

Grupos y Campos

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.

Una operación binaria ($*$) definida en un conjunto S no vacío es una relación que asigna a cada par de elementos $a, b \in S$ una imagen $a * b = c$, que puede o no pertenecer a S .

EJEMPLO 1.1. 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 1.2. La tabla 1.1 especifica la operación binaria AND, que establece una operación lógica utilizada en la electrónica y la computación

\wedge	0	1
0	0	0
1	0	1

Tabla 1.1. 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:

$$0 \cdot 1 = 0 \quad 1 \cdot 0 = 0$$

$$1 \cdot 1 = 1 \quad 0 \cdot 0 = 0$$

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

EJEMPLO 1.3. Sea la siguiente operación binaria

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

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 esa misma naturaleza.

EJEMPLO 1.4. 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

Sea la operación binaria $(*)$, definida en S . Si el resultado de aplicar S está definido dentro del mismo S , entonces $(*)$ es cerrada; es decir, la operación binaria es cerrada si

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

EJEMPLO 1.5. Sea la operación binaria $x \ddagger y = x^y \quad \forall x, y \in \mathbb{Z}$. Se obtiene un resultado que puede o no pertenecer a los números enteros. Si el segundo operando 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.

Existen casos más claros que permiten establecer la cerradura de una operación binaria; el ejemplo clásico es cuando dicha operación está definida por una tabla.

EJEMPLO 1.6. Sea el conjunto $X = \{\ddot{a}, \ddot{o}, \ddot{u}\}$ y la operación definida por la tabla 1.2.

β	\ddot{a}	\ddot{o}	\ddot{u}
\ddot{A}	\ddot{a}	\ddot{o}	\ddot{u}
\ddot{O}	\ddot{o}	\ddot{o}	\ddot{a}
\ddot{U}	\ddot{a}	\ddot{o}	\ddot{u}

Tabla 1.2. Operación Eszett definida para X .

Al aplicar la operación a una pareja de elementos, se puede observar que la operación es cerrada ya que, al buscar el resultado en la tabla, siempre se obtendrá como resultado un elemento del conjunto X ; es decir, la tabla no contiene elementos fuera del conjunto donde se define la operación.

$$\ddot{a} \beta \ddot{o} = \ddot{o} \quad \ddot{u} \beta \ddot{u} = \ddot{u} \quad \ddot{o} \beta \ddot{u} = \ddot{a}$$

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 1.7. 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 1.8. Para el conjunto X y la operación de la tabla 1.2, la asociación no puede cumplirse ya que

$$\ddot{o} \beta (\ddot{o} \beta \ddot{u}) = \ddot{o} \beta \ddot{a} \Rightarrow \ddot{o}$$

$$(\ddot{o} \beta \ddot{o}) \beta \ddot{u} = \ddot{o} \beta \ddot{u} \Rightarrow \ddot{a}$$

que son dos resultados completamente diferentes.

EJEMPLO 1.9. 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 1.10. 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 1.11. 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 1.12. En el conjunto X del ejemplo 1.6 y la operación de la tabla 1.2, se puede verificar que existen dos elementos neutros por la izquierda: \ddot{a} y \ddot{u} .

$$\ddot{a} \beta \ddot{a} = \ddot{a} \quad \ddot{a} \beta \ddot{o} = \ddot{o} \quad \ddot{a} \beta \ddot{u} = \ddot{u}$$

$$\ddot{u} \beta \ddot{a} = \ddot{a} \quad \ddot{u} \beta \ddot{o} = \ddot{o} \quad \ddot{u} \beta \ddot{u} = \ddot{u}$$

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

$$\ddot{a} \beta \ddot{a} = \ddot{a} \quad \ddot{o} \beta \ddot{a} = \ddot{o} \quad \ddot{u} \beta \ddot{a} = \ddot{a}$$

$$\ddot{a} \beta \ddot{u} = \ddot{u} \quad \ddot{o} \beta \ddot{u} = \ddot{a} \quad \ddot{u} \beta \ddot{u} = \ddot{u}$$

Por lo tanto, la operación β 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. Cabe destacar que si no existiese el elemento neutro, entonces tampoco existen los inversos pues ambas propiedades están ligadas.

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

- ✓ $a * \check{a} = e, \forall a \in S$, entonces \check{a} es el elemento inverso de a por la derecha.
- ✓ $\check{a} * a = e, \forall a \in S$, entonces \check{a} es el elemento inverso de a por la izquierda.
- ✓ $a * \check{a} = \check{a} * a \Rightarrow e, \forall a \in S$, entonces \check{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 1.13. 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 1.14. 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 uno 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 1.15. Para la multiplicación de matrices de orden dos 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 1.16. Para el conjunto X y la operación de la tabla 1.2, la conmutación no puede consumarse en los casos

$$\check{a} \text{ } \text{ } \check{u} = \check{u}$$

$$i \circ \ddot{a} = \ddot{a}$$

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

EJEMPLO 1.17. 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:

- ✓ $a * b \in G$
- ✓ $(a * b) * c = a * (b * c)$
- ✓ $\exists e \in G, a * e = e * a \Rightarrow a$
- ✓ $\exists \check{a} \in G, a * \check{a} = \check{a} * a \Rightarrow e$

