Tema 2

Estructuras algebraicas básicas

2.1. Operación interna

Definición 29. *Dados tres conjuntos A, B y C, se llama* ***ley de composición*** *en los conjuntos A y B y resultado en el conjunto C, y se denota por "$\oplus$", a una aplicación*[1]*:*

$$\begin{array}{rcl} \oplus : A \times B & \longrightarrow & C \\ (a,b) & \longrightarrow & f(a,b) = a \oplus b = c \in C \end{array}$$

Definición 30. *Dada $\oplus : A \times B \to C$, se dirá que la ley de composición $\oplus$ es* ***interna*** *si $A = B = C$.*

Por lo tanto, una ley de composición $\oplus : A \times A \to A$ es una ley de composición interna.[2]

Ejemplo 23. *La suma y el producto ordinarios en $\mathbb{R}$, denotados respectivamente por "$+$" y "$\cdot$", son leyes de composición interna:*

$$\begin{array}{rcl} + : \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ (x,y) & \longrightarrow & z = x + y \end{array} \qquad \begin{array}{rcl} \cdot : \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ (x,y) & \longrightarrow & z = x \cdot y \end{array}$$

Ejemplo 24. *La operación* resta *no es una operación interna en $\mathbb{N}$, ya que el resultado de restar entre sí números naturales puede producir números negativos, que no están en $\mathbb{N}$. Por ejemplo: $1, 2 \in \mathbb{N}$ pero $1 - 2 = -1 \notin \mathbb{N}$.*

[1] A una ley de composición de $A \times B \to C$ se le conoce, también, con el nombre de **operación binaria**. La notación $\oplus$ es arbitraria, y podría elegirse cualquier otra. A lo largo de este capítulo se utilizarán diversos símbolos para representar este tipo de leyes de composición: $\oplus$, $\otimes$, $\odot$, $*$, $\cdot$, $+$, $\cdot$.

[2] Una ley de composición interna se llama, también, **operación binaria interna** u operación interna.

De la misma forma, la operación división no es interna en ninguno de los conjuntos numéricos habituales $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$, ya que el resultado que se obtendría al dividir entre 0 no está definido en ninguno de estos conjuntos.

Visto desde otra perspectiva: sólo determinadas operaciones resultan internas en cada conjunto. Así pues, parece necesario definir las leyes que no son internas:

Definición 31. *Dados dos conjuntos A y B, se llama* ***ley de composición externa*** *a una aplicación $A \times A \to B$, que a todo par de elementos de A asocia un elemento de B.*

La resta entre números naturales, del ejemplo anterior, resulta así una operación externa de la forma $\mathbb{N} \times \mathbb{N} \to \mathbb{Z}$.

Pero existe otra forma de ley de composición externa, con dos variantes:

Definición 32. *Dados dos conjuntos A y B, se dice que una aplicación de la forma:*

$$\begin{aligned} \odot \ : A \times B &\longrightarrow A \\ (a, b) &\longrightarrow c = a * b \end{aligned}$$

es una ***ley de composición externa por la derecha****, y a los elementos del conjunto B se les llama* ***multiplicadores*** *o* ***escalares*** *de la operación*[3]*.*

Si la aplicación es de la forma:

$$\begin{aligned} \odot \ : B \times A &\longrightarrow A \\ (b, a) &\longrightarrow c = b \odot a \end{aligned}$$

se dirá que es una ***ley de composición externa por la izquierda****.*

Ejemplo 25. *Un ejemplo típico de operación externa es el producto de un escalar por vector en un espacio vectorial, que se verá con detalle en la sección siguiente. Si llamamos K al conjunto de escalares (cuerpo) sobre el que definiremos el espacio vectorial V, un producto de un* escalar *de K por un* vector *de V será de la forma:*

$$\begin{aligned} \bullet \ : K \times V &\longrightarrow V \\ (\lambda, v) &\longrightarrow u = \lambda \cdot v \end{aligned}$$

Ejemplo 26. *Un caso particular del ejemplo anterior es el producto de escalares por funciones reales de variable real. Si A es el conjunto de las funciones reales de variable real, $f \in A$ es una función de A, $\mathbb{R}$ el conjunto de los números reales y $k \in \mathbb{R}$ un número real, la aplicación*

$$\begin{aligned} \bullet \ : \mathbb{R} \times A &\longrightarrow A \\ \big(k, f\big) &\longrightarrow (k \cdot f)\,(x) = kf(x), \ \forall\, x \in \mathbb{R} \end{aligned}$$

resulta ser una operación externa en A.

