Álgebra Lineal - Clase 1

Gabriela Jeronimo

FCEN-UBA

Segundo cuatrimestre 2020

Esquema de la clase

- Espacios vectoriales.
- Subespacios.
- Generadores.

Bibliografía recomendada.
G. Jeronimo, J. Sabia, S. Tesauri. *Algebra Lineal*. Cursos de Grado. Fascículo 2. Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, 2008.

Capítulo 1 (Sección 1.1).

Operaciones en un conjunto

Definición.

Sea A un conjunto no vacío. Una operación (o ley de composición interna) en A es una función $* : A \times A \to A$.

Notación: $*(a, b) = c$ se escribe $a * b = c$.

Ejemplos.

- $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $+(a, b) = a + b$, es una operación en $\mathbb{N}$.
- $-(a, b) = a - b$, no es una operación en $\mathbb{N}$.
- $+$, $\cdot$ y $-$ son operaciones en $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$.

Sea $* : A \times A \to A$ una operación.

i) $*$ es asociativa si $(a * b) * c = a * (b * c) \ \ \forall\, a, b, c \in A$.

ii) $*$ tiene elemento neutro si $\exists\, e \in A$ tal que $e * a = a * e = a$ para cada $a \in A$.

iii) Si $*$ tiene elemento neutro e, todo elemento tiene inverso para $*$ si $\forall\, a \in A$, $\exists\, a' \in A$ tal que $a * a' = a' * a = e$.

iv) $*$ es conmutativa si $a * b = b * a \ \ \forall\, a, b \in A$.

Observar que si $*$ tiene elemento neutro, éste es único, ya que si e y e' son elementos neutros, $e' = e * e' = e$.

Definición.

Si A es un conjunto y $*$ es una operación en A que satisface las propiedades i), ii) y iii), $(A, *)$ se llama un grupo.
Si además $*$ cumple iv), se dice que $(A, *)$ es un grupo abeliano o conmutativo.

Ejemplos.

- $(\mathbb{N}, +)$ no es un grupo: no tiene elemento neutro.
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ y $(\mathbb{C}, +)$ son grupos abelianos.
- $(\mathbb{Z}, \cdot)$ no es un grupo: sólo 1 y -1 tienen inverso multiplicativo.
- $(\mathbb{Q} - \{0\}, \cdot)$, $(\mathbb{R} - \{0\}, \cdot)$ y $(\mathbb{C} - \{0\}, \cdot)$ son grupos abelianos.
- $S_{\mathbb{R}} = \{f : \mathbb{R} \to \mathbb{R} \,/\, f \text{ es biyectiva}\}$, $* = \circ$.
  $(S_{\mathbb{R}}, \circ)$ es un grupo.
- C un conjunto, $\mathcal{P}(C) = \{S \subseteq C\}$ y
  $\triangle : \mathcal{P}(C) \times \mathcal{P}(C) \to \mathcal{P}(C)$, $A \triangle B = (A \cup B) - (A \cap B)$.
  $(\mathcal{P}(C), \triangle)$ es un grupo abeliano.

Observación.

Si $(G, *)$ es un grupo, $\forall a \in G$ existe un único inverso para a.

En efecto, si b y c son inversos de a y e es el elemento neutro de $(G, *)$, entonces $b = e * b = (c * a) * b = c * (a * b) = c * e = c$.

Anillos y cuerpos

Definición

Sea A un conjunto y sean $+$ y $\cdot$ operaciones en A. Se dice que $(A, +, \cdot)$ es un anillo si

i) $(A, +)$ es un grupo abeliano.

ii) $\cdot$ es asociativa y tiene elemento neutro.

iii) Valen las propiedades distributivas: $\forall a, b, c \in A$,
   - $a \cdot (b + c) = a \cdot b + a \cdot c$
   - $(b + c) \cdot a = b \cdot a + c \cdot a$

Si $\cdot$ es conmutativa, se dice que $(A, +, \cdot\,)$ es un anillo conmutativo.

