, sino que permite definir una nueva operación dentro del conjunto al cual se asocia la primera operación binaria. Este tipo de criterio se presenta en los anillos.

Sea A un conjunto no vacío, donde se definen las operaciones $(*)$ y $(\diamond)$. El sistema $(A,*,\diamond)$ es un anillo, si se cumplen $\forall\, a,b,c \in A$:

Para la primera operación se satisface

1. La asociación, $(a * b) * c = a * (b * c)$
2. La conmutación, $a * b = b * a$
3. La existencia del elemento neutro, $e * a = a$
4. La existencia de elementos inversos

Para la segunda operación se satisface

5. La asociación, $(a \diamond b) \diamond c = a \diamond (b \diamond c)$
6. La distribución por la izquierda sobre la primera operación, $a \diamond (b * c) = (a \diamond b) * (a \diamond c)$
   La distribución por la derecha sobre la primera operación, $(b * c) \diamond a = (b \diamond a) * (c \diamond a)$

La primera operación define al grupo abeliano $(A,*)$. Por lo que un anillo es un grupo abeliano para la primera operación definida; dicha estructura de grupo se conoce como la **estructura aditiva del anillo**.

Un caso peculiar es el elemento neutro de la primera operación, e, que es conocido como el **cero del anillo**; se debe hacer hincapié que el término cero no se refiere al número 0, ya que A puede ser un conjunto no-numérico.

Ejemplo 7.25. El sistema $(\mathbb{R}, +, \cdot)$ es un anillo, ya que los números reales cumplen las propiedades de asociación, existencia de elemento neutro, existencia de elementos inversos y conmutación para la suma:

- $(x + y) + z = x + (y + z)$
- $x + y = y + x$
- $0 + x = x$
- $x + (-x) = 0$

Mientras tanto, la multiplicación cumple con la asociación, y la distribución sobre la suma:

- $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
- $(y + z) \cdot x = (y \cdot x) + (z \cdot x)$

Ejemplo 7.26. Dado el grupo abeliano del ejemplo 7.24, la primera operación de la tabla 7.3, y definiendo ahora $(A, +, \times)$, donde la segunda operación se muestra en la tabla 7.4, se puede determinar si este nuevo sistema es anillo o no.

×	***a***	***b***
a	*a*	*a*
b	*a*	*a*

Tabla 7.4. Segunda operación binaria en A.

Debido a que un anillo contiene a un grupo abeliano para su primera operación, entonces sólo bastará con probar las propiedades de asociación y distribución para la segunda operación.

Asociación:

$$a \times (a \times b) = (a \times a) \times b$$
$$a \times a = a \times b$$
$$a = a$$

$$b \times (a \times a) = (b \times a) \times a$$
$$b \times a = b \times a$$
$$a = a$$

$$a \times (b \times a) = (a \times b) \times a$$
$$a \times a = a \times a$$
$$a = a$$

$$b \times (a \times b) = (b \times a) \times b$$
$$b \times a = a \times b$$
$$a = a$$

$$a \times (b \times b) = (a \times b) \times b$$
$$a \times b = a \times b$$
$$a = a$$

$$b \times (b \times a) = (b \times b) \times a$$
$$b \times a = b \times a$$
$$a = a$$

Por lo que la asociación en la segunda operación se cumple.

Distribución sobre la primera operación:

$$a \times (a + b) = (a \times a) + (a \times b)$$
$$a \times b = a + a$$
$$a = a$$

$$a \times (b + b) = (a \times b) + (a \times b)$$
$$a \times a = a + a$$
$$a = a$$

$$a \times (b + a) = (a \times b) + (a \times a)$$
$$a \times b = a + a$$
$$a = a$$

$$b \times (a + a) = (b \times a) + (b \times a)$$
$$b \times a = a + a$$
$$a = a$$

$$b \times (a + b) = (b \times a) + (b \times b)$$
$$b \times b = a + b$$
$$b = b$$

$$b \times (b + a) = (b \times b) + (b \times a)$$
$$b \times b = b + a$$
$$b = b$$

Y la distribución por la izquierda se cumple; para la distribución por la derecha se realiza el procedimiento análogo, resultando como conclusión el cumplimiento de la distribución de $(+)$ sobre $(\times)$. Por lo que el sistema $(A, +, \times)$ es un anillo.