[3]Esta ley se llama, también, **operación externa** por la derecha.

Propiedades 8. *Las leyes de composición no han de satisfacer, en general, ningún requisito en especial. Sin embargo, sólo serán interesantes aquellas que, en cada caso, verifiquen ciertas propiedades. De ellas, se exponen aquí las más interesantes, comenzando por las que se refieren a leyes de composición interna:*

Asociativa $a_1 \oplus (a_2 \oplus a_3) = (a_1 \oplus a_2) \oplus a_3,\ \forall\, a_1, a_2, a_3 \in A$

Conmutativa $a_1 \oplus a_2 = a_2 \oplus a_1,\ \forall\, a_1, a_2 \in A$

Distributiva *Dado el conjunto A y las leyes $\oplus$ y $\odot$, se dice que $\odot$ es* ***distributiva por la izquierda*** *respecto a $\oplus$ si:*

$$a_1 \odot (a_2 \oplus a_3) = (a_1 \odot a_2) \oplus (a_1 \odot a_3)\,,\ \forall\, a_1, a_2, a_3 \in A$$

de la misma forma, se dice que $\odot$ es ***distributiva por la derecha*** *respecto a $\oplus$ si:*

$$(a_2 \oplus a_3) \odot a_1 = (a_2 \odot a_1) \oplus (a_3 \odot a_1)\,,\ \forall\, a_1, a_2, a_3 \in A$$

finalmente, $\odot$ es ***distributiva*** *respecto de $\oplus$, si lo es por la izquierda y por la derecha, esto es:*

$$\begin{aligned}(a_1 \oplus a_2) \odot (a_3 \oplus a_4) = &(a_1 \odot a_3) \oplus (a_1 \odot a_4) \oplus \\ &\oplus (a_2 \odot a_3) \oplus (a_2 \odot a_4)\,,\ \forall\, a_1, a_2, a_3, a_4 \in A\end{aligned}$$

Elemento neutro *Se dice que una ley de composición interna en A tiene* ***elemento neutro*** *si:*

$$\exists\, e \in A \ /\ e \oplus a = a \oplus e = a,\ \forall\, a \in A$$

El elemento neutro[4] *se denotará por e.*

Elemento simétrico *Dada una ley de composición interna en A con elemento neutro e, se llama* ***elemento simétrico****, si existe, del elemento $a \in A$, a un elemento $\bar{a}$ tal que*[5]*:*

$$a \oplus \bar{a} = a \oplus \bar{a} = e$$

[4]Para la operación suma ordinaria en $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, el elemento neutro es el "0" para la suma, y para el producto ordinario el "1".

[5]Para la suma ordinaria, el elemento simétrico de un elemento x es $-x$, y se llama **elemento opuesto**. Para el producto ordinario entre números reales o racionales no nulos, el elemento simétrico es $\frac{1}{x}$, y se denomina **elemento inverso o recíproco**. Por otra parte, para el producto ordinario de matrices, que se estudiará más adelante, el elemento simétrico se llama **matriz inversa** y se representan por $\mathbf{A}^{-1}$.

