1. Estructuras algebráicas, campos y espacios vectoriales

El álgebra lineal se puede definir como el estudio de los espacios vectoriales. En esta sección definiremos qué son, así como algunas nociones básicas que guiarán nuestro estudio de este tipo de estructuras algebráicas durante el curso. Antes, discutiremos brevemente qué constituye una estructura algebráica y repasaremos la definición de la estructura de campo —necesaria para definir la de espacio vectorial.

1.1. Estructuras algebráicas

¿Qué es el álgebra, y qué es lo que estudia? A menudo en los primeros cursos de álgebra esta cuestión no queda clara. El hecho de que esta área de las matemáticas tenga una historia de evolución que comenzó hace miles de años y continúa hasta hoy en día complica aún más la situación. A pesar de no ser la visión más general que existe, en este curso tomaremos por respuesta que el álgebra es el estudio de estructuras algebráicas.

1.1.1. Definición de estructura algebráica y propiedades de sus operaciones

Def. Una *estructura algebráica* es un conjunto no vacío A con (al menos) una operación en A y una colección (posiblemente vacía) de relaciones en A. Denotamos a una estructura algebráica formada por un conjunto A, operaciones $\star, *$ y una relación $\sim$, como $(A, \star, *, \sim)$. Decimos que:

- $\star$ es *binaria* si toma **pares ordenados** de elementos de A y devuelve elementos de A, i.e., si su dominio es $A \times A$ y su contradominio es A, lo que denotamos como $\star : A \times A \to A$;
- $\star$ es *asociativa* si, para cualesquiera $a, b, c \in A$, se tiene que
$$(a \star b) \star c = a \star (b \star c);$$
- $\star$ es *conmutativa* si, para cualesquiera $a, b \in A$, se tiene que
$$a \star b = b \star a;$$
- $\star$ tiene un elemento *identidad* (o *neutro*) si existe $e \in A$ tal que, para todo $a \in A$,
$$e \star a = a = a \star e;$$
- $b \in A$ es el elemento *inverso* de $a \in A$ (*bajo* $\star$) si $\star$ tiene un elemento identidad $e \in A$ y
$$a \star b = e = b \star a;$$
- $B \subseteq A$ es *cerrado bajo la operación* $\star$ si, para cualesquiera $x, y \in B$,
$$x \star y \in B;$$
- $\star$ se *distribuye con respecto a* $*$ si ambas operaciones son operaciones binarias y, para cualesquiera $a, b, c \in A$,
$$a \star (b * c) = (a \star b) * (a \star c) \quad \& \quad (b * c) \star a = (b \star a) * (c \star a).$$

Observemos que, por definición, la relación de "ser inverso bajo una operación" es simétrica. Es decir, a es inverso de b bajo la operación $\star$ si, y sólo si, b es inverso de a bajo $\star$. Más aún, por definición, el elemento identidad de una operación, si existe, siempre es su propio inverso bajo esa operación. Frecuentemente diremos simplemente *identidad* o *neutro* para referirnos al elemento identidad de una operación. Así mismo, utilizaremos sólo la palabra *estructura* para referirnos a una estructura algebráica.

1.1.2. Ejemplos de estructuras algebráicas

Para cualquier conjunto arbitrario A, su conjunto potencia $\mathscr{P}(A)$ junto con las operaciones de unión e intersección de conjuntos ($\cup$ y $\cap$, respectivamente) y la relación "contención" ($\subseteq$) forma una estructura algebráica, que podemos escribir explícitamente como $(\mathscr{P}(A), \cup, \cap, \subseteq)$. Observemos que ambas operaciones son binarias, asociativas y conmutativas, como seguramente viste en tu curso de Álgebra.

Exercise ejercicio-1 Consideremos la estructura algebráica $(\mathscr{P}(A), \cup, \cap, \subseteq)$, donde A es un conjunto arbitrario. ¿Quienes son los elementos neutros de $\cup$ y $\cap$? Demuéstralo.

El conjunto de los números naturales ($\mathbb{N}$) junto con la operación de suma ($+$) y la relación "menor o igual que" ($\leq$) forma una estructura algebráica $(\mathbb{N}, +, \leq)$. Observemos que, en este caso, $+$ es una operación binaria, asociativa y conmutativa. Si incluimos al número 0 en el conjunto $\mathbb{N}$, entonces 0 es el elemento identidad de la suma, y es el único elemento de $\mathbb{N}$ que tiene inverso (¿Por qué?).

