Capítulo I.1

Preliminares

Este capítulo tiene como objetivo introducir, de forma breve, los preliminares fundamentales en los que se apoya el presente libro. Dichos preliminares se pueden agrupar en dos bloques, uno centrado en las estructuras algebraicas básicas (véase Subsección I.1.1) y otro en el desarrollo de algunas técnicas elementales del análisis matricial (véase Subsección I.1.2). Para un estudio más profundo de cada uno de estos bloques el lector puede consultar, por ejemplo, los libros [6, 11] y [8, 9], respectivamente.

I.1.1. Estructuras algebraicas básicas

En este libro se trabaja, principalmente, con la estructura de espacio vectorial que se extiende, posteriormente en el Capítulo I.7, a la noción de espacio euclídeo. Por otra parte, el concepto de espacio vectorial se apoya, a su vez, en la estructura de cuerpo. En esta sección se introducen brevemente las estructuras algebraicas básicas que conducen a la noción de cuerpo.

I.1.1.1. Algo de conjuntos

Aunque de manera informal, definimos un conjunto como una colección de objetos que denominamos elementos. Como ejemplos más importantes tenemos los conjuntos $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ que representan los conjuntos de los números naturales[1], enteros, racionales, reales y complejos, respectivamente.

Si A es un conjunto, utilizamos la notación $a \in A$ y $a \notin A$ para indicar, respectivamente, que a es un elemento de (pertenece a) A y que a no es un elemento de (no pertence a) A. Asimismo, si A y B son conjuntos, se dice que B es un subconjunto de A, y se escribe $B \subset A$, si todos los elementos de B son elementos de A; es decir, si $\forall x \in B$ se cumple que $x \in A$. Obsérvese que $A \subset A$ y, por tanto, A es siempre subconjunto de A. Se dice que $A = B$ si A y B tienen exactamente los mismos elementos, lo que

[1] Recordar que el conjunto $\mathbb{N}$ contiene al número 0

es equivalente a exigir que $A \subset B$ y $B \subset A$. Como consecuencia de esta definición se deduce que[2], por ejemplo, $\{a, b, b\} = \{a, b\} = \{b, a\}$.

Seguidamente, introducimos ciertas manipulaciones entre conjuntos, a partir de las cuales se generan nuevos conjuntos. Sean A, B dos conjuntos.

1. Diferencia. Se define el conjunto $A \setminus B = \{x \,|\, x \in A \text{ pero } x \notin B\}$.
   a) Al conjunto $A \setminus A$ se le llama conjunto vacío y se representa como $\emptyset$. Obsérvese que $\emptyset \subset A$.
2. Unión. Se define el conjunto $A \cup B = \{x \,|\, x \in A \text{ o } x \in B\}$.
3. Intersección. Se define el conjunto $A \cap B = \{x \,|\, x \in A \text{ y } x \in B\}$.

Sean $A_1, \ldots, A_n$, conjuntos no vacíos.

4. Producto cartesiano. Se define el conjunto
$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, \ldots, a_n) \text{ donde } a_i \in A_i \; \forall i \in \{1, \ldots, n\}\}$$
   a) A los elementos de $A_1 \times A_2$ se les llama pares, a los de $A_1 \times A_2 \times A_3$ ternas, etc. En general, a los elementos de $A_1 \times \cdots \times A_n$ se les llama n-tuplas.
   b) Si $A_1 = A_2 = \cdots = A_n = A$, la notación se simplifica escribiendo A^n.
5. Partes de un conjunto. Se define las partes de un conjunto A, y se representa como $\mathscr{P}(A)$, como el conjunto formado por todos los subconjuntos de A. Obsérvese que $\emptyset, A \in \mathscr{P}(A)$.

Ejemplo I.1.1.1 $\mathbb{N} \times \mathbb{R} \ni (1, \sqrt{2}) \notin \mathbb{R} \times \mathbb{N}$. $\mathbb{N}^2 \ni (1, 2) \notin \mathbb{N}^3$. $((1/2, 1/3), -2) \in \mathbb{Q}^2 \times \mathbb{Z}$. $\mathscr{P}(A) \ni \emptyset \notin A$ *pero* $\emptyset \subset A$.