Elemento regular o simplificable *Se dice que el elemento $a \in A$ es **regular o simplificable** para la ley de composición interna "$\oplus$" si se verifica:*

$$Si \;\; a \oplus a_1 = a \oplus a_2 \;\Rightarrow\; a_1 = a_2, \;\forall\, a_1, a_2 \in A$$

y:

$$Si \;\; a_1 \oplus a = a_2 \oplus a \;\Rightarrow\; a_1 = a_2, \;\forall\, a_1, a_2 \in A$$

La estructura de espacio vectorial, entre otras, constituye la base sobre la que se apoya el Álgebra Lineal. Los espacios vectoriales son estructuras matemáticas que cumplen unas determinadas propiedades. Estas propiedades son poco restrictivas, de forma que numerosos problemas reales pueden modelizarse mediante espacios vectoriales.

Para abordar el estudio de los espacios vectoriales recordaremos previamente una serie de definiciones de conceptos que son la base sobre la que se apoya la definición de espacio vectorial.

Hemos utilizado como ejemplo de estructuras los conjuntos de números $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ que se estudiarán con detalle en el capítulo siguiente.

Definición 33. *Se llama **estructura algebraica** a un conjunto A y unas operaciones $\oplus, \otimes, \odot, \ldots$ –internas o externas– definidas en él, de forma que se verifican ciertas propiedades. Se denota por $(A, \oplus, \otimes, \odot, \ldots)$.*

Se exponen a continuación las estructuras más habituales, y las necesarias para llegar, finalmente, al espacio vectorial.

2.2. Grupos

Definición 34. *Se llama **grupo** a una estructura $(G, \otimes)$ que verifica las propiedades:*

1. $(x \otimes y) \otimes z = x \otimes (y \otimes z)\,, \;\forall\, x, y, z \in G$ *(Propiedad Asociativa)*
2. $\exists\, e \in G \;/\; x \otimes e = e \otimes x = x, \;\forall\, x \in G$ *(Existencia de Elemento Neutro)*
3. $\forall x \in G \;\; \exists\, y \in G \;/\; y \otimes x = x \otimes y = e$ *(Existencia de Elemento Simétrico)*

Definición 35. *Se llama **grupo conmutativo ó Abeliano** a un grupo $(G, \otimes)$ que verifica:*

4. $x \otimes y = y \otimes x, \;\forall\, x, y \in G$ *(Propiedad conmutativa)*

Ejemplo 1. *En el grupo $(\mathbb{R}, +)$ el elemento neutro es el "0" y el elemento simétrico es el elemento opuesto $(-x)$. De la misma forma, en el grupo $(\mathbb{R}_0 = \mathbb{R} - \{0\}, \cdot)$ el elemento neutro es el "1" y el elemento simétrico es el inverso*[6] *$(1/x)$. Ambos son grupos conmutativos. Además:*

[6] Quizás con más precisión, a éste elemento se le denomina también *recíproco*.

1. *Los conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ son grupos abelianos respecto a la suma ordinaria*

2. *Los conjuntos $\mathbb{Q}_0, \mathbb{R}_0$ y $\mathbb{C}_0$ son grupos abelianos respecto al producto (sin el "0")*

3. *El conjunto $\mathcal{M}_{m\times n}(\mathbb{R})$ de matrices con m filas y n columnas y coeficientes en $\mathbb{R}$ es un grupo conmutativo respecto a la suma matricial.*[7]

2.3. Anillos

Se analizarán a continuación los anillos, un tipo de estructuras con dos operaciones relacionadas entre sí. Estructuras algebraicas de este tipo son los conjuntos numéricos $\mathbb{Z}, \mathbb{Q}$ y $\mathbb{R}$, de forma que estas estructuras resultan relativamente familiares; esto, no obstante, puede resultar un inconveniente porque anima a generalizar las propiedades a las que se está acostumbrado al manejar números. Esto, como se verá, no es siempre acertado.