Anillo conmutativo

Un anillo conmutativo se define a partir de un anillo. Sea el sistema $(A, *, \diamond)$ un anillo. Si para la segunda operación definida se cumple

$$a \diamond b = b \diamond a \qquad \forall\, a, b \in A$$

Se dice que el anillo es conmutativo.

Ejemplo 7.27. Tomando el ejemplo anterior, donde la estructura $(A, +, \times)$ es un anillo, ahora se verificará el cumplimiento de la conmutatividad para la segunda operación:

$$a \times b = b \times a$$
$$a = a$$

Por lo que la conmutación se cumple; en consecuencia, el anillo $(A, +, \times)$ es conmutativo.

Anillo con unidad

Si un anillo $(A, *, \diamond)$ posee elemento neutro para la segunda operación:

$$f \diamond a = a \qquad \forall\, a \in A$$

Entonces, el anillo tiene unidad (f). Al igual que el cero del anillo, al decir la unidad del anillo no se habla precisamente del número 1, sino del elemento neutro para la segunda operación de A.

Ejemplo 7.28. Siguiendo con el anillo $(A, +, \times)$ se deberá encontrar el elemento neutro de la segunda operación:

$$f \times a = a \Rightarrow e = b$$
$$f \times b = b \Rightarrow e = b$$

Entonces, el elemento neutro $f = b$ existe y es único. En consecuencia, el anillo $(A, +, \times)$ tiene unidad.

En este caso, el anillo $(A, +, \times)$ cumple las dos propiedades (conmutación y elemento neutro) en la segunda operación; entonces, este tipo de estructura, que conjunta al anillo conmutativo y al anillo con unidad, se conoce como **anillo conmutativo con unidad**.

Dominio entero

Si en un anillo existen elementos que presentan la característica

$$a \neq e, b \neq e \rightarrow a \diamond b = e$$

Donde e es el cero del anillo y además $e \neq f$, siendo f la unidad del anillo. Se dice entonces, que el anillo posee divisores propios de cero. Por el contrario, la estructura que no posee este tipo de elementos se conoce como dominio entero.

Si un anillo conmutativo con unidad $(A, *, \diamond)$ posee la propiedad

$$a \diamond b = e \quad \Rightarrow \quad e = e, b = e$$

Donde e es el cero del anillo, se dice entonces que $(A, *, \diamond)$ es un dominio entero.

Ejemplo 7.29. El anillo $(\mathbb{R}, +, \cdot)$, cuyo cero es 0 y su unidad es 1, es un dominio entero, ya que se cumple $0 \neq 1$; además, si se tiene $a \cdot b = 0$ significa que $a = 0$, $b = 0$ ó $a = b \Rightarrow 0$:

$$a \cdot b = 0$$
$$a \cdot b + c = a$$
$$a(b + 1) = a$$

$$b + 1 = 1$$
$$b = 1 - 1$$
$$b = 0$$

De manera similar se puede demostrar que para este producto a es 0. Por lo tanto, el anillo $(\mathbb{R}, +, \cdot)$ no tiene divisores propios de cero, y es un dominio entero.

Ejemplo 7.30. Sea M el siguiente conjunto:

$$M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{R} \right\}$$

Y las operaciones de suma y multiplicación en las matrices. El sistema $(M, +, \cdot)$ define un anillo con unidad, donde el cero del anillo es

$$O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Y su unidad es

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Se verifica inmediatamente que la matriz nula e identidad son diferentes entre sí. Sin embargo, este anillo si posee divisores propios de cero; es decir,

$$\exists\, A, B \neq O \in M, A \cdot B = O$$

Tomando como caso particular a la matriz

$$A = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$$

Al multiplicarla por si misma se tiene que

$$\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} (1)(1) + (1)(-1) & (1)(1) + (1)(-1) \\ (-1)(1) + (-1)(-1) & (-1)(1) + (-1)(-1) \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Donde se observa que la matriz A es un divisor propio de cero.