Exercise ejercicio-2 Consideremos la estructura algebráica $(\mathbb{N}, +, \leq)$. Demuestra que ningún subconjunto finito F de $\mathbb{N}$ es cerrado bajo la suma.

El conjunto de los números enteros junto con las operaciones de suma y multiplicación forma una estructura algebráica $(\mathbb{Z}, +, \cdot)$. Similarmente, los conjuntos de los números racionales y los reales con las mismas operaciones —entre números racionales y reales, respectivamente— forman las estructuras $(\mathbb{Q}, +, \cdot)$ y $(\mathbb{R}, +, \cdot)$. Claramente, estas tres estructuras son distintas, pues los conjuntos que los forman son distintos. Sin embargo, $(\mathbb{Q}, +, \cdot)$ y $(\mathbb{R}, +, \cdot)$ forman el mismo *tipo* de estructura algebráica puesto que, como veremos más adelante, sus operaciones cumplen las mismas propiedades. Estudiaremos este tipo de estructura, conocida como *campo*, en la sección 1.2 como un primer paso hacia la definición de otro tipo de estructura conocida como *espacio vectorial*, que definiremos en 1.3. Además, veremos que no se necesitan relaciones para definir a estos tipos de estructuras. Por lo tanto, de ahora en adelante asumiremos que nuestras estructuras algebráicas no tienen relaciones.

Antes de definir estos tipos de estructuras algebráicas, veremos algunas nociones generales de estructuras que usaremos tanto en campos como en espacios vectoriales.

1.1.3. Unicidad de identidades e inversos

Sean $(A, \star)$ una estructura algebráica y $e \in A$ un elemento identidad de la operación $\star$. Entonces

(a) e es único;

(b) si la operación $\star$ es asociativa y $a \in A$ tiene un inverso b bajo $\star$, entonces b es único.

Demostración.

(a) Supongamos que $e' \in A$ es un elemento identidad de $\star$. Entonces $e = e \star e' = e'$. Por lo tanto, el elemento identidad e de $\star$ es único.

(b) Supongamos que $\star$ es asociativa, $a \in A$ y que existe $b \in A$ tal que b es inverso de a bajo $\star$. Adicionalmente, supongamos que $b' \in A$ es un inverso de a bajo $\star$. Entonces

$$\begin{aligned} b &= b \star e && (e \text{ es neutro}) \\ &= b \star (a \star b') && (b' \text{ es inverso de } a) \\ &= (b \star a) \star b' && (\star \text{ es asociativa}) \\ &= e \star b' && (b \text{ es inverso de } a) \\ &= b'. \end{aligned}$$

Por lo tanto, los elementos inversos bajo $\star$, si existen, son únicos.

□

1.1.4. Funciones que preservan estructura

Las estructuras no sólo se pueden estudiar a través de las interacciones de sus operaciones con *elementos*, sino también a través de sus interacciones con *funciones*. Sin embargo, trabajar con funciones *arbitarias* para estudiar estructuras puede ser de poca utilidad. Un tipo de funciones muy útiles para estudiar la relación entre dos estructuras algebráicas son aquellas que **presevan su estructura**.

Def. Sean $(A, \star)$ y $(B, \diamondsuit)$ estructuras algebráicas. Decimos que una función $f : A \to B$ es *compatible con las operaciones $\star$ y $\diamondsuit$* si, para todo $x, y \in A$, se cumple que

$$f(x \star y) = f(x) \diamondsuit f(y).$$

En este caso, también decimos que la función f *preserva la estructura* de $(A, \star)$ y $(B, \diamondsuit)$.

En caso de que tengamos estructuras algebráicas con dos operaciones $(A, \star, *)$ y $(B, \diamondsuit, \spadesuit)$, diremos que una función $f : A \to B$ *preserva su estructura* si es compatible con los pares de operaciones $(\star, \diamondsuit)$ y $(*, \spadesuit)$, i.e., si, para todo $x, y \in A$, se cumple que

$$\begin{gathered} f(x \star y) = f(x) \diamondsuit f(y) \\ \& \\ f(x * y) = f(x) \spadesuit f(y). \end{gathered}$$

1.2. Campos

Un campo es un tipo de estructura algebráica que formaliza varias de las nociones intuitivas que adquirimos durante nuestra educación básica sobre la aritmética en los números reales; esto es, que la suma y la multiplicación son operaciones binarias, asociativas y conmutativas, que la multiplicación se distribuye con respecto a la suma, y que el 0 y el 1 son números "especiales" en cierto sentido, el cual precisaremos más adelante.

