

Apéndice A

Estructuras algebraicas

Definición A.1. Dado X un conjunto no vacío se define una *ley de composición interna* como una función:

$$\begin{aligned} * : X \times X &\rightarrow X \\ (x, y) &\rightarrow *(x, y) = x * y \end{aligned}$$

Algunos ejemplos de leyes de composición interna son:

- | | | |
|-------------------------|--|------------------------------|
| ■ $(\mathbb{N}, +)$ | ■ $(\mathbb{R}, -)$ | ■ $(\mathbb{R}[x], +)$ |
| ■ (\mathbb{N}, \cdot) | ■ $(\mathbb{R}^+, +)$ | ■ $(\mathbb{R}[x], \cdot)$ |
| ■ $(\mathbb{Z}, +)$ | ■ (\mathbb{R}^+, \cdot) | ■ $(\{V, F\}, \wedge)$ |
| ■ (\mathbb{Z}, \cdot) | ■ (\mathbb{R}^+, \div) | ■ $(\{V, F\}, \vee)$ |
| ■ $(\mathbb{Z}, -)$ | ■ $(\mathcal{M}_{n \times n}(\mathbb{R}), +)$ | ■ $(\mathcal{P}(A), \cup)$ |
| ■ $(\mathbb{R}, +)$ | ■ $(\mathcal{M}_{n \times n}(\mathbb{R}), \cdot)$ | ■ $(\mathcal{P}(A), \cap)$ |
| ■ (\mathbb{R}, \cdot) | ■ $(\mathcal{F}_A = \{f : A \rightarrow A\}, \circ)$ | ■ $(\mathcal{P}(A), \Delta)$ |

No son leyes de composición interna:

- | | | |
|---------------------|------------------------|------------------------|
| ■ $(\mathbb{N}, -)$ | ■ (\mathbb{N}, \div) | ■ (\mathbb{R}, \div) |
|---------------------|------------------------|------------------------|

Definición A.2. Una *estructura algebraica* es un conjunto X no vacío dotado de una o varias leyes de composición interna.

A.1. Propiedades básicas

Sea X conjunto no vacío, $* : X \times X \rightarrow X$ y $\diamond : X \times X \rightarrow X$, leyes de composición interna.

Asociatividad. Diremos que $*$ es asociativa si y solo si:

$$\forall x, y, z \in X, \quad x * (y * z) = (x * y) * z$$

La asociatividad es la propiedad más básica que se le puede pedir a una estructura algebraica con ley de composición interna, es por eso que cuando pensamos en leyes de composición interna son estas las que primero asoman por nuestra cabeza, ya que son las que hemos estudiado desde que eramos pequeños. Las operaciones que no tienen esta propiedad no cumplen buenas propiedades y por ello ya no las consideraremos un ejemplo de aquí en adelante.

Son asociativas:

▪ $(\mathbb{N}, +)$	▪ (\mathbb{R}, \cdot)	▪ (\mathcal{F}_A, \circ)	▪ $(\mathcal{P}(A), \cup)$
▪ (\mathbb{N}, \cdot)	▪ $(\mathbb{R}^+, +)$	▪ $(\mathbb{R}[x], +)$	
▪ $(\mathbb{Z}, +)$	▪ (\mathbb{R}^+, \cdot)	▪ $(\mathbb{R}[x], \cdot)$	▪ $(\mathcal{P}(A), \cap)$
▪ (\mathbb{Z}, \cdot)	▪ $(\mathcal{M}_{n \times n}(\mathbb{R}), +)$	▪ $(\{V, F\}, \wedge)$	
▪ $(\mathbb{R}, +)$	▪ $(\mathcal{M}_{n \times n}(\mathbb{R}), \cdot)$	▪ $(\{V, F\}, \vee)$	▪ $(\mathcal{P}(A), \Delta)$

Vale la pena probar el caso de la composición de funciones: Sean $h, g, h \in \mathcal{F}_A$, sabemos que dos funciones son iguales, si la imagen de ambas es igual para cada elemento del dominio, de modo que para probar la asociatividad de (\mathcal{F}_A, \circ) debemos probar que $\forall x \in A ((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x)$. Sea $x \in A$ cualquiera:

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = (f \circ (g \circ h))(x)$$

No son asociativas:

▪ $(\mathbb{Z}, -)$	▪ $(\mathbb{R}, -)$	▪ (\mathbb{R}^+, \div)
---------------------	---------------------	--------------------------

Conmutatividad. Diremos que $*$ es conmutativa si y solo si:

$$\forall x, y \in X, \quad x * y = y * x$$

Si bien, la conmutatividad es una propiedad que usamos regularmente y le atribuimos a muchas operaciones, sin ella aún podemos tener muy buenas propiedades en una estructura algebraica por dar dos ejemplos relevantes podemos considerar: $(\mathcal{M}_{n \times n}(\mathbb{R}), \cdot)$ y (\mathcal{F}_A, \circ) . Es muy frecuente que la demos por hecho, sin ir más lejos existe el dicho popular “el orden de los factores no altera el producto” y, aunque esto es cierto en números reales, naturales, enteros, etc. no es así en la matrices.