Definición 36. *Se llama **anillo**, y se denota por $(A, \oplus, \odot)$, a un conjunto A dotado de dos operaciones "$\oplus$" y "$\odot$" que verifica las propiedades siguientes:*

1. *$(A, \oplus)$ es un grupo abeliano. Su elemento neutro lo denotaremos como 0.*

2. $(x \odot y) \odot z = x \odot (y \odot z)\,,\ \forall\, x, y, z \in A$ *(propiedad asociativa)*

3. $\left.\begin{array}{c} x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z) \\ (x \oplus y) \odot z = (x \odot z) \oplus (y \odot z) \end{array}\right\}\ \forall x, y, z \in A$ *(prop. distributiva)*

Definición 37. *$(A, \oplus, \odot)$ se llamará **anillo unitario** si verifica:*

4. $\exists^{\bullet}\, \bar{e} \in A \ /\ x \odot \bar{e} = \bar{e} \odot x = x,\ \forall\, x \in A$

Definición 38. *$(A, \oplus, \odot)$ se llamará **anillo conmutativo** si verifica:*

5. $x \odot y = y \odot x,\ \forall\, x, y \in A$ *(propiedad conmutativa)*

Definición 39. *Un elemento x de un anillo unitario $(A, \oplus, \odot)$ se dice **inversible** si posee simétrico respecto de la segunda operación, "$\odot$", es decir existe $y \in A$ tal que*

$$x \odot y = y \odot x = \bar{e}$$

Ejemplo 27. *En el anillo $(\mathbb{Z}, +, \cdot)$ los únicos elementos inversibles son el 1 y el -1, de forma que $(-1)\cdot(-1) = 1 \cdot 1 = 1$ (el 1 es el elemento neutro para la operación "$\cdot$"). Esto choca directamente con lo que sucede en el anillo*

[7] Si $A = (a_{ij}), B = (B_{ij}) \in \mathcal{M}_{m\times n}(\mathbb{R})$ son dos matrices reales, la suma $A + B = (a_{ij} + b_{ij})$

$(\mathbb{R},+,\cdot)$, en el que el único elemento no inversible es el 0 (precisamente, el elemento neutro para la operación "+").

Con respecto a los conjuntos numéricos, se cumple que $(\mathbb{Z},+,\cdot)$ es un anillo conmutativo unitario. Los conjuntos $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ y $(\mathbb{C},+,\cdot)$ son anillos conmutativos unitarios, en los que todos los elementos, salvo el nulo, son inversibles.

Otro ejemplo muy utilizado de anillo es el conjunto $\mathbb{Z}_m$ con las operaciones:

$$[a]+[b]=[a+b] \quad [a][b]=[ab]$$

siendo $a,b\in\{0,1,\ldots,m-1\}$.

Por analogía con los conjuntos numéricos, es habitual denotar al elemento neutro, respecto de $\odot$, de un anillo unitario $(A,\oplus,\odot)$ como 1.

En determinados anillos es posible encontrar dos elementos no nulos que, al operarlos entre sí mediante la segunda operación –a la que habitualmente denominamos con el producto–, se obtiene el elemento neutro de la primera –el 0, habitualmente–. En otras palabras, es posible multiplicar dos elementos no nulos y que el resultado sea cero. A estos elementos se les conoce como *divisores de cero*:

Definición 40. *En un anillo $(A,\oplus,\odot)$ se dice que un elemento $a\in A$ no nulo es un **divisor de cero** si existe otro elemento no nulo $b\in A$ tal que $a\odot b=0$.*

Un ejemplo claro de este tipo de comportamiento se puede observar en el anillo $(\mathcal{M}_n(\mathbb{R}),+,\cdot)$, donde $\mathcal{M}_n(\mathbb{R})$ es el conjunto de las matrices cuadradas de tamaño n con coeficientes en $\mathbb{R}$ y "+","·" son las operaciones suma y producto habituales entre matrices.[8] Si tomamos las matrices no nulas $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$ y $\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$, su producto es:

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

Un caso especial de anillos son aquellos en los que no existen divisores de cero, es decir:

$$\forall\, x,y\in A \quad \big(x\odot y=0 \;\Leftrightarrow\; (x=0\;\vee\; y=0)\big)$$

a estos anillos se les denomina *anillos íntegros* o *dominios de integridad*.