Definición de campo

Si a la segunda operación se le agrega la posibilidad de la existencia de elementos inversos, se obtendrá la estructura algebraica más completa: el campo o cuerpo. Dicha estructura contiene las propiedades ya estudiadas en el Álgebra Superior al momento de formalizar el conjunto de los números reales y de los números complejos: cerradura, asociación, conmutación, elemento neutro y elementos inversos para las operaciones de suma y multiplicación; y la distribución de la

multiplicación sobre la suma. $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son los únicos campos numéricos; esto no quiere decir que sean los únicos, ya que pueden establecerse operaciones con conjuntos no-numéricos.

Sea K un conjunto no vacío, y sean $(*)$ y $(\diamond)$ dos operaciones binarias definidas sobre K. El sistema $(K,*,\diamond)$ es un campo, si

Para la primera operación se cumple:

1. La asociación, $a*(b*c)=(a*b)*c$
2. La conmutación, $a*b=b*a$
3. La existencia del elemento neutro, $e*a=a$
4. La existencia de elementos inversos, $\breve{a}*a=e$

Para la segunda operación se cumple:

5. La asociación, $a\diamond(b\diamond c)=(a\diamond b)\diamond c$
6. La conmutación, $a\diamond b=b\diamond a$
7. La existencia del elemento neutro, $f\diamond a=a$
8. La existencia de elementos inversos, $\tilde{a}\diamond a=f, \forall\, a\neq e$
9. La distribución por la izquierda sobre la primera operación, $a\diamond(b*c)=(a\diamond b)*(a\diamond c)$
   La distribución por la derecha sobre la primera operación, $(b*c)\diamond a=(b\diamond a)*(c\diamond a)$

Donde *e* es el cero del campo y *f* es la unidad del campo.

En forma general y compacta, un campo es un sistema $(K,*,\diamond)$ si se demuestra que

- $(K,*)$ es un grupo abeliano.
- $(K-\{e\},\diamond)$ es un grupo abeliano.
- $(\diamond)$ es distributiva sobre $(*)$ tanto por la izquierda como por la derecha.

Ejemplo 7.31. Los sistemas $(\mathbb{R},+,\cdot)$ y $(\mathbb{C},+,\cdot)$ son campos, ya que en ambos conjuntos, con las operaciones de suma y multiplicación se cumplen las 9 propiedades de un campo. Además, se tiene que el cero del campo no tiene inverso en la multiplicación y es diferente de la unidad del campo; en ambos sistemas éstos últimos elementos pertenecen tanto a los números reales como a los números complejos.

Ejemplo 7.32. Sea el conjunto V, definido por:

$$V=\{(x,y,z)|x,y,z\in\mathbb{R}\}$$

Y las operaciones definidas como:

$$(x_1,y_1,z_1)+(x_2,y_2,z_2)=(x_1+x_2,y_1+y_2,z_1+z_2)$$

$$(x_1,y_1,z_1)\oplus(x_2,y_2,z_2)=(x_1x_2,y_1y_2,z_1z_2)$$

Se debe verificar si la estructura $(V, +, \oplus)$ es un campo. En este caso, la primera operación define una suma tradicional de vectores; por lo tanto, las propiedades de la primera operación del campo

son:

- Asociación, $\bar{u} + (\bar{v} + \bar{w}) = (\bar{u} + \bar{v}) + \bar{w}$
- Conmutación, $\bar{u} + \bar{v} = \bar{v} + \bar{u}$
- Elemento neutro, $\bar{e} + \bar{u} = \bar{u} \Rightarrow \bar{e} = \bar{0}$
- Elementos inversos, $\bar{a} + \bar{u} = \bar{e} \Rightarrow \bar{a} = -\bar{u}$

Para todo $\bar{u}, \bar{v}, \bar{w} \in V$.

En la segunda operación es necesario demostrar que las 5 características restantes del campo se satisfacen correctamente.