Son Conmutativas

▪ $(\mathbb{N}, +)$	▪ $(\mathbb{R}, +)$	▪ $(\mathcal{M}_{n \times n}(\mathbb{R}), +)$	▪ $(\{V, F\}, \vee)$
▪ (\mathbb{N}, \cdot)	▪ (\mathbb{R}, \cdot)	▪ $(\mathbb{R}[x], +)$	▪ $(\mathcal{P}(A), \cup)$
▪ $(\mathbb{Z}, +)$	▪ $(\mathbb{R}^+, +)$	▪ $(\mathbb{R}[x], \cdot)$	▪ $(\mathcal{P}(A), \cap)$
▪ (\mathbb{Z}, \cdot)	▪ (\mathbb{R}^+, \cdot)	▪ $(\{V, F\}, \wedge)$	▪ $(\mathcal{P}(A), \Delta)$

Existencia de neutro. Diremos que $*$ tiene elemento neutro si y solo si:

$$\exists e \in X, \forall x \in X, \quad x * e = e * x = x$$

Esta también es una propiedad muy básica, cabe notar que aunque la operación sea o no conmutativa la operación con el neutro, sea por la derecha o la izquierda debe dar el mismo resultado. En el caso de las estructuras algebraicas conmutativas basta con probar el resultado solo por un lado, pero en las que no lo son se hace indispensable hacer la verificación por izquierda y derecha.

Tienen elemento neutro:

- | | |
|---|--|
| ■ $(\mathbb{N}, \cdot), e = 1$ | ■ $(\mathcal{F}_A, \circ), e = f_{id}, (\forall x \in A, f_{id}(x) = x)$ |
| ■ $(\mathbb{Z}, +), e = 0$ | ■ $(\mathbb{R}[x], +), e = 0$ |
| ■ $(\mathbb{Z}, \cdot), e = 1$ | ■ $(\mathbb{R}[x], \cdot), e = 1$ |
| ■ $(\mathbb{R}, +), e = 0$ | ■ $(\{V, F\}, \wedge), e = V$ |
| ■ $(\mathbb{R}, \cdot), e = 1$ | ■ $(\{V, F\}, \vee), e = F$ |
| ■ $(\mathbb{R}^+, \cdot), e = 1$ | ■ $(\mathcal{P}(A), \cup), e = \emptyset$ |
| ■ $(\mathcal{M}_{n \times n}(\mathbb{R}), +), e = \theta$ (matriz nula) | ■ $(\mathcal{P}(A), \cap), e = A$ |
| ■ $(\mathcal{M}_{n \times n}(\mathbb{R}), \cdot), e = I$ (matriz identidad) | ■ $(\mathcal{P}(A), \Delta), e = \emptyset$ |

No tienen elemento neutro:

- | | |
|---------------------|-----------------------|
| ■ $(\mathbb{N}, +)$ | ■ $(\mathbb{R}^+, +)$ |
|---------------------|-----------------------|

Teorema A.1. Si el neutro existe es único.

Demostración. Por reducción al absurdo, supongamos que existen $e_1, e_2 \in X$ tales que para todo $x \in X$:

$$x * e_1 = e_1 * x = x \tag{A.1}$$

$$x * e_2 = e_2 * x = x \tag{A.2}$$

Luego por (A.2):

$$e_1 = e_1 * e_2$$

pero también por (A.1)

$$e_2 = e_1 * e_2$$

Por lo tanto, $e_1 = e_2$. $\rightarrow \leftarrow$ ■

Existencia de inverso. Dada $(X, *)$ una estructura algebraica con elemento neutro, diremos que $x \in X$ tiene elemento inverso si y solo si:

$$\exists y \in X, \quad x * y = y * x = e$$

(Notación: el inverso de x se denota por x^{-1}).

Observación A.1. Cabe notar que esta es una propiedad de los elementos de X y no de la operación. Además, el neutro siempre tiene inverso que es sí mismo.

Algunas estructuras algebraicas con elemento inverso en todos su elementos son:

- $(\mathbb{Z}, +), e = 0$
- $(\mathbb{R}^+, \cdot), e = 1$
- $(\mathbb{R}[x], +), e = 0$
- $(\mathbb{R}, +), e = 0$
- $(\mathcal{M}_{n \times n}(\mathbb{R}), +), e = \theta$
- $(\mathcal{P}(A), \Delta), e = \emptyset$

Algunas estructuras algebraicas con elemento inverso en algunos de sus elementos aparte del neutro son:

- $(\mathbb{R}, \cdot), e = 1$. Tienen inverso todos excepto 0.
- $(\mathcal{M}_{n \times n}(\mathbb{R}), \cdot), e = I$. Tienen inverso solo las matrices invertibles ($|A| \neq 0$)
- $(\mathcal{F}_A, \circ), e = f_{id}$. Tienen inverso solo las funciones biyectivas.