A continuación se enuncian algunas propiedades básicas sobre conjuntos, cuya demostración se deja como ejercicio para el lector.

Proposición I.1.1.1 *Sean A, B, C, D conjuntos. Se cumple que*

1. *Si $A \subset B, C \subset D$ entonces $A \times C \subset B \times D$.*
2. $A \times (B \cup C) = (A \times B) \cup (A \times C),\; A \times (B \cap C) = (A \times B) \cap (A \times C)$.
3. $A \cup B = B \cup A,\; A \cap B = B \cap A$.
4. $A \cup A = A,\; A \cap A = A$.
5. $A \cup (B \cup C) = (A \cup B) \cup C,\; A \cap (B \cap C) = (A \cap B) \cap C$.

[2] En general, utilizamos la notación $\{\cdots\}$ para representar conjuntos

6. *$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.*

7. *$A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$.*

8. *Si A es un conjunto de cardinal[3] n, entonces el cardinal de $\mathscr{P}(A)$ es 2^n.*

En la última parte de esta subsección introducimos el concepto de conjunto cociente. Para ello, en primer lugar, hablaremos de correspondencias, aplicaciones, relaciones binarias y relaciones de equivalencia. Pero antes de sumergirnos en el formalismo matemático, veamos la idea que subyace a la construcción. Supongamos que estamos trabajando con un conjunto y, para nuestro estudio, no queremos distinguir entre aquellos elementos que se comportan igual bajo cierto criterio. La idea es construir un nuevo conjunto, en general más pequeño que el primero y por tanto simplificado, en el que todos los elementos que se comportan igual bajo el criterio establecido sean indistinguibles. Al conjunto resultado se le llama conjunto cociente y al criterio se le denomina relación de equivalencia. Como ejemplo ilustrativo de esta idea intuitiva, consideremos el conjunto de monedas que aparece en la Fig. I.1.1, izquierda, y tomemos como criterio el valor de la moneda; es decir, dos monedas del mismo valor se consideran *iguales.* Entonces, el conjunto cociente es el conjunto que aparece en la Fig. I.1.1, derecha. Se pasa así de un conjunto con 28 elementos a un conjunto con 8 elementos.

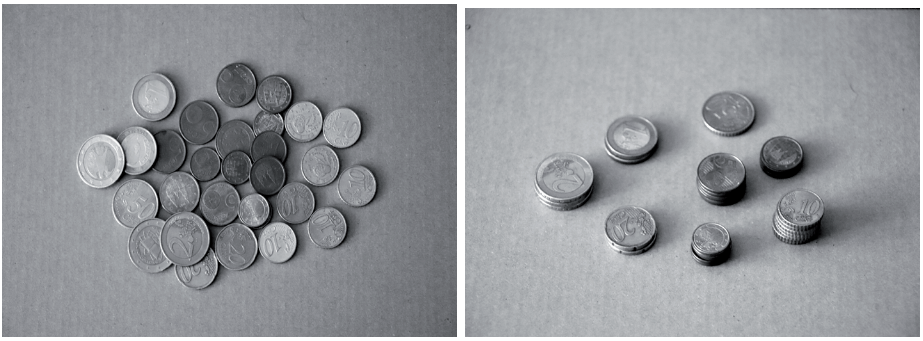

Figura I.1.1: Izquierda: conjunto de partida. Derecha: conjunto cociente

Procedemos ahora con los detalles formales. Sean A y B conjuntos no vacíos. Una **correspondencia de A en B** es una terna $\gamma := (\Gamma, A, B)$, donde $\Gamma \in \mathscr{P}(A \times B)$. A Γ se le llama **grafo de la correspondencia**, a A **conjunto de salida** y a B **conjunto de llegada**. De esta forma, un elemento $a \in A$ se corresponde con aquellos elementos $b \in B$ para los que $(a, b) \in \Gamma$.