Ejemplo 28. *Los anillos $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ y $(\mathbb{C},+,\cdot)$, con las operaciones $+$ y $\cdot$ habituales en ellos, son dominios de integridad.*

[8] Si $A=(a_{ij}), B=(b_{ij})\in\mathcal{M}_n(\mathbb{R})$, la matriz producto AB tiene como coeficiente ij el resultado de multiplicar la fila i-ésima de A por la columna j-ésima de B, es decir

$$(AB)_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj}=(a_{i1},\ldots,a_{in})\begin{pmatrix}b_{1j}\\ \vdots\\ b_{nj}\end{pmatrix}.$$

2.4. Cuerpos

Definición 41. *Se llama* ***cuerpo*** *a un anillo unitario* $(K, \oplus, \odot)$*, tal que* $(K - \{0\}, \odot)$ *es un grupo, es decir todo elemento* $x \in K$ *distinto de* 0 *es inversible respecto de* $\odot$*.*

Si el anillo $(K, \oplus, \odot)$ es conmutativo, se dice que el cuerpo K es conmutativo.

Ejemplo 2. *Los conjuntos* $\mathbb{Q}$*,* $\mathbb{R}$ *y* $\mathbb{C}$ *son cuerpos conmutativos respecto a las operaciones suma y producto ordinarias.*

El anillo $\mathbb{Z}_m$ *es un cuerpo si* m *es un número primo y son la base para la construcción de cualquier cuerpo finito cuyo cardinal es siempre de la forma* p^n*, siendo* p *un primo y* n *un número natural. Estos cuerpos se utilizan en Criptografía, Teoría de Códigos, etc.*

2.5. Espacios Vectoriales

Definición 42. *Se dice que un conjunto* V *tiene estructura de* ***espacio vectorial*** *sobre un cuerpo* K *si:*

- *En* V *hay definida una operación interna (suma) que confiere a* V *estructura de grupo abeliano*
- *En* V *hay definida una operación externa (producto)*

$$: K \times V \to V$$

que verifica las siguientes operaciones:

1. $\lambda\,(u + v) = \lambda u + \lambda v,\ \forall\, u, v \in V,\ \forall\, \lambda \in K$
2. $(\lambda + \mu)\, u = \lambda u + \mu u,\ \forall\, u \in V,\ \forall\, \lambda, \mu \in K$
3. $\lambda\,(\mu u) = (\lambda\mu)\, u,\ \forall\, u \in V,\ \forall\, \lambda, \mu \in K$
4. $1 \cdot u = u,\ \forall\, u \in V$

Los elementos del espacio vectorial reciben el nombre de *vectores*, y los elementos del cuerpo K *escalares*.

Ejemplo 29. *Son ejemplos de espacios vectoriales* $\mathbb{R}^n$*,* $\mathbb{C}^n$*,* $\mathbb{Z}_m^n$*, para cualquier natural* n*, (en general* K^n*, si* K *es un cuerpo) y* $\mathcal{M}_{m\times n}(\mathbb{R})$*.*

Sea V un K-espacio vectorial. Si $\emptyset \neq U \subseteq V$ es un subconjunto no vacío de V, se dice que U es un *subespacio vectorial de* V, si U es un espacio vectorial sobre K, considerando en U las mismas operaciones definidas en V.

Proposición 2. *Sea $\emptyset \neq U \subseteq V$ un subconjunto no vacío de V, son equivalentes:*

1. *U es un subespacio vectorial de V*
2. *Dados $\vec{u}, \vec{u'} \in U$ y $\alpha \in K$, se tiene que $\vec{u} + \vec{u'} \in U$ y $\alpha\vec{u} \in U$*
3. *Dados $\vec{u}, \vec{u'} \in U$ y $\alpha, \beta \in K$, se tiene que $\alpha\vec{u} + \beta\vec{u'} \in U$*

Sea V un K-espacio vectorial y sea $S = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_p\}$ un subconjunto cualquiera de vectores de V. Una *combinación lineal* de los vectores de S es un vector $\vec{v}$ que se escribe como

$$\vec{v} = \alpha_1\vec{v}_1 + \alpha_2\vec{v}_2 + \cdots \alpha_p\vec{v}_p = \sum_{i=1}^{p} \alpha_i\vec{v}_i.$$

donde $\alpha_i \in K$.