Algunas estructuras algebraicas con elemento inverso solo para el neutro son:

- $(\mathbb{N}, \cdot), e = 1$
- $(\{V, F\}, \wedge), e = V$
- $(\mathcal{P}(A), \cap), e = A$
- $(\mathbb{Z}, \cdot), e = 1$
- $(\{V, F\}, \vee), e = F$
- $(\mathbb{R}[x], \cdot), e = 1$
- $(\mathcal{P}(A), \cup), e = \emptyset$

Elemento cancelable. Diremos que $a \in X$ es cancelable si y solo si:

$$\begin{aligned} \forall x, y \in X, \quad a * x = a * y &\implies x = y, \\ x * a = y * a &\implies x = y \end{aligned}$$

Algunas estructuras donde todos sus elementos son cancelables son:

- $(\mathbb{N}, +)$
- (\mathbb{R}^+, \cdot)
- (\mathbb{N}, \cdot)
- $(\mathcal{M}_{n \times n}(\mathbb{R}), +)$
- $(\mathbb{Z}, +)$
- $(\mathbb{R}[x], +)$
- $(\mathbb{R}, +)$
- $(\{V, F\}, \wedge)$
- $(\mathbb{R}^+, +)$
- $(\{V, F\}, \vee)$
- (\mathbb{Z}, \cdot) excepto el cero
- (\mathcal{F}_A, \circ) solo las funciones biyectivas y las inyectivas son cancelables por la izquierda
- (\mathbb{R}, \cdot) excepto el cero
- $(\mathcal{M}_{n \times n}(\mathbb{R}), \cdot)$ solo las matrices invertibles
- $(\mathbb{R}[x], \cdot)$ excepto 0.

Elemento absorbente. Diremos que $*$ tiene elemento absorbente si y solo si:

$$\exists a \in X, \forall x \in X, \quad x * a = a * x = a$$

Existen varios ejemplos de elementos absorbentes, 0 con la operación “ \cdot ” en $\mathbb{Z}, \mathbb{R}, \mathbb{C}$, la matriz nula en el producto de matrices, F con la operación \wedge en $\{V, F\}$, etc.

Elemento idempotente. Diremos que $x \in X$ es idempotente si y solo si:

$$x * x = x$$

Claramente si existe el neutro, este siempre es idempotente, pero no es necesariamente el único caso. El caso más simple es en $\{V, F\}$ donde ambos elementos son idempotentes con las operaciones “ \wedge ” y “ \vee ”.

Distributividad. Diremos que \diamond es distributiva con respecto a $*$ si y solo si:

$$\begin{aligned}\forall x, y, z \in X, \quad x \diamond (y * z) &= (x \diamond y) * (x \diamond z) \\ \forall x, y, z \in X, \quad (y * z) \diamond x &= (y \diamond x) * (z \diamond x)\end{aligned}$$

Hasta aquí habíamos estudiado propiedades con solo una ley de composición interna. La distributividad requiere de dos leyes de composición interna. Es importante notar el orden en que van las dos operaciones ya que, por ejemplo, en \mathbb{Z} “ \cdot ” es distributiva con respecto a “ $+$ ”, pero “ $+$ ” no es distributiva con respecto a “ \cdot ”. Por otro lado, sabemos que en $\{V, F\}$ “ \wedge ” es distributiva con respecto a “ \vee ” y “ \vee ” es distributiva con respecto a “ \wedge ”.

A.2. Clasificación de estructuras algebraicas

Dependiendo de las propiedades que cumplen las leyes de composición interna asociadas a una estructura algebraica podemos clasificar estas estructuras. Una clasificación básica es:

A.2.1. Monoide

$(M, *)$ es un monoide si y solo si:

1. $*$ es asociativa
2. $*$ tiene elemento neutro.

Propiedades. Si $(M, *)$ es monoide:

1. El neutro es único.
Ya fue demostrado.
2. Si el inverso existe es único.

Demostración. Por reducción al absurdo, sea $x \in X$ con inverso para la operación $*$, supongamos que existen $y, y' \in X$ tal que $y \neq y'$ y:

$$\begin{aligned}x * y &= y * x = e \\ x * y' &= y' * x = e\end{aligned}$$

Consideramos que:

$$\begin{aligned}y * x &= e & / * y' \\ (y * x) * y' &= e * y' \\ y * (x * y') &= y' & \text{(Por asociatividad y definición de neutro)} \\ y * e &= y' \\ y &= y' \rightarrow \leftarrow\end{aligned}$$

■

3. Si $a \in M$ tiene inverso, entonces a es cancelable.

Demostración. Sea $a \in M$ con inverso a^{-1} . Supongamos que:

$$\begin{array}{ll}
 a * x = a * y & / a^{-1} * \\
 a^{-1} * (a * x) = a^{-1} * (a * y) & \\
 (a^{-1} * a) * x = (a^{-1} * a) * y & \text{(Por asociatividad de *)} \\
 e * x = e * y & \text{(Por definición de inverso)} \\
 x = y & \text{(Por definición de neutro)}
 \end{array}$$

Luego, $a * x = a * y \implies x = y$. Para probar que $x * a = y * a \implies x = y$ se hace de manera análoga. ■

A.2.2. Grupos

Definición A.3. Un grupo es una estructura algebraica $(G, *)$ tal que:

1. $*$ es asociativa
2. $*$ tiene elemento neutro
3. todos los elementos tienen elemento inverso.

Definición A.4. $(G, *)$ es grupo Abeliano si y solo si:

1. $(G, *)$ es grupo
2. $*$ es conmutativa.

Definición A.5. $(G, *)$ es un grupo finito si y solo si:

1. $(G, *)$ es grupo
2. $|G| < \infty$.

Definición A.6. $(G, *)$ es grupo cíclico si y solo si:

1. $(G, *)$ es grupo
2. $\exists a \in G, \forall x \in G, \exists n \in \mathbb{Z}, x = a^n$.