Quizá viste este tipo de estructura explícitamente en tu curso de Álgebra y/o implícitamente en tu curso de Cálculo I (a través de los *axiomas de campo* —o *de cuerpo*[1]— *para los números reales*); sin embargo, a continuación mencionaremos su definición y estudiaremos los dos ejemplos de campos que más utilizaremos durante este curso (el campo real y el complejo) antes de definir los espacios vectoriales.

[1] En francés, este tipo de estructura es llamado *corps*, cuya traducción directa al español es "cuerpo".

1.2.1. Definición de campo

Def. Un *campo* es un conjunto, que suele denotarse por K[a], con dos operaciones binarias llamadas *suma* y *multiplicación*, denotadas por $+$ y $\cdot$, respectivamente, tales que cumplen las siguientes propiedades[b]:

$\forall\ a, b, c \in K$	$a + (b + c) = (a + b) + c \ \ \& \ \ a \cdot (b \cdot c) = (a \cdot b) \cdot c$	Asociatividad
$\forall\ a, b \in K$	$a + b = b + a \ \ \& \ \ a \cdot b = b \cdot a$	Conmutatividad
$\exists\ 0, 1 \in K$ t.q., $\forall\ a \in K$,	$a + 0 = a \quad \& \quad 1 \cdot a = a$	Identidades (neutros)[c]
$\forall\ a \in K$	$\exists\ -a \in K$ t.q. $a + (-a) = 0$	Inversos aditivos[d]
$\forall\ a \neq 0 \in K$	$\exists\ a^{-1} \in K$ t.q. $a \cdot a^{-1} = 1$	Inversos multiplicativos[e]
$\forall\ a, b, c \in K$	$a \cdot (b + c) = a \cdot b + a \cdot c$	Distributividad[f].

[a] En inglés, la palabra "campo" se traduce como *field*, por lo que el conjunto suele denotarse por F en vez de K.

[b] A estas propiedades también se les conoce como *axiomas de campo*.

[c] Por el lema **??**, sabemos que los elementos identidad de operaciones en estructuras algebráicas son únicos. Por convención, se suele denotar al neutro aditivo de un campo como 0 y al neutro multiplicativo, como 1. Además, como en este caso las operaciones son conmutativas, podemos escribir esta propiedad de manera más sucinta.

[d] Por el mismo lema, sabemos que los inversos, si existen, son únicos. Por convención, si a es elemento de un campo, su inverso aditivo suele denotarse por $-a$.

[e] Por convención, si a es un elemento de un campo distinto del neutro aditivo, su inverso multiplicativo suele denotarse por a^{-1} o $\frac{1}{a}$.

[f] Observemos que podemos escribir esta propiedad de forma resumida, pues $+$ y $\cdot$ son binarias y conmutativas.

En otras palabras, una estructura algebráica $(K, +, \cdot)$ es un campo si:

- $+$ es una operación binaria, asociativa, conmutativa, con elemento identidad e inversos aditivos para **todos sus elementos**;
- $\cdot$ es una operación binaria, asociativa, conmutativa, con elemento identidad e inversos multiplicativos para **todos sus elementos excepto el neutro aditivo**;
- $\cdot$ se distribuye con respecto a $+$.

Nótese la asimetría en la propiedad de existencia de inversos aditivos en ambas operaciones: el neutro aditivo **no** requiere tener inverso *multiplicativo*, mientras que **todos** los elementos deben tener inversos **aditivos**. Frecuentemente escribiremos sólamente K para referirnos al campo $(K, +, \cdot)$ y escribiremos la multiplicación implícitamente, omitiendo el símbolo "$\cdot$".

1.2.2. Ejemplos de campos

El campo real

El conjunto de los números reales $\mathbb{R}$ junto con las operaciones de suma y multiplicación (que aprendimos desde la educación básica) cumplen todas las propiedades enlistadas en la sección 1.2.1, por lo que forman un campo $(\mathbb{R}, +, \cdot)$, conocido como el *campo real*. Este campo puede ser representado geométricamente con la recta real, como en la Figura 1.