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

EJEMPLO 1.18. 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. $a + b \in \mathbb{Z}, \forall a, b \in \mathbb{Z}$
2. $(a + b) + c = a + (b + c)$
3. $\exists 0 \in \mathbb{Z}, a + 0 = 0 + a \Rightarrow a$
4. $\exists -a \in \mathbb{Z}, a + (-a) = (-a) + a \Rightarrow 0$

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

$$z_1 \circ z_2 = \overline{z_1 z_2}$$

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

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

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

$$\overline{z_1 z_2} \text{ } z_3 = z_1 \text{ } \overline{z_2 z_3}$$

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

$$z_1 z_2 \overline{z_3} \neq \overline{z_1} z_2 z_3$$

Se obtiene que ambos lados de la igualdad son diferentes; por lo tanto, \mathbb{C} bajo la operación $\text{ } \text{ } \text{ }$ no es un grupo.

EJEMPLO 1.20. 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

$$(x \sim y) \sim z = x \sim (y \sim z)$$

$$2xy \sim z = x \sim 2yz$$

$$2(2xy)z = 2x(2yz)$$

$$4xyz = 4xyz$$

la propiedad asociativa se cumple.

Por otro lado,

$$e \sim x = x$$

$$2ex = x$$

$$2e = 1$$

$$e = \frac{1}{2}$$

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

Finalmente,

$$\check{x} \sim x = e$$

$$2\check{x}x = \frac{1}{2}$$

$$\check{x} = \frac{1}{2x}$$

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 1.21. 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

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

Análogamente,

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

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 1.22. 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.

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

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

EJEMPLO 1.23. Sea M el siguiente conjunto:

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

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 1.24. Sea el conjunto $A = \{a, b\}$ y la operación definida en la tabla 1.3.

+	A	b
a	a	b
b	b	a

Tabla 1.3. Operación binaria en A.

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

Cerradura: todos los resultados posibles en la tabla pertenecen al conjunto; por lo tanto, la operación es cerrada.

Asociación:

$$\begin{aligned} a + (a + b) &= (a + a) + b \\ a + b &= b + a \\ b &= b \end{aligned}$$

$$\begin{aligned} b + (a + a) &= (b + a) + a \\ b + a &= b + a \\ b &= b \end{aligned}$$

$$\begin{aligned} a + (b + a) &= (a + b) + a \\ a + b &= b + a \\ b &= b \end{aligned}$$

$$\begin{aligned} b + (a + b) &= (b + a) + b \\ b + b &= b + b \\ a &= a \end{aligned}$$

$$\begin{aligned} a + (b + b) &= (a + b) + b \\ a + a &= b + b \\ a &= a \end{aligned}$$

$$\begin{aligned} b + (b + a) &= (b + b) + a \\ b + b &= a + a \\ a &= a \end{aligned}$$

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:

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

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

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

Elementos inversos:

$$\check{a} + a = a \Rightarrow \check{a} = a$$

$$\check{b} + b = a \Rightarrow \check{b} = a$$

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

Finalmente, la propiedad conmutativa queda como:

$$\begin{aligned} a + b &= b + a \\ b &= b \end{aligned}$$

La conmutación también es válida para la operación. Por lo tanto, se concluye que $(A, +)$ es un grupo abeliano.

Definición de campo

Supóngase ahora un conjunto con dos operaciones binarias; la estructura que se obtendrá será 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.

Sean K un conjunto no vacío, $(*)$ y (\diamond) dos operaciones binarias cerradas definidas en K . $(K, *, \diamond)$ 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, $\check{a} * a = e$

Para la segunda operación se cumple:

1. La asociación, $a \diamond (b \diamond c) = (a \diamond b) \diamond c$
2. La conmutación, $a \diamond b = b \diamond a$
3. La existencia del elemento neutro, $f \diamond a = a$
4. La existencia de elementos inversos, $\check{a} \diamond a = f, \forall a \neq e$

Para ambas operaciones se cumple:

5. La distribución de la segunda operación sobre la primera, $(b * c) \diamond a = (b \diamond a) * (c \diamond a)$

donde e es el cero del campo (neutro de $*$) y f es la unidad del campo (neutro de \diamond).

EJEMPLO 1.25. 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 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 1.26. Sea el conjunto V , definido por:

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

y las operaciones definidas como:

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

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

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 características restantes del campo se satisfacen correctamente.

Asociación:

$$\begin{aligned} (x_1, y_1, z_1) \oplus [(x_2, y_2, z_2) \oplus (x_3, y_3, z_3)] &= [(x_1, y_1, z_1) \oplus (x_2, y_2, z_2)] \oplus (x_3, y_3, z_3) \\ (x_1, y_1, z_1) \oplus (x_2 x_3, y_2 y_3, z_2 z_3) &= (x_1 x_2, y_1 y_2, z_1 z_2) \oplus (x_3, y_3, z_3) \\ (x_1 x_2 x_3, y_1 y_2 y_3, z_1 z_2 z_3) &= (x_1 x_2 x_3, y_1 y_2 y_3, z_1 z_2 z_3) \end{aligned}$$

Por lo cual, se cumple la propiedad.