Propiedades. Si $(G, *)$ es grupo:

1. $\forall a, b \in G, \exists! x \in G, a * x = b$

Demostración. Para ver que x existe basta con verificar que $x = a^{-1} * b$ cumple con la ecuación:

$$a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$$

Para ver que x es único, supongamos que existe x e y solución de la ecuación:

$$\left. \begin{array}{l} a * x = b \\ a * y = b \end{array} \right\} \implies a * x = a * y$$

Luego,

$$\begin{array}{ll} a * x = a * y & / a^{-1} * \\ a^{-1} * (a * x) = a^{-1} * (a * y) & \\ (a^{-1} * a) * x = (a^{-1} * a) * y & \text{(Por asociatividad de *)} \\ e * x = e * y & \text{(Por definición de elemento inverso)} \\ x = y & \text{(Por definición de neutro)} \end{array}$$

■

2. $\forall a \in G, a$ es cancelable.
3. Si G es finito, cada línea o columna de la tabla pitagórica de G es una permutación de los elementos de G .
4. Si G es finito, es isomorfo a un grupo de permutaciones.

Subgrupos

Dado $(G, *)$ un grupo se dice H es un subgrupo de G si $H \subseteq G$ y $(H, *)$ es grupo.

Teorema A.2 (Caracterización de subgrupos). *Dado $(G, *)$ un grupo y $H \subseteq G, H \neq \emptyset$. H es un subgrupo de G si y solo si:*

$$\forall h_1, h_2 \in H, h_1 * h_2^{-1} \in H$$

Demostración. En primer lugar, notemos que el teorema plantea una equivalencia, de este modo comenzaremos por probar la implicancia más simple que es: si H es un subgrupo, entonces $\forall h_1, h_2 \in H, h_1 * h_2^{-1} \in H$.

Supongamos que H es subgrupo, entonces se tiene que:

1. $e \in H$
2. $\forall h \in H, h^{-1} \in H$
3. $\forall h, h' \in H, h * h' \in H$

Sean $h_1, h_2 \in H$ cualesquiera. De (2) se tiene que $h_2^{-1} \in H$, como $h_1, h_2^{-1} \in H$ de (3) se deduce que $h_1 * h_2^{-1} \in H$. De este modo como esto se cumple para $h_1, h_2 \in H$ cualesquiera, podemos hacer una generalización universal y tenemos $\forall h_1, h_2 \in H, h_1 * h_2^{-1} \in H$.

Ahora debemos demostrar que si:

$$\forall h_1, h_2 \in H, h_1 * h_2^{-1} \in H \quad (\text{A.3})$$

se cumplen las tres condiciones que ya hemos enumerado. Veamos el caso de (1). De este modo supongamos que se cumple (A.3).

Sea $h \in H$, este existe ya que sabemos que $H \neq \emptyset$, luego instanciamos (A.3) con $h_1 = h_2 = h$, así obtenemos $h * h^{-1} \in H$, pero $h * h^{-1} = e$, luego $e \in H$.

Ahora que ya hemos demostrado que $e \in H$, podemos usar este hecho para demostrar (2). Sea $h \in H$ cualquiera, instanciamos (A.3) con $h_1 = e$ y $h_2 = h$, y obtenemos: $e * h^{-1} \in H$, por definición de e tenemos que $h^{-1} \in H$ y como esto se cumple para h cualquiera, tenemos que $\forall h \in H, h^{-1} \in H$.

Por último demostraremos (3). Como de costumbre, sean $h, h' \in H$ cualesquiera. Nuevamente, basta instanciar (A.3) y obtendremos la propiedad; en este caso; las instancias serán $h_1 = h$ y $h_2 = h'^{-1}$ (recordemos que acabamos de probar que, bajo el supuesto de (A.3) el inverso de un elemento en H también está en H). Así obtenemos: $h * (h'^{-1})^{-1} \in H$, pero como el inverso del inverso es el mismo elemento, tenemos que $h * h' \in H$. Como esto se cumple para $h, h' \in H$ cualesquiera, entonces $\forall h, h' \in H, h * h' \in H$. ■

A.2.3. Anillo

Definición A.7. $(A, *, \diamond)$ es un anillo si y solo si:

1. $(A, *)$ es grupo Abeliano
2. (A, \diamond) es asociativa
3. \diamond es distributiva con respecto a $*$.

Definición A.8. $(A, *, \diamond)$ es un anillo con unidad si y solo si:

1. $(A, *, \diamond)$ es un anillo
2. \diamond tiene neutro.

Definición A.9. $(A, *, \diamond)$ es un anillo conmutativo si y solo si:

1. $(A, *, \diamond)$ es un anillo
2. \diamond es conmutativa.

Propiedades. Sea $(A, +, \cdot)$ un anillo. Se define la ley de composición interna “ $-$ ” como:

$$\forall a, b \in A, \quad a - b = a + (-b)$$

donde $-b$ es el inverso de b para $+$. Entonces, se cumple que:

1. $\forall a \in A, \quad a \cdot 0 = 0 \cdot a = 0$, donde 0 es el neutro para +.