Asociación:

$$(x_1, y_1, z_1) \oplus [(x_2, y_2, z_2) \oplus (x_3, y_3, z_3)] = [(x_1, y_1, z_1) \oplus (x_2, y_2, z_2)] \oplus (x_3, y_3, z_3)$$
$$(x_1, y_1, z_1) \oplus (x_2 x_3, y_2 y_3, z_2 z_3) = (x_1 x_2, y_1 y_2, z_1 z_2) \oplus (x_3, y_3, z_3)$$
$$(x_1 x_2 x_3, y_1 y_2 y_3, z_1 z_2 z_3) = (x_1 x_2 x_3, y_1 y_2 y_3, z_1 z_2 z_3)$$

Por lo cual, se cumple la propiedad.

Conmutación:

$$(x_2, y_2, z_2) \oplus (x_3, y_3, z_3) = (x_3, y_3, z_3) \oplus (x_2, y_2, z_2)$$
$$(x_2 x_3, y_2 y_3, z_2 z_3) = (x_3 x_2, y_3 y_2, z_3 z_2)$$

Y por la conmutación en la multiplicación de los números reales, se satisface la propiedad.

Elemento neutro:

$$(x, y, z) \oplus (e_1, e_2, e_3) = (x, y, z)$$
$$(x e_1, y e_2, z e_3) =$$

Entonces, se plantean las ecuaciones

$$x e_1 = x$$
$$y e_2 = y$$
$$z e_3 = z$$

Por la multiplicación en los reales se obtiene que el elemento neutro del campo para la segunda operación es $\bar{e} = (1, 1, 1)$; y se satisface la propiedad.

Elementos inversos:

$$(x, y, z) \oplus (a_1, a_2, a_3) = (x, y, z)$$
$$(x a_1, y a_2, z a_3) =$$

Las ecuaciones resultantes son

$$xa_1 = 1$$
$$ya_2 = 1$$
$$za_3 = 1$$

Nuevamente, con la multiplicación en los reales se obtiene que el elemento inverso general del campo en la segunda operación es $\bar{a} = \left(\frac{1}{x}, \frac{1}{y}, \frac{1}{z}\right)$; y esta propiedad se satisface, ya que el único elemento que no tiene inverso es $\bar{0} = (0, 0, 0)$.

Distribución:

$$(x_1, y_1, z_1) \oplus [(x_2, y_2, z_2) + (x_3, y_3, z_3)]$$
$$= [(x_1, y_1, z_1) \oplus (x_2, y_2, z_2)] + [(x_1, y_1, z_1) \oplus (x_3, y_3, z_3)]$$
$$(x_1, y_1, z_1) \oplus (x_2 + x_3, y_2 + y_3, z_2 + z_3) = (x_1x_2, y_1y_2, z_1z_2) + (x_1x_3, y_1y_3, z_1z_3)$$
$$\big(x_1(x_2 + x_3), y_1(y_2 + y_3), z_1(z_2 + z_3)\big) = (x_1x_2 + x_1x_3, y_1y_2 + y_1y_3, z_1z_2 + z_1z_3)$$

Por lo que la distribución por la derecha está satisfecha. La distribución por la izquierda sigue el mismo procedimiento; al basarse en la multiplicación y suma de los números reales; entonces, se concluye que la distribución en ambos sentidos se cumple satisfactoriamente. El sistema $(V, +, \oplus)$ tiene estructura de campo.

Como punto final, se debe notar que un campo es un dominio entero, ya que la existencia de elementos inversos en la segunda operación establece que todos los elementos del campo poseen inverso, excepto el cero del campo; por lo que se concluye que los respectivos elementos neutros de cada operación son diferentes y no existen divisores propios de cero.

Isomorfismos y homomorfismos

Dentro de la Álgebra Moderna pueden establecerse relaciones entre las estructuras algebraicas y sus operaciones. Dichas relaciones permiten intercambiar los símbolos u operaciones de una estructura sin alterar sus propiedades algebraicas o sus resultados.

Homomorfismos

Sean $(G, +)$ y $(G', *)$ dos grupos. Un homomorfismo de A en B es una función $f: A \to B$ tal que

$$f(a + b) = f(a) * f(b) \quad \forall\, a, b \in G$$

El término viene de los vocablos griegos ομός (*homos*, mismo) y μορφή (*morphe*, forma).