Conmutación:

$$\begin{aligned} (x_2, y_2, z_2) \oplus (x_3, y_3, z_3) &= (x_3, y_3, z_3) \oplus (x_2, y_2, z_2) \\ (x_2 x_3, y_2 y_3, z_2 z_3) &= (x_3 x_2, y_3 y_2, z_3 z_2) \end{aligned}$$

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

Elemento neutro:

$$\begin{aligned} (x, y, z) \oplus (e_1, e_2, e_3) &= (x, y, z) \\ (x e_1, y e_2, z e_3) &= \end{aligned}$$

Entonces, se plantean las ecuaciones

$$\begin{aligned} x e_1 &= x \\ y e_2 &= y \\ z e_3 &= z \end{aligned}$$

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:

$$\begin{aligned}(x, y, z) \oplus (a_1, a_2, a_3) &= (x, y, z) \\ (xa_1, ya_2, za_3) &= \end{aligned}$$

Las ecuaciones resultantes son

$$\begin{aligned}xa_1 &= 1 \\ ya_2 &= 1 \\ za_3 &= 1\end{aligned}$$

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:

$$\begin{aligned}(x_1, y_1, z_1) \oplus [(x_2, y_2, z_2) + (x_3, y_3, z_3)] &= [(x_1, y_1, z_1) \oplus (x_2, y_2, z_2)] + [(x_1, y_1, z_1) \oplus (x_3, y_3, z_3)] \\ (x_1, y_1, z_1) \oplus (x_2 + x_3, y_2 + y_3, z_2 + z_3) &= (x_1x_2, y_1y_2, z_1z_2) + (x_1x_3, y_1y_3, z_1z_3) \\ (x_1(x_2 + x_3), y_1(y_2 + y_3), z_1(z_2 + z_3)) &= (x_1x_2 + x_1x_3, y_1y_2 + y_1y_3, z_1z_2 + z_1z_3)\end{aligned}$$

Por lo que la distribución está satisfecha. Entonces, se concluye que la distribución en ambos sentidos se cumple satisfactoriamente. El sistema $(V, +, \oplus)$ tiene estructura de campo.

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 $f: A \rightarrow B$ 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 1.27. Sean el grupo

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

donde se define la multiplicación matricial tradicional, y el grupo $(\mathbb{R} - \{0\}, \times)$, donde (\times) es la multiplicación usual en \mathbb{R} . Si se define la función

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

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

Al aplicar la definición de isomorfismo se establece que

$$\begin{aligned} f(A \cdot B) &= f(A) \times f(B) \\ |A \cdot B| &= |A| \times |B| \end{aligned}$$

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

EJEMPLO 1.28. Sean el anillo $(D_3, +, \cdot)$, donde

$$D_3 = \left\{ \begin{pmatrix} a & & \\ & a & \\ & & a \end{pmatrix} \mid a \in \mathbb{R} \right\}$$

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

$$f \left(\begin{pmatrix} a & & \\ & a & \\ & & a \end{pmatrix} \right) = 3a(2 + i)$$

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

$$\begin{aligned} f \left(\begin{pmatrix} a & & \\ & a & \\ & & a \end{pmatrix} + \begin{pmatrix} b & & \\ & b & \\ & & b \end{pmatrix} \right) &= f \begin{pmatrix} a & & \\ & a & \\ & & a \end{pmatrix} + f \begin{pmatrix} b & & \\ & b & \\ & & b \end{pmatrix} \\ f \begin{pmatrix} a+b & & \\ & a+b & \\ & & a+b \end{pmatrix} &= 3a(2+i) + 3b(2+i) \\ 3(a+b)(2+i) &= (3a+3b)(2+i) \\ 3(a+b)(2+i) &= 3(a+b)(2+i) \end{aligned}$$

Para la segunda operación:

$$f \left(\begin{pmatrix} a & & \\ & a & \\ & & a \end{pmatrix} \cdot \begin{pmatrix} b & & \\ & b & \\ & & b \end{pmatrix} \right) = f \begin{pmatrix} a & & \\ & a & \\ & & a \end{pmatrix} \cdot f \begin{pmatrix} b & & \\ & b & \\ & & b \end{pmatrix}$$

$$f \begin{pmatrix} ab & & \\ & ab & \\ & & ab \end{pmatrix} = [3a(2+i)] \cdot [3b(2+i)]$$

$$3(ab)(2+i) = 9ab(2+i)^2$$

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

Isomorfismos

Se considera que una función $f: A \rightarrow A'$ 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 1.29. 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 .

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

$$= b^{\log_b x} b^{\log_b y}$$

$$= x \cdot y$$

Lo cual indica que si existe la función inversa, entonces la función es *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 1.30. 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 1.5 y 1.6, respectivamente.

\oplus	0	1
0	0	1
1	1	1

Tabla 1.5.
Operación en A.

\odot	a	b
a	a	a
b	a	b

Tabla 1.6.
Operación en B.

Determinese si $f: A \rightarrow B$, 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.