Demostración. Sea $a \in A$ cualquiera,

$$a \cdot 0 = a \cdot (0 + 0)$$

Por distributividad de \cdot con respecto a +

$$\begin{aligned} a \cdot 0 &= (a \cdot 0) + (a \cdot 0) & / + -(a \cdot 0) \\ (a \cdot 0) + -(a \cdot 0) &= [(a \cdot 0) + (a \cdot 0)] + -(a \cdot 0) \end{aligned}$$

Por asociatividad de +

$$(a \cdot 0) + -(a \cdot 0) = (a \cdot 0) + [(a \cdot 0) + -(a \cdot 0)]$$

Como la suma de un número y su opuesto es cero, obtenemos

$$\begin{aligned} 0 &= (a \cdot 0) + 0 \\ 0 &= a \cdot 0 \end{aligned}$$

De este modo $\forall a \in A, a \cdot 0 = 0$. El caso $0 \cdot a = 0$ es análogo. ■

2. $\forall a, b \in A, \quad -(a \cdot b) = (-a) \cdot b = a \cdot (-b)$

Demostración. Sean $a, b \in A$ cualesquiera, probemos que $(a \cdot b) + ((-a) \cdot b) = 0$. Por distributividad

$$(a \cdot b) + ((-a) \cdot b) = (a + (-a)) \cdot b = 0 \cdot b = b$$

El caso $(a \cdot b) + (a \cdot (-b)) = 0$ es análogo. ■

3. $\forall a, b, c \in A, \quad \begin{aligned} a \cdot (b - c) &= (a \cdot b) - (a \cdot c) \quad \text{y} \\ (b - c) \cdot a &= (b \cdot a) - (c \cdot a) \end{aligned}$

Demostración. Sean $a, b, c \in A$ cualesquiera.

$$a \cdot (b - c) = a \cdot (b + (-c)) = (a \cdot b) + (a \cdot (-c)) = (a \cdot b) + -(a \cdot c) = (a \cdot b) - (a \cdot c)$$

Nuevamente el caso $(b - c) \cdot a = (b \cdot a) - (c \cdot a)$ es análogo. ■

Teorema A.3. Sea $(A, +, \cdot)$ un anillo y $\emptyset \neq A' \subseteq A$. A' es subanillo de A si y solo si se cumplen:

$$\forall a, a' \in A', a - a' \in A' \tag{A.4}$$

$$\forall a, a' \in A', a \cdot a' \in A' \tag{A.5}$$

Demostración. Claramente la condición (A.4) garantiza que A' es un subgrupo de A y la condición (A.5) garantiza que \cdot es ley de composición interna en A' , las propiedades de asociatividad y distributividad no es necesario verificarlas ya que se heredan por el hecho que $A' \subseteq A$. ■

Definición A.10. Un anillo $(A, +, \cdot)$ tiene divisores de cero si y solo si:

$$\exists a, b \in A \setminus \{0\}, \quad a \cdot b = 0$$

A.2.4. Cuerpo

Definición A.11. $(K, +, \cdot)$ es cuerpo un si y solo si:

1. $(K, +, \cdot)$ es anillo con unidad.
2. todo elemento distinto de 0 tiene inverso para \cdot .

Definición A.12. $(K, +, \cdot)$ es cuerpo conmutativo un si y solo si:

1. $(K, +, \cdot)$ es cuerpo
2. \cdot es conmutativa.

Propiedades. Si $(K, +, \cdot)$ es un cuerpo, no tiene divisores de cero.

Demostración. Por reducción al absurdo, supongamos que $a \cdot b = 0$ $a \neq 0$ y $b \neq 0$. Como $a \neq 0$ y K es cuerpo, a tiene inverso a^{-1} , luego:

$$\begin{aligned}
 a \cdot b &= 0 & /a^{-1}. \\
 a^{-1} \cdot (a \cdot b) &= a^{-1} \cdot 0 \\
 (a^{-1} \cdot a) \cdot b &= 0 & \text{(Por asociatividad y propiedad (1) de anillos)} \\
 1 \cdot b &= 0 & \text{(Por definición de inverso)} \\
 b &= 0 \rightarrow \leftarrow
 \end{aligned}$$

■

Teorema A.4. Dado $(K, +, \cdot)$ un cuerpo. Sea $(\mathcal{M}_{n \times n}(K), +, \cdot)$ las matrices de $n \times n$ con coeficientes en K , dotadas de la suma componente a componente y el producto:

$$\forall A, B \in \mathcal{M}_{n \times n}(K), [A \cdot B]_{i,j} = A_{i1}B_{1j} + A_{i2}B_{2j} + \cdots + A_{in}B_{nj}$$

Entonces, $(\mathcal{M}_{n \times n}(K), +, \cdot)$ es un anillo con unidad.

Demostración. En primer lugar, notemos que como $(K, +, \cdot)$ es un anillo podemos trabajar con $A_{i1}B_{1j} + A_{i2}B_{2j} + \cdots + A_{in}B_{nj}$ como $\sum_{k=1}^n A_{ik}B_{kj}$. Ya que las propiedades de las sumatorias solo utilizan las propiedades de un anillo.

En primer lugar debemos probar que $(\mathcal{M}_{n \times n}(K), +, \cdot)$ es un grupo Abelian, pero al ser esta una operación componente a componente en un grupo Abelian, podemos heredar todas las propiedades que necesitamos.