[3]Si A es un conjunto con un número de finito n de elementos, se define el **cardinal de A**, y se representa por $\#(A)$, como n

Ejemplo I.1.1.2 *Sea* $A = \{1, 2, 3\}$ *y* $B = \{a, b, c\}$*. Consideramos la correspondencia* $\gamma := (\Gamma = \{(1, a), (1, b), (2, c)\}, A, B)$*. El conjunto de salida es* A*, el de llegada es* B*.* 1 *se corresponde con a y con b,* 2 *se corresponde con c y* 3 *no se corresponde con ningún elemento.*

Una **aplicación** entre los conjuntos no vacíos A y B es una correspondencia $\gamma = (\Gamma, A, B)$ donde todo elemento de A se corresponde exactamente con un elemento de B. Es decir, para todo $a \in A$ se cumple que $\#(\{b \in B \mid (a, b) \in \Gamma\}) = 1$. En el caso de aplicaciones, se suele escribir

$$\begin{array}{rccc} \gamma: & A & \longrightarrow & B \\ & a & \longmapsto & \gamma(a) \end{array}$$

donde $\gamma(a)$ es el único elemento en $\{b \in B \mid (a, b) \in \Gamma\}$.

Ejemplo I.1.1.3 *La correspondencia en el Ejemplo I.1.1.2 no es una aplicación pues* 1 *se corresponde con dos elementos. La correspondencia* $(\{(1, a), (2, c)\}, \{1, 2, 3\}, \{a, b, c\})$ *tampoco es una aplicación pues* 3 *no se corresponde con ningún elemento. Sin embargo* $(\{(1, a), (2, c)\}, \{1, 2\}, \{a, b, c\})$ *sí es una aplicación.*

Una **relación binaria** es una correspondencia donde el conjunto de salida y el de llegada son el mismo. En este caso, si $\mathscr{R} := (\Gamma, A, A)$ y $a, b \in A$, se suele escribir

$$a\mathscr{R}b$$

para indicar que a se corresponde con b; es decir, que $(a, b) \in \Gamma$. Finalmente, una **relación de equivalencia**, en un conjunto no vacío A, es una relación binaria $\mathscr{R}$ que satisface las siguientes propiedades:

1. $\forall a \in A$ se tiene que $a\mathscr{R}a$ (*Propiedad reflexiva*),
2. si $a, b \in A$ son tales que $a\mathscr{R}b$ entonces $b\mathscr{R}a$ (*Propiedad simétrica*),
3. si $a, b, c \in A$ son tales que $a\mathscr{R}b$ y $b\mathscr{R}c$ entonces $a\mathscr{R}c$ (*Propiedad transitiva*).

Estamos ya en condiciones de introducir el concepto de conjunto cociente. Dada una relación de equivalencia en A, $\mathscr{R}$, se define el **conjunto cociente** de A respecto $\mathscr{R}$, y se representa por $A/\mathscr{R}$, como el conjunto

$$A/\mathscr{R} = \{[a], \mid a \in A\}$$

donde

$$[a] = \{x \in A \mid x\mathcal{R}a\}.$$

Al conjunto $[a]$ se le llama **clase de equivalencia** y a a **representante de la clase**. En el ejemplo de las monedas, las clases de equivalencia son cada uno de los *montoncitos* que componen el conjunto de la derecha en la Fig. I.1.1.

En la siguiente proposición se enuncian las propiedades fundamentales de un conjunto cociente.

Proposición I.1.1.2 *Sea A un conjunto no vacío y $\mathscr{R}$ una relación de equivalencia en A. Se verifica que*

1. $\forall a \in A$, $[a] \neq \emptyset$.
2. $\forall a, b \in A$, *si* $b \in [a]$ *entonces* $a \in [b]$.
3. $\forall a, b \in A$, $[a] = [b]$ *si y sólo si* $a\mathscr{R}b$.
4. $\forall a, b \in A$, *si* $[a] \neq [b]$ *entonces* $[a] \cap [b] = \emptyset$.
5. $A = \cup_{a \in A}[a]$.