Ejemplo 7.33. Sean el grupo

$$M_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| ad - bc \neq 0; a, b, c, d \in \mathbb{R} \right\}$$

Donde se define la multiplicación matricial tradicional, y el grupo $(\mathbb{R}-\{0\},\cdot)$. Si se define la función

$$f(A)=\det A$$

Determínese si $f: A \to \mathbb{R}-\{0\}$ es un homomorfismo.

Al aplicar la definición de isomorfismo se establece que

$$f(A\cdot B)=f(A)\cdot f(B)$$
$$|A\cdot B|=|A|\cdot|B|$$

Por propiedades de los determinantes se sabe que la igualdad es verdadera; por lo tanto, $f: A \to \mathbb{R}-\{0\}$ es un homomorfismo.

Ejemplo 7.34. Sean el anillo $(D_3,+,\cdot)$, donde

$$D_3=\left\{\begin{pmatrix} a & & \\ & b & \\ & & c \end{pmatrix}\middle| a,b,c\in\mathbb{R}\right\}$$

Y el anillo $(\mathbb{C},+,\cdot)$. Determina si la función

$$f\begin{pmatrix} a & & \\ & b & \\ & & c \end{pmatrix}=(a+b)+ci$$

Es un homomorfismo.

En este caso se tienen dos operaciones binarias; por lo tanto, la propiedad del homomorfismo se deberá probar dos veces:

$$f(A+B)=f(A)+f(B)$$

$$f(A\cdot B)=f(A)\cdot f(B)$$

Para toda $A,B\in D_3$. En la primera operación se tiene

$$f\left(\begin{pmatrix} a_1 & & \\ & b_1 & \\ & & c_1 \end{pmatrix}+\begin{pmatrix} a_2 & & \\ & b_2 & \\ & & c_2 \end{pmatrix}\right)=f\begin{pmatrix} a_1 & & \\ & b_1 & \\ & & c_1 \end{pmatrix}+f\begin{pmatrix} a_2 & & \\ & b_2 & \\ & & c_2 \end{pmatrix}$$
$$f\begin{pmatrix} a_1+a_2 & & \\ & b_1+b_2 & \\ & & c_1+c_2 \end{pmatrix}=(a_1+b_1)+c_1i+(a_2+b_2)+c_2i$$
$$(a_1+a_2+b_1+b_2)+(c_1+c_2)i=(a_1+b_1+a_2+b_2)+(c_1+c_2)i$$

Para la segunda operación:

$$f\left(\begin{pmatrix} a_1 & & \\ & b_1 & \\ & & c_1 \end{pmatrix}\cdot\begin{pmatrix} a_2 & & \\ & b_2 & \\ & & c_2 \end{pmatrix}\right)=f\begin{pmatrix} a_1 & & \\ & b_1 & \\ & & c_1 \end{pmatrix}\cdot f\begin{pmatrix} a_2 & & \\ & b_2 & \\ & & c_2 \end{pmatrix}$$

$$f\begin{pmatrix} a_1a_2 & & \\ & b_1b_2 & \\ & & c_1c_2 \end{pmatrix}=[(a_1+b_1)+c_1i]\cdot[(a_2+b_2)+c_2i]$$

$$(a_1a_2+b_1b_2)+(c_1c_2)i=$$

Al realizar las operaciones, se observa que no existe igualdad. Se concluye que la función dada no es un homomorfismo entre los anillos.

Isomorfismos

Se considera que una función $f: A \to A'$ entre dos estructuras algebraicas es un isomorfismo, si además de ser homomorfismo es una función uno-a-uno y sobre; es decir,

- A cada elemento de A le corresponde un asociado en A'.
- Todos los elementos de A se asocian con todos los elementos de A'.
- La función f tiene inversa.
- El elemento neutro de A se transforma en el neutro de A'.

Ejemplo 7.35. Sean los grupos $(\mathbb{R}^+,\cdot)$ y $(\mathbb{R},+)$. Se define la función

$$f(x)=\log_b x$$

Por propiedades de los logaritmos se sabe que

$$f(x\cdot y)=f(x)+f(y)$$
$$\log_b(x\cdot y)=\log_b x+\log_b y$$

Por lo tanto, la función es un homomorfismo. Para verificar si es un isomorfismo se prueba el elemento neutro del primer grupo, que es 1.

$$f(1\cdot 1)=\log_b 1+\log_b 1$$
$$=0$$

Que es el elemento neutro para el segundo grupo.