En segundo lugar debemos probar que:

1. $(\mathcal{M}_{n \times n}(K), \cdot)$ es asociativo.

$$\begin{aligned}
 [(A \cdot B) \cdot C]_{ij} &= \sum_{k=1}^n [A \cdot B]_{ik} C_{kj} = \sum_{k=1}^n \sum_{l=1}^n (A_{il} \cdot B_{lk}) \cdot C_{kj} \\
 [(A \cdot B) \cdot C]_{ij} &= \sum_{k=1}^n \sum_{l=1}^n (A_{il} \cdot B_{lk} \cdot C_{kj}) \\
 [(A \cdot B) \cdot C]_{ij} &= \sum_{l=1}^n \sum_{k=1}^n (A_{il} \cdot B_{lk} \cdot C_{kj}) \\
 [(A \cdot B) \cdot C]_{ij} &= \sum_{l=1}^n A_{il} \cdot \sum_{k=1}^n (B_{lk} \cdot C_{kj}) \\
 [(A \cdot B) \cdot C]_{ij} &= \sum_{l=1}^n A_{il} \cdot [B \cdot C]_{lj} \\
 [(A \cdot B) \cdot C]_{ij} &= [A \cdot (B \cdot C)]_{ij}
 \end{aligned}$$

2. \cdot es distributivo con respecto a $+$

$$\begin{aligned}
 [A \cdot (B + C)]_{ij} &= \sum_{k=1}^n A_{ik} \cdot [B + C]_{kj} = \sum_{k=1}^n A_{ik} \cdot (B_{kj} + C_{kj}) \\
 [A \cdot (B + C)]_{ij} &= \sum_{k=1}^n ((A_{ik} \cdot B_{kj}) + (A_{ik} \cdot C_{kj})) \\
 [A \cdot (B + C)]_{ij} &= \sum_{k=1}^n (A_{ik} \cdot B_{kj}) + \sum_{k=1}^n (A_{ik} \cdot C_{kj}) \\
 [A \cdot (B + C)]_{ij} &= [A \cdot B]_{ij} + [A \cdot C]_{ij} \\
 [A \cdot (B + C)]_{ij} &= [(A \cdot B) + (A \cdot C)]_{ij}
 \end{aligned}$$

Para probar que $[(A + B) \cdot C]_{ij} = [(A \cdot C) + (B \cdot C)]_{ij}$ se procede de manera análoga.

3. Existe neutro para \cdot .

Sea I la matriz identidad definida como:

$$I_{ij} = \begin{cases} 1 & \text{Si } i = j \\ 0 & \text{Si } i \neq j \end{cases}$$

$$\begin{aligned}
 [A \cdot I]_{ij} &= \sum_{k=1}^n (A_{ik} \cdot I_{kj}) = A_{ij} \cdot I_{jj} = A_{ij} \\
 [I \cdot A]_{ij} &= \sum_{k=1}^n (I_{ik} \cdot A_{kj}) = I_{ii} \cdot A_{ij} = A_{ij}
 \end{aligned}$$

■

A.3. Homomorfismos

Dadas $(X, *)$, (Y, \diamond) estructuras algebraicas y una función $f : X \rightarrow Y$. Se dice que f es un homomorfismo si y solo si:

$$\forall x_1, x_2 \in X, f(x_1 * x_2) = f(x_1) \diamond f(x_2)$$

Además si f es biyectiva, diremos que es un isomorfismo; y si $X = Y$ y f es biyectiva, entonces es un automorfismo.

Teorema A.5. Sean $(X, *)$ e (Y, \diamond) estructuras algebraicas y $f : X \rightarrow Y$ un epimorfismo. Entonces:

1. Si $*$ es asociativa en X , \diamond es asociativa en Y .
2. Si $*$ es conmutativa en X , \diamond es conmutativa en Y .
3. Si $*$ tiene un neutro e_* en X , \diamond tiene un neutro $e_\diamond = f(e_*)$ en Y .
4. Si $(X, *)$ e (Y, \diamond) tienen elemento neutro, entonces si $x \in X$ tiene elemento inverso x^{-1} , $f(x) \in Y$ tiene elemento inverso y $f(x)^{-1} = f(x^{-1})$.

Demostración.

1. Supongamos que f es un homomorfismo sobreyectivo y $(X, *)$ es asociativa. Sean $y, y', y'' \in Y$ cualesquiera, como f es sobreyectiva $\exists x, x', x'' \in X, y = f(x) \quad \wedge \quad y' = f(x') \quad \wedge \quad y'' = f(x'')$. Luego:

$$\begin{aligned} y \diamond (y' \diamond y'') &= f(x) \diamond (f(x') \diamond f(x'')) && \text{(Por definición de homomorfismo)} \\ &= f(x) \diamond f(x' * x'') && \text{(Por definición de homomorfismo)} \\ &= f(x * (x' * x'')) && \text{(Por asociatividad de *)} \\ &= f((x * x') * x'') && \text{(Por definición de homomorfismo)} \\ &= (f(x) \diamond f(x')) \diamond f(x'') && \text{(Por definición de homomorfismo)} \\ &= (y \diamond y') \diamond y'' \end{aligned}$$

Luego, $\forall y, y', y'' \in Y, y \diamond (y' \diamond y'') = (y \diamond y') \diamond y''$

2. Supongamos que f es un homomorfismo sobreyectivo y $(X, *)$ es conmutativa. Sean $y, y' \in Y$ cualesquiera, como f es sobreyectiva $\exists x, x' \in X, y = f(x) \quad \wedge \quad y' = f(x')$. Luego:

$$\begin{aligned} y \diamond y' &= f(x) \diamond f(x') && \text{(Por definición de homomorfismo)} \\ &= f(x * x') && \text{(Por conmutatividad de *)} \\ &= f(x' * x) && \text{(Por definición de homomorfismo)} \\ &= f(x') \diamond f(x) && \text{(Por definición de homomorfismo)} \\ &= y' \diamond y \end{aligned}$$