Ejemplo I.1.1.4 *Sea m un número entero positivo. En $\mathbb{Z}$ consideramos la relación binaria: si $x, y \in \mathbb{Z}$, entonces $x\mathscr{R}y$ si y sólo si m divide a $x - y$. Veamos, en primer lugar, que $\mathscr{R}$ es una relación de equivalencia.*

1. *Propiedad reflexiva: para todo $x \in \mathbb{Z}$ se cumple que m divide a $x - x = 0$ y, por tanto, $x\mathscr{R}x$.*
2. *Propiedad simétrica: sean $x, y \in \mathbb{Z}$ tal que $x\mathscr{R}y$. Entonces m divide a $x - y$. Por tanto, m divide a $y - x$ y en consecuencia $y\mathscr{R}x$.*
3. *Propiedad transitiva: sean $x, y, z \in \mathbb{Z}$ tal que $x\mathscr{R}y$ e $y\mathscr{R}z$. Entonces m divide a $x - y$ y también a $y - z$. Es decir, existen $a, b \in \mathbb{Z}$ tal que $x - y = am, y - z = bm$. Entonces, $x - z = (a + b)m$. Por tanto, $x\mathscr{R}z$.*

A continuación determinamos el conjunto cociente $\mathbb{Z}/\mathscr{R}$. Observamos que si m divide a $a - b$, con $a, b \in \mathbb{Z}$, entonces existe $\lambda \in \mathbb{Z}$ tal que $a = b + \lambda m$. Por tanto, la clase de equivalencia de a es

$$[\,a\,] = \{a + \textit{múltiplos de } m\}.$$

Además,

$$\mathbb{Z}/\mathscr{R} = \{[0], \ldots, [m - 1]\}.$$

Este conjunto cociente se suele representa como $\mathbb{Z}_m$, a m se le llama módulo y a la relación de equivalencia $\mathscr{R}$ se le denomina "congruencia módulo m" y se suele escribir

$$a \equiv b \textit{ mod } m$$

para indicar que a y b están relacionados.

I.1.1.2. El concepto de grupo

Seguidamente se estudia el concepto de grupo, que permitirá llegar a la noción de cuerpo. Para ello, previamente, se definen las estructuras de grupoide, semigrupo y monoide (véase Fig. I.1.2).

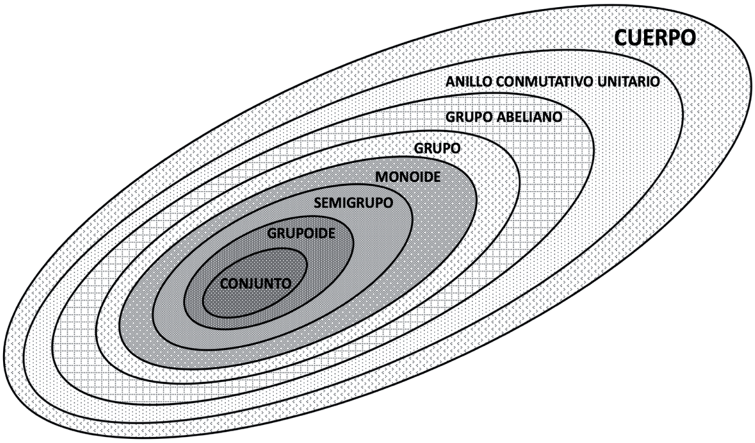

Figura I.1.2: Estructuras algebraicas

Definición I.1.1.1 *Sea $A \neq \emptyset$ un conjunto no vacío. Una* operación interna en *A es una aplicación de $A \times A$ en A. Es decir, una operación interna asigna a cada par de elementos de A un único elemento de A.*

Definición I.1.1.2 *Sea $A \neq \emptyset$ un conjunto no vacío y $\star$ una operación interna en A. Entonces se dice que $(A, \star)$ es un* grupoide.

Observación I.1.1.1 *Si $(A, \star)$ es un grupoide y $x, y \in A$, se escribe $x \star y$ para representar el resultado de la operación de x con y, vía la operación interna $\star$.*

En la siguiente definición se van incluyendo progresivamente propiedades hasta llegar a la noción de grupo abeliano.

Definición I.1.1.3 *Sea $(A, \star)$ un grupoide. Se dice que*

1. *$(A, \star)$ es un* semigrupo *si se cumple la propiedad asociativa. Es decir,*

$$\forall x, y, z \in A \text{ se cumple que } (x \star y) \star z = x \star (y \star z).$$

2. *$(A, \star)$ es un* monoide *si es un semigrupo y además existe* elemento neutro. *Es decir,*

$$\exists e \in A \text{ tal que } \forall x \in A \text{ se cumple que } e \star x = x = x \star e.$$

   A e se le llama elemento neutro.