Notaremos 0 y 1 a los elementos neutros de $+$ y $\cdot$ respectivamente.

Ejemplos.

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ son anillos conmutativos.
- $(\mathbb{Z}/n\mathbb{Z}), +, \cdot)$, $n \in \mathbb{N}$, son anillos conmutativos.

- Si $(A, +, \cdot)$ es un anillo conmutativo, entonces $(A[X], +, \cdot)$ con las operaciones usuales es un anillo conmutativo.
- $\{f : \mathbb{R} \to \mathbb{R}\}$ con las operaciones usuales de suma y producto de funciones es un anillo conmutativo.
- Si C es un conjunto, $(\mathcal{P}(C), \triangle, \cap)$ es un anillo conmutativo.
- $(\mathbb{R}^{n\times n}, +, \cdot)$ es un anillo (no es conmutativo).

Un anillo conmutativo $(A, +, \cdot)$ se llama un dominio de integridad o dominio íntegro si para $a, b \in A$, $a \cdot b = 0 \;\Rightarrow\; a = 0 \text{ o } b = 0$.

Ejemplos.

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ y $(\mathbb{C}, +, \cdot)$ son dominios íntegros.
- A dominio íntegro $\Rightarrow$ $A[X]$ dominio íntegro.
- $\mathbb{Z}/6\mathbb{Z}$ no es un dominio íntegro: $2 \cdot 3 = 0$ en $\mathbb{Z}/6\mathbb{Z}$, pero $2 \neq 0$ y $3 \neq 0$.
- $\mathbb{Z}/m\mathbb{Z}$ es un dominio íntegro $\iff$ m es primo.

Definición.

Sea K un conjunto, y sean $+$ y $\cdot$ operaciones en K. Se dice que $(K, +, \cdot)$ es un cuerpo si $(K, +, \cdot)$ es un anillo conmutativo y todo elemento no nulo de K tiene inverso multiplicativo. Es decir:

i) $(K, +)$ es un grupo abeliano,

ii) $(K - \{0\}, \cdot)$ es un grupo abeliano, y

iii) vale la propiedad distributiva de $\cdot$ con respecto a $+$.

Ejemplos.

- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ y $(\mathbb{C}, +, \cdot)$ son cuerpos.
- $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ es un cuerpo $\iff$ p es primo.

Observación.

Todo cuerpo $(K, +, \cdot)$ es un dominio de integridad.

Supongamos que $a \cdot b = 0$. Si $a = 0$ $\checkmark$.

Si $a \neq 0$, $\exists a^{-1}$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Entonces:

$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 \Rightarrow (a^{-1} \cdot a) \cdot b = 0 \Rightarrow 1 \cdot b = 0 \Rightarrow b = 0.$

Otro ejemplo.

Sea $\mathbb{Q}[\sqrt{2}] = \left\{ \sum_{i=0}^{n} a_i(\sqrt{2})^i \,/\, a_i \in \mathbb{Q},\ n \in \mathbb{N}_0 \right\} \subset \mathbb{R}$.

$(\mathbb{Q}[\sqrt{2}], +, \cdot)$ es un cuerpo.

$\forall k \in \mathbb{N}$, $(\sqrt{2})^{2k} = 2^k$ y $(\sqrt{2})^{2k+1} = 2^k\sqrt{2}$
$\Rightarrow \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \,/\, a, b \in \mathbb{Q}\}$.

- $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$, 0 y $1 \in \mathbb{Q}[\sqrt{2}] \rightsquigarrow (\mathbb{Q}[\sqrt{2}], +, \cdot)$ anillo conmutativo.
- Todo elemento no nulo tiene inverso multiplicativo:
  $a + b\sqrt{2} \neq 0 \Rightarrow (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \neq 0$
  (porque $a, b \in \mathbb{Q}$ y $\sqrt{2} \notin \mathbb{Q}$)
  $\Rightarrow (a + b\sqrt{2})^{-1} = \dfrac{a}{a^2 - 2b^2} + \dfrac{-b}{a^2 - 2b^2}\sqrt{2}$.