Luego, $\forall y, y' \in Y, y \diamond y' = y' \diamond y$

3. Supongamos que f es un homomorfismo sobreyectivo y $(X, *)$ tiene neutro e_* . Sea $y \in Y$ cualquiera, como f es sobreyectiva $\exists x \in X, y = f(x)$. Probemos que $f(e_*)$ cumple la función del neutro en Y . Luego:

$$\begin{aligned} y \diamond f(e_*) &= f(x) \diamond f(e_*) = f(x * e_*) = f(x) = y \\ f(e_*) \diamond y &= f(e_*) \diamond f(x) = f(e_* * x) = f(x) = y \end{aligned}$$

Luego, $\forall y \in Y, y \diamond f(e_*) = f(e_*) \diamond y = y$, por lo tanto (Y, \diamond) tiene neutro $e_\diamond = f(e_*)$.

4. Supongamos que f es un homomorfismo sobreyectivo, $(X, *)$ tiene neutro e_* y $x \in X$ tiene inverso x^{-1} . Sea $f(x) \in Y$, probemos que $f(x^{-1})$ cumple la función del inverso de $f(x)$ en Y . Luego:

$$\begin{aligned} f(x) \diamond f(x^{-1}) &= f(x * x^{-1}) = f(e_*) = e_\diamond \\ f(x^{-1}) \diamond f(x) &= f(x^{-1} * x) = f(e_*) = e_\diamond \end{aligned}$$

Luego, $f(x)^{-1}$ existe y es: $f(x^{-1})$.

■

Corolario A.6. Sean $(X, *)$ e (Y, \diamond) estructuras algebraicas y $f : X \rightarrow Y$ un isomorfismo. Entonces:

1. $*$ es asociativa en X si y solo si \diamond es asociativa en Y .
2. $*$ es conmutativa en X si y solo si \diamond es conmutativa en Y .
3. $*$ tiene un neutro e_* en X si y solo si \diamond tiene un neutro $e_\diamond = f(e_*)$ en Y .
4. Si $(X, *)$ e (Y, \diamond) tienen elemento neutro, entonces $x \in X$ tiene elemento inverso x^{-1} si y solo si $f(x) \in Y$ tiene elemento inverso y $f(x)^{-1} = f(x^{-1})$.

Demostración. Basta aplicar el teorema anterior considerando los homomorfismos f y f^{-1} . ■

Definición A.13. Dados $(G, *)$ y (H, \circ) dos grupos y $f : G \rightarrow H$ un homomorfismo, diremos que f es un homomorfismo de grupos.

Teorema A.7. Dados $(G, *)$ y (H, \circ) dos grupos y $f : G \rightarrow H$ un homomorfismo de grupos. Entonces:

- $e_\circ = f(e_*)$
- $f(g)^{-1} = f(g^{-1})$

Demostración.

1. Sea $g \in G$, luego $f(g) \in H$, como H es grupo existe una única solución para la ecuación $f(g) \circ x = f(g)$, esta solución claramente corresponde a e_\circ , pero:

$$f(g) \circ f(e_*) = f(g * e_*) = f(g)$$

Luego $f(e_*)$ cumple la ecuación y como la solución es única $e_\circ = f(e_*)$

2. Sea $g \in G$, luego $f(g) \in H$, como H es grupo existe una única solución para la ecuación $f(g) \circ x = e_\circ$, esta solución claramente corresponde a $f(g)^{-1}$, pero:

$$f(g) \circ f(g^{-1}) = f(g * g^{-1}) = f(e_*) = e_\circ$$

Luego $f(g^{-1})$ cumple la ecuación, y como la solución es única $f(g)^{-1} = f(g^{-1})$

■

A.4. Ejercicios

P1. Estudie las estructuras:

1. $(\mathbb{R}^2, *)$, $(a, b) * (c, d) = (a + c, b + d + 2bd)$
2. Sea $S = \{a + b\sqrt{2} : a, b \in \mathbb{R}\}$, se definen $*$, \diamond tales que:

$$\begin{aligned}x * y &= (a + b\sqrt{2})(c + d\sqrt{2}) \\ x \diamond y &= (a + b\sqrt{2}) + (c + d\sqrt{2})\end{aligned}$$

3. $(\mathbb{N}, *)$, $a * b = \max\{a, b\}$
4. $(\mathbb{N}, *)$, $a * b = \max\{a, b\} - \min\{a, b\}$
5. $S = \{1, 2, 3, 6\}$ estudie $(S, *)$ donde $a * b = \text{MCD}(a, b)$. (MCD = máximo Común Divisor).
6. $S = \{1, 2, 5, 10\}$, (S, \wedge, \vee) donde: $a \vee b = \text{MCD}(a, b)$, $a \wedge b = \text{mcm}(a, b)$ (mcm: mínimo común múltiplo).
7. $X \neq \emptyset$, $(\mathcal{P}(X), \cup, \cap)$
8. $X \neq \emptyset$, $(\mathcal{P}(X), \Delta, \cap)$ donde Δ es la diferencia simétrica.

P2. Sea $G = \{a \in \mathbb{R} : -1 < a < 1\}$ y sea $a * b = \frac{a+b}{1+ab}$ Demuestre que $(G, *)$ es grupo Abeliano.