3. $(A, \star)$ *es un* grupo *si es un monoide y además todo elemento tiene* elemento inverso. *Es decir,*

$$\forall x \in A \textit{ existe un elemento } y \in A \textit{ tal que } x \star y = y \star x = e.$$

A y *se le llama* elemento inverso de x *y se suele representar como* x^{-1}*; salvo cuando la operación es la suma en cuyo caso se escribe* $-x$ *y se llama* opuesto de x.

4. $(A, \star)$ *es un* grupo abeliano (o conmutativo) *si es un grupo y se cumple la propiedad conmutativa. Es decir,*

$$\forall x, y \in A \textit{ se cumple que } x \star y = y \star x.$$

Observación I.1.1.2

1. *El elemento neutro, si existe, es único.*

2. *En un monoide, el elemento inverso, si existe, es único. Esta propiedad no se verifica en general en un grupoide no asociativo con elemento neutro.*

Para terminar esta subsección, en la Tabla I.1.1 se analiza la estructura algebraica de algunos de los conjuntos de números más importantes. De forma más concreta, se estudian $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, el conjunto de los múltiplos de un número entero positivo m (que representamos como $m\mathbb{Z}$), el conjunto de los enteros gaussianos

$$\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} \mid a, b \in \mathbb{Z}\}$$

y el conjunto de los racionales gaussianos

$$\mathbb{Q}(\mathrm{i}) = \{a + b\mathrm{i} \mid a, b \in \mathbb{Q}\}.$$

I.1.1.3. El concepto de cuerpo

Finalmente llegamos al concepto de cuerpo. En la subsección anterior hemos considerado sólo una operación y hemos exigido la estructura de grupo abeliano. Ahora, introducimos una segunda operación y exigimos también la estructura de grupo abeliano respecto a la segunda operación, previa exclusión del elemento neutro respecto a la primera operación.

Definición I.1.1.4 *Sea* $A \neq \emptyset$ *un conjunto no vacío en el que consideramos dos operaciones internas, que convenimos en llamar suma y multiplicación y que representamos por "+" y "·". Se dice que* $(A, +, \cdot)$ *es un* anillo *si se verifica que*

1. $(A, +)$ *es un grupo abeliano.*

Conjunto	$\star$	Grupoide	Semigrupo	Monoide	Grupo	Grupo Abel.
$\mathbb{N}$	$+$	x	x	x		
$\mathbb{N}$	$\cdot$	x	x	x		
$\mathbb{Z}$	$+$	x	x	x	x	x
$\mathbb{Z}$	$\cdot$	x	x	x		
$m\mathbb{Z}$	$+$	x	x	x	x	x
$m\mathbb{Z}$	$\cdot$	x	x			
Impares	$+$					
Impares	$\cdot$	x	x	x		
$\mathbb{Q}$	$+$	x	x	x	x	x
$\mathbb{Q}$	$\cdot$	x	x	x		
$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$	$\cdot$	x	x	x	x	x
$\mathbb{R}$	$+$	x	x	x	x	x
$\mathbb{R}$	$\cdot$	x	x	x		
$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$	$\cdot$	x	x	x	x	x
$\mathbb{C}$	$+$	x	x	x	x	x
$\mathbb{C}$	$\cdot$	x	x	x		
$\mathbb{C}^* = \mathbb{C} \setminus \{0\}$	$\cdot$	x	x	x	x	x
$\mathbb{Z}[\mathrm{i}]$	$+$	x	x	x	x	x
$\mathbb{Z}[\mathrm{i}]$	$\cdot$	x	x	x		
$\mathbb{Q}(\mathrm{i})$	$+$	x	x	x	x	x
$\mathbb{Q}(\mathrm{i})$	$\cdot$	x	x	x		
$\mathbb{Q}(\mathrm{i})^* = \mathbb{Q}(\mathrm{i}) \setminus \{0\}$	$\cdot$	x	x	x	x	x

Tabla I.1.1: Estructura algebraica, respecto a una operación, de los principales conjuntos

2. *$(A, \cdot)$ es un semigrupo.*

3. *Para todo $x, y, z \in A$ se cumple que*[4]

$$x(y+z) = xy + xz, \ \ (y+z)x = yx + zx.$$

Si además

4. *$(A, \cdot)$ es un monoide, se dice que $(A, +, \cdot)$ es un* **anillo unitario**. *En un anillo unitario, a los elementos invertibles respecto a la multiplicación se les llama* **unidades**; *representamos por $\mathscr{U}(A)$ al conjunto de unidades de A.*

Si

5. *$(A, +, \cdot)$ cumple todo lo anterior y además la operación "$\cdot$" es conmutativa, se dice que $(A, +, \cdot)$ es un* **anillo conmutativo unitario**.