Para verificar la función inversa se toma a ambos lados la función exponencial en la base b.

$$e^{\log_b(x\cdot y)}=e^{\log_b x+\log_b y}$$
$$=e^{\log_b x}e^{\log_b y}$$
$$=x\cdot y$$

Lo cual indica que si existe la función inversa, entonces la función en *uno-a-uno*. Con respecto a la propiedad *sobre*, todo número real positivo tiene su correspondiente logaritmo dentro de los

números reales. En consecuencia, la función logaritmo entre los grupos $(\mathbb{R}^+,\cdot)$ y $(\mathbb{R},+)$ es un isomorfismo.

Ejemplo 7.36. Sean los grupos $(A,\oplus)$ y $(B,\odot)$, donde $A=\{0,1\}$ y $B=\{a,b\}$ y las operaciones en cada conjunto están definidas por las tablas 7.5 y 7.6, respectivamente.

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

Tabla 7.5.
Operación en A.

$\odot$	a	b
a	a	a
b	a	b

Tabla 7.6.
Operación en B.

Determínese si $f: A \to B$, donde $f(0)=a$ y $f(1)=b$ es un isomorfismo.

Comprobando cada operación se tiene

$$\begin{aligned} f(0\oplus 0) &= f(0)\odot f(0)\\ f(0) &= a\odot a\\ &= a \end{aligned}$$

$$\begin{aligned} f(1\oplus 1) &= f(1)\odot f(1)\\ f(1) &= b\odot b\\ &= b \end{aligned}$$

$$\begin{aligned} f(0\oplus 1) &= f(0)\odot f(1)\\ f(1) &= a\odot b\\ b &= a \end{aligned}$$

Como la última expresión no es cierta, entonces la función dada no es un isomorfismo.

Espacio vectorial

Existe una estructura algebraica donde se definen dos operaciones, que a diferencia del anillo y del campo, una de esas operaciones trabaja con dos conjuntos diferentes. Dicha estructura se conoce como **espacio vectorial**.

Sean dos conjuntos no vacíos V y K, donde K es un campo. En V se definen las operaciones

1. Suma de vectores $\bar{u}+\bar{v}$.
2. Multiplicación por un escalar $\alpha\bar{u}$.

El conjunto V es un espacio vectorial sobre el campo K, si para todo vector $\bar{u},\bar{v},\bar{w}\in V$ y para todo escalar $\alpha,\beta\in K$ se cumple que

1. $\bar{u}+\bar{v}\in V$.
2. $(\bar{u}+\bar{v})+\bar{w}=\bar{u}+(\bar{v}+\bar{w})$.

3. $\bar{u} + \bar{v} = \bar{v} + \bar{u}$.
4. $\bar{u} + \bar{0} = \bar{u}$, donde $\bar{0}$ es el elemento neutro para la suma.
5. $\bar{u} + (-\bar{u}) = \bar{0}$, donde $-\bar{u}$ es el elemento inverso de $\bar{u}$ para la suma.
6. $\alpha\bar{u} \in V$.
7. $(\alpha\beta)\bar{u} = \alpha(\beta\bar{u})$.
8. $(\alpha + \beta)\bar{u} = \alpha\bar{u} + \beta\bar{u}$.
9. $\alpha(\bar{u} + \bar{v}) = \alpha\bar{u} + \alpha\bar{v}$.
10. $(1)\bar{u} = \bar{u}$, donde 1 es la unidad del campo.

Algunos ejemplos de este tipo de estructura son los espacios $\mathbb{R}^n$, los números complejos y reales, los polinomios, y las matrices de orden $m \times n$.

Los espacios vectoriales son el centro del estudio del Álgebra Lineal, la cual permite establecer conceptos, relaciones y justificaciones de métodos y procedimientos utilizados en otras ramas de la Matemática como la Geometría Analítica, el Cálculo, o incluso la misma Álgebra Superior.