P3. Sea $(G, *)$ un grupo tal que: $\forall a, b \in G, (a * b)^2 = a^2 * b^2$ (Notación: $a^n = \underbrace{a * \dots * a}_{n \text{ veces}}$).

1. Demuestre que $(G, *)$ es Abeliano.
2. Pruebe que: $\forall n \geq 2, \forall a, b \in G, (a * b)^n = a^n * b^n$

P4. Demuestre que si G es un grupo finito de orden impar, necesariamente algún elemento es su propio inverso.

P5. Sea $(G, *)$ un grupo, y estudie del punto de vista de morfismo, las aplicaciones:

1. $\phi : G \rightarrow G$, $\phi(x) = a * x$
2. $\phi : G \rightarrow G$, $\phi(x) = a^{-1} * x * a$ ¿Qué sucede si G es Abeliano?

P6. Dado un polígono regular convexo de 6 lados. Estudie el grupo de rotaciones asociado. Generalice para polígono regular de n lados.

P7. Sea la permutación $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$. Sea $G = \{p^n : n \in \mathbb{N}\}$ Demuestre que (G, \circ) es un grupo cíclico de orden 6. Estudie los subgrupos.

P8. Sea $G = \left\{ \phi_{a,b} : x \rightarrow ax + \frac{b}{a} : b \in \mathbb{R}, a \neq 0 \right\}$

1. Demuestre que (G, \circ) es un grupo.
2. Demuestre que $G^1 = \{ \phi_b : x \rightarrow x + b : b \in \mathbb{R} \}$ es un subgrupo

P9. Demuestre que $T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, c, d \in \mathbb{Z} \right\}$ es un subanillo de $M_{22}(\mathbb{Z})$ con la suma y el producto de matrices usuales.

P10. Sea $M(\mathbb{Z}_3) = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{Z}_3 \right\}$. Pruebe que $(M, +, \cdot)$ $(+, \cdot$ suma y producto de matrices inducidas por \mathbb{Z}_3) es un cuerpo de 9 elementos y $\left(M \setminus \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}, \cdot \right)$ es un grupo cíclico de orden 8.

P11. Sea $(A, +, \cdot)$ un anillo, definimos: $\text{CE}(A) = \{c \in A : c \cdot x = x \cdot c, \forall x \in A\}$ Demuestre que $\text{CE}(A)$ es un subanillo de A .

P12. Sea $X \neq \emptyset$

1. Demuestre $(\mathcal{P}(X), \Delta, \cap)$ es un anillo.
2. Dado $S \subseteq X$ se define la función $f : \mathcal{P}(X) \rightarrow \mathcal{P}(X)$ $A \rightarrow f(A) = A \cap S$. Pruebe que f es un homomorfismo.

P13. Sea $(A, +, \cdot)$ un anillo, dado $a \in A$, definimos $f_a : A \rightarrow A$ $x \rightarrow f(x) = a \cdot x$. Sea $F_a = \{f_a : a \in A\}$, pruebe que:

1. $(F_a, +, \circ)$ es un anillo con la suma y composición de funciones.
2. $(F_a, +, \circ)$ es isomorfo a $(A, +, \cdot)$ (considere $\varphi : A \rightarrow F_a$ $a \rightarrow \varphi(a) = f_a$)

P14. Estudie las propiedades de $F_{\sqrt{3}} = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$ y de $F_{\sqrt{3}}(\mathbb{R}) = \{a + b\sqrt{3} : a, b \in \mathbb{R}\}$ clasifique las estructuras $(F_{\sqrt{3}}, +, \cdot)$ y $(F_{\sqrt{3}}(\mathbb{R}), +, \cdot)$

P15. Estudie las propiedades de $*$ definida por: $* : (\mathbb{Z}_2 \times \mathbb{Z}_3)^2 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 :$

$$([a]_2, [b]_3) * ([c]_2, [d]_3) = ([a]_2 \odot_2 [c]_2, [b]_3 \oplus_3 [d]_3)$$

P16. Sea $E \neq \emptyset$, sobre E se definen dos leyes de composición interna $*$ y \diamond , son elementos neutros e y f respectivamente, y que cumplen:

$$\forall x, y, u, v \in E, (x * y) \diamond (u * v) = (x \diamond u) * (y \diamond v)$$

1. $e = f$
2. $\forall x, v \in E, x * v = x \diamond v$
3. $*$ es asociativa y conmutativa.

P17. Sea $\mathcal{F} = \{f : f : \mathbb{N} \rightarrow \mathbb{R}\}$. Se define en \mathcal{F} la ley de composición interna $*$ por:

$$(f * g)(n) = \sum_{j=0}^n f(j)g(n-j), \quad \forall n \in \mathbb{N}$$

1. Dadas $f(n) = n$ y $g(n) = 1$ pruebe que:

$$1.1) (g * g)(n) = n + 1$$

$$1.2) (f * g)(n) = \frac{n(n+1)}{2}$$

$$1.3) (f * f)(n) = \frac{n(n+1)(n-1)}{6}$$

2. Pruebe que $*$ es asociativa, conmutativa, posee elemento neutro, distribuye con respecto a $+$ (suma de funciones $(f + g)(n) = f(n) + g(n)$). (Indicación: para demostrar que es asociativa puede usar que $\sum_{i=0}^n \sum_{j=0}^i S_{i,j} = \sum_{j=0}^n \sum_{i=j}^n S_{i,j}$)