[4]En lo que sigue, abusando de la notación, omitiremos el símbolo "$\cdot$" al escribir el producto de dos elementos.

Observación I.1.1.3 *En un anillo unitario $(A, +, \cdot)$ al elemento neutro respecto de "$+$" se le llama* cero *de A y se representa por 0_A o simplemente por 0. Similarmente, al elemento neutro respecto de "$\cdot$" se le llama* uno *de A y se representa por 1_A o simplemente por 1.*

Ejemplo I.1.1.5 *Sea A el conjunto de las funciones continuas de $\mathbb{R}$ en $\mathbb{R}$ y sean "$+$" y "$\cdot$" la suma y multiplicación usual de funciones, respectivamente. Entonces $(A, +, \cdot)$ es un anillo conmutativo unitario y su elemento 1 es la función constante*

$$\begin{array}{rccc} 1_A : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & 1 \end{array}$$

En un anillo (conmutativo) unitario A, se verifica que $(\mathscr{U}(A), \cdot)$ es un grupo (abeliano). Si este grupo resulta ser $A \setminus \{0_A\}$ aparece la noción de cuerpo. De forma más precisa.

Definición I.1.1.5 *Un* cuerpo *es un anillo conmutativo unitario $(\mathbb{K}, +, \cdot)$ en el que $\mathscr{U}(\mathbb{K}) = \mathbb{K} \setminus \{0_{\mathbb{K}}\}$.*

Observación I.1.1.4 *En un cuerpo $\mathbb{K}$ se verifican las siguientes propiedades básicas:*

1. *$\forall a \in \mathbb{K}$ se verifica que $a \cdot 0 = 0 \cdot a = 0$.*
2. *$\forall a, b \in \mathbb{K}$ se verifica que $(-a) \cdot b = -(a \cdot b)$, $a \cdot (-b) = -(a \cdot b)$, $(-a) \cdot (-b) = a \cdot b$.*
3. *Si $a, b \in \mathbb{K}$ son tal que $a \cdot b = 0$ entonces $a = 0$ o $b = 0$.*

Finalmente, en la Tabla I.1.2 se analiza la estructura de los grupos abelianos aditivos, vistos en la Tabla I.1.1, al incluir la multiplicación.

	Anillo conm.	Anillo conm. unitario	cuerpo
$(m\mathbb{Z}, +, \cdot)$	x		
$(\mathbb{Z}, +, \cdot)$	x	x	
$(\mathbb{Q}, +, \cdot)$	x	x	x
$(\mathbb{R}, +, \cdot)$	x	x	x
$(\mathbb{C}, +, \cdot)$	x	x	x
$(\mathbb{Z}[\mathrm{i}], +, \cdot)$	x	x	
$(\mathbb{Q}(\mathrm{i}), +, \cdot)$	x	x	x

Tabla I.1.2: Estructura algebraica, respecto a dos operaciones, de los principales conjuntos

I.1.2. Análisis matricial básico

En esta sección se recuerdan algunas cuestiones relativas al análisis matricial, desde unas primeras definiciones y propiedades asociadas a matrices, la triangulación gaussiana, determinante, el cálculo del rango de una matriz por Gauss y la resolución de sistemas mediante Gauss $PA = LU$. Para ello, en todo lo que sigue, se asume que $\mathbb{K}$ es un cuerpo.

I.1.2.1. Primeras definiciones y propiedades

Comenzamos con el concepto de matriz y submatriz.