Ejemplos 2. *1. $\vec{0}$ es combinación lineal de cualquier conjunto de vectores sin más que tomar $\alpha_i = 0$ para todo i.*

2. En $\mathbb{R}^3$, se tiene que

$$(1, 1, 0) = (-1)(2, 1, -1) + 1(3, 2, -1)$$

Proposición 3. *El conjunto $\{$combinaciones lineales de $S\}$ es un subespacio vectorial de V llamado* subespacio generado o engendrado *por S y se denota $< S >$*

Definición 43. *Sea $S = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_p\}$ un conjunto de vectores de V. Se dice que S es un conjunto* libre *o* un conjunto de vectores linealmente independientes *si, para toda combinación lineal de los vectores de S:*

$$\sum_{i=1}^{p} \alpha_i\vec{v}_i = \alpha_1\vec{v}_1 + \cdots + \alpha_p\vec{v}_p = \vec{0},$$

se tiene que $\alpha_i = 0$, para todo i. Equivalentemente, S es libre si, ningún vector de S es combinación lineal de los demás.

Análogamente, se define:

Definición 44. *Sea $S = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_p\}$ un conjunto de vectores de V. Se dice que S es un conjunto* ligado *o* un conjunto de vectores linealmente dependientes *si, existe una combinación lineal de los vectores de S:*

$$\sum_{i=1}^{p} \alpha_i\vec{v}_i = \alpha_1\vec{v}_1 + \cdots + \alpha_p\vec{v}_p = \vec{0},$$

donde algún $\alpha_i \neq 0$. Equivalentemente, S es ligado si, algún vector de S es combinación lineal de los demás.

Ejemplo 30. *En $\mathbb{R}^3$, los vectores $\{(1,1,0),(2,1,-1),(3,2,-1)\}$ forman un conjunto ligado.*

Sea V un K-espacio vectorial.

Definición 45. *Se dice que V es un espacio vectorial* de tipo finito *(o finitamente generado) si existe $S \subseteq V$ finito tal que $V =< S >$. S es un* sistema de generadores de V.

Definición 46. *Un conjunto de vectores $B = \{\vec{v}_1, \ldots, \vec{v}_p\}$ de V es una* base *de V si:*

- *B es un sistema de generadores de V ($V =< B >$)*
- *B es un conjunto libre.*

Ejemplo 31. *En K^n, el conjunto*

$$\{(1,0,\ldots,0),(0,1,\ldots,0),\ldots,(0,0,\ldots,1)\}$$

es una base (llamada base canónica)

Teorema 1. *Sea $B = \{\vec{v}_1, \ldots, \vec{v}_p\} \subseteq V$. Son equivalentes:*

1. *B es una base de V.*
2. *Cualquier vector de V se escribe de* manera única *como combinación lineal de los vectores de la base de B.*

Si $\vec{v} = \alpha_1\vec{v}_1 + \alpha_2\vec{v}_2 + \cdots + \alpha_p\vec{v}_p$, los escalares $\alpha_1, \alpha_2, \ldots, \alpha_p$ se llaman *coordenadas del vector $\vec{v}$* respecto de la base B.

Proposición 4. *Sea $V \neq \{\vec{0}\}$ un espacio vectorial de tipo finito. V siempre admite una base.*

Proposición 5. *Sean B y B' dos bases de V. Entonces $|B| = |B'|$ y a este cardinal común se le llama* dimensión *de V.*

Sea S un conjunto de vectores de un espacio vectorial V de tipo finito. Se denomina *rango* de S a $dim(< S >)$, luego el rango de S es el mayor número de vectores linealmente independientes que hay dentro de S.