Definición I.1.2.1 *Una* matriz de orden $m \times n$ *sobre un cuerpo* $\mathbb{K}$ *es una tabla* A *de* m *filas y* n *columnas, formada por elementos* $a_{ij} \in \mathbb{K}$*, del tipo*

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

Una submatriz *de* A *es una matriz formada a partir de* A *suprimiendo filas y/o columnas. Se llama* diagonal principal *de* A *a la diagonal formada por los elementos de la forma* a_{ii}*.*

Se escribe $A = (a_{ij})_{1\leq i\leq m, 1\leq j\leq n}$ o bien $A = (a_{ij})_{1\leq i,j\leq n}$ si la matriz es cuadrada.

Observación I.1.2.1

1. *La* matriz nula $m \times n$ *se define como la matriz* $A = (a_{ij})_{1\leq i\leq m,1\leq j\leq n}$ *donde* $a_{ij} = 0\ \forall i\ \forall j$*; se representa por* $\mathbf{0}$*.*
2. *La* matriz identidad $n \times n$ *se define como la matriz* $A = (a_{ij})_{1\leq i,j\leq n}$ *donde* $a_{ii} = 1\ \forall i$ *y* $a_{ij} = 0$ *si* $i \neq j$*; se representa por* I*.*

Dadas dos matrices $m \times n$, $A = (a_{ij})_{1\leq i\leq m,1\leq j\leq n}$ y $B = (b_{ij})_{1\leq i\leq m,1\leq j\leq n}$, se define la suma de A con B como la matriz $m \times n$

$$A + B = (a_{ij} + b_{ij})_{1\leq i\leq m,1\leq j\leq n}.$$

Si $\lambda \in \mathbb{K}$, se define la multiplicación de λ por A como la matriz $m \times n$

$$\lambda A = (\lambda a_{ij})_{1\leq i\leq m,1\leq j\leq n}.$$

Si $A = (a_{ij})_{1\leq i\leq m,1\leq j\leq n}$ es una matriz $m \times n$ y $B = (b_{ij})_{1\leq i\leq n,1\leq j\leq p}$ es una matriz $n \times p$, se define la multiplicación de A por B como la matriz $m \times p$

$$A \cdot B = (c_{ik})_{1\leq i\leq m,1\leq k\leq p}$$

donde $c_{ik} = \sum_{\ell=1}^{n} a_{i\ell} b_{\ell k}$.

Proposición I.1.2.1 *Sean* A, B, C *matrices con los tamaños adecuados,* $\lambda, \mu \in \mathbb{K}$*,* $\mathbf{0}$ *la matriz nula e* I *la matriz identidad. Se verifica que*

1. $A + (B + C) = (A + B) + C$
2. $A + \mathbf{0} = \mathbf{0} + A$
3. $A + (-A) = (-A) + A = \mathbf{0}$
4. $A + B = B + A$
5. $\lambda(A + B) = \lambda A + \lambda B$
6. $(\lambda + \mu)A = \lambda A + \mu A$
7. $\lambda(\mu A) = (\lambda\mu)A$
8. $1\,A = A$
9. $A(BC) = (AB)C$
10. $A\,\mathrm{I} = \mathrm{I}\,A = A$
11. $A(B + C) = AB + AC$

Existen distintos tipos de matrices cuya importancia justifica que les sea asignado un nombre concreto. Se exponen a continuación algunos de estos tipos:

1. Matriz fila: $m = 1$; matriz columna: $n = 1$; matriz cuadrada: $m = n$.
2. Matriz triangular superior: A es cuadrada y $a_{ij} = 0\ \forall i > j$; matriz triangular inferior: A es cuadrada y $a_{ij} = 0\ \forall i < j$.
3. Matriz diagonal: $m = n$ y $a_{ij} = 0\ \forall i \neq j$.
4. Matriz traspuesta: si $A = (a_{ij})_{1 \le i \le m, 1 \le j \le n}$, la matriz traspuesta de A se representa por A^T y se define como $A^T = (a_{ji})_{1 \le j \le n, 1 \le i \le m}$.
5. Matriz simétrica: $A = A^T$;
6. Matriz antisimétrica: $A = -A^T$.
7. Matriz ortogonal: $A \cdot A^T = I$.
8. Matriz hermítica: Si A es una matriz cuadrada sobre $\mathbb{C}$, entonces $A = \overline{(A^T)}$, es decir, $a_{i,j} = \overline{a_{j,i}}$, donde $\overline{a}$ representa al conjugado del número complejo a.

Se exponen a continuación algunas propiedades de la matriz traspuesta. Todas las demostraciones de estas propiedades pueden deducirse de forma directa a partir de la definición de matriz traspuesta.

Proposición I.1.2.2 *Sean A, B matrices con los tamaños adecuados y $\lambda \in \mathbb{K}$. Se verifica que*

1. $(A^T)^T = A$.
2. $(\lambda A)^T = \lambda A^T$.
3. $(A + B)^T = A^T + B^T$.
4. $(A \cdot B)^T = B^T \cdot A^T$.

Proposición I.1.2.3 *Sean A, B matrices con los tamaños adecuados y $\mathbb{K} = \mathbb{C}$. Se verifica que*

1. $\overline{\overline{A}} = A$.
2. $\overline{A+B} = \overline{A} + \overline{B}$.
3. $\overline{A \cdot B} = \overline{A} \cdot \overline{B}$.
4. $\overline{A}^T = \overline{A^T}$.

I.1.2.2. Determinante de una matriz

Asociado al concepto de matriz cuadrada se encuentra el de determinante. De acuerdo con la manera en la que presentamos este concepto, se necesitan algunas nociones previas, relativas a permutaciones de números que pasamos a describir.

Una permutación de los números $\{1, \ldots, n\}$ es una disposición ordenada de todos ellos sin repetir ninguno. Se representa por S_n al conjunto de todas las permutaciones de $\{1, \ldots, n\}$; obsérvese que el cardinal de S_n es $n!$.

Sea $\sigma = (i_1, \ldots, i_n) \in S_n$. Se define el índice de σ, y se representa por $\epsilon(\sigma)$, como el número de veces que $i_j < i_k$ siendo $k < j$.

Definición I.1.2.2 *Se define el* determinante *de* $A = (a_{ij})_{1 \leq i,j \leq n}$ *como*

$$\det(A) = \sum_{\sigma=(i_1,\ldots,i_n)\in S_n} (-1)^{\epsilon(\sigma)} a_{1i_1} \cdots a_{ni_n}.$$

$\det(A)$ *también se suele representar por* $|A|$.

Observación I.1.2.2 *Aplicamos la Definición I.1.2.2 al caso de órdenes 1,2,3.*

1. *Caso* $n = 1$. *Sea* $A = (a_{11})$. $S_1 = \{(1)\}$ *y*

$$\det(A) = (-1)^{\epsilon((1))} a_{11} = (-1)^0 a_{11} = a_{11}.$$

2. *Caso* $n = 2$. *Sea* $A = (a_{ij})_{1 \leq i,j \leq 2}$. *Entonces*

$$S_2 = \{\sigma_1 = (1,2), \sigma_2 = (2,1)\}$$

Así,

$$\det(A) = (-1)^{\epsilon(\sigma_1)} a_{11}a_{22} + (-1)^{\epsilon(\sigma_2)} a_{12}a_{21} = a_{11}a_{22} - a_{12}a_{21}.$$

3. *Caso* $n = 3$. *Sea* $A = (a_{ij})_{1 \leq i,j \leq 3}$. *Entonces*

$$\begin{aligned} S_3 = \; & \{\sigma_1 = (1,2,3), \sigma_2 = (1,3,2), \sigma_3 = (2,1,3), \\ & \sigma_4 = (2,3,1), \sigma_5 = (3,1,2), \sigma_6 = (3,2,1)\} \end{aligned}$$

Así,

$$\begin{aligned} \det(A) &= (-1)^{\epsilon(\sigma_1)} a_{11}a_{22}a_{33} + (-1)^{\epsilon(\sigma_2)} a_{11}a_{23}a_{32} + (-1)^{\epsilon(\sigma_3)} a_{12}a_{21}a_{33} \\ &\quad + (-1)^{\epsilon(\sigma_4)} a_{12}a_{23}a_{31} + (-1)^{\epsilon(\sigma_5)} a_{13}a_{21}a_{32} + (-1)^{\epsilon(\sigma_6)} a_{13}a_{22}a_{31} \\ &= a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}. \end{aligned}$$