Similarmente, para $d \in \mathbb{N}$ libre de cuadrados, $(\mathbb{Q}[\sqrt{d}], +, \cdot)$ es un cuerpo.

Espacios vectoriales

Sean A y B dos conjuntos. Una acción de A en B es una función $\cdot : A \times B \to B$. Notación: $\cdot(a, b) = a \cdot b$.

Definición.

Sea K un cuerpo. Sean V un conjunto no vacío, $+$ una operación en V y $\cdot$ una acción de K en V. Se dice que $(V, +, \cdot)$ es un K-espacio vectorial si se cumplen las siguientes condiciones:

1. $(V, +)$ es un grupo abeliano.
2. La acción $\cdot : K \times V \to V$ satisface:
   (a) $a \cdot (v + w) = a \cdot v + a \cdot w \quad \forall\, a \in K;\ \forall\, v, w \in V$.
   (b) $(a + b) \cdot v = a \cdot v + b \cdot v \quad \forall\, a, b \in K;\ \forall\, v \in V$.
   (c) $1 \cdot v = v \quad \forall\, v \in V$.
   (d) $(a \cdot b) \cdot v = a \cdot (b \cdot v) \quad \forall\, a, b \in K;\ \forall\, v \in V$.

Los elementos de V se llaman vectores y los elementos de K se llaman escalares.

La acción $\cdot : K \times V \to V$ se llama producto por escalares.

En lo que sigue K es un cuerpo.

Ejemplos.

- K es un K-espacio vectorial.
- $K^n = \{(x_1, \dots, x_n) \,/\, x_i \in K \ \forall 1 \leq i \leq n\}$.

  $$\begin{aligned} + \ &: \ K^n \times K^n \to K^n, \\ &\quad (x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n) \\ \cdot \ &: \ K \times K^n \to K^n, \quad \lambda \cdot (x_1, \dots, x_n) = (\lambda x_1, \dots, \lambda x_n) \end{aligned}$$

  $(K^n, +, \cdot)$ es un K-espacio vectorial.
- $K^{n \times m} = \{$matrices de n filas y m columnas de elementos en $K\}$.

  $$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1m} \\ A_{21} & A_{22} & \cdots & A_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ A_{n1} & A_{n2} & \cdots & A_{nm} \end{pmatrix}, \qquad \begin{array}{l} A_{ij} \in K \\ \forall 1 \leq i \leq n, 1 \leq j \leq m. \end{array}$$

  $$+ \ : \ K^{n \times m} \times K^{n \times m} \to K^{n \times m}, \ (A + B)_{ij} = A_{ij} + B_{ij}$$

  $$\cdot \ : \ K \times K^{n \times m} \to K^{n \times m}, \ (\lambda \cdot A)_{ij} = \lambda \cdot A_{ij}$$

  $(K^{n \times m}, +, \cdot)$ es un K-espacio vectorial.

- $\mathbb{R}$ es un $\mathbb{Q}$-espacio vectorial; $\mathbb{C}$ es un $\mathbb{R}$-espacio vectorial y un $\mathbb{Q}$-espacio vectorial.
- $\mathbb{C}^n$ es un $\mathbb{R}$-espacio vectorial.
- $\mathbb{Q}[\sqrt{2}]$ es un $\mathbb{Q}$-espacio vectorial.
- $K^Z = \{f : Z \to K \ / \ f$ es función$\}$, para Z conjunto no vacío.

  $$+ : K^Z \times K^Z \to K^Z, \ (f+g)(x) = f(x) + g(x) \quad \forall x \in Z,$$
  $$\cdot : K \times K^Z \to K^Z, \ (\lambda \cdot f)(x) = \lambda \cdot f(x) \quad \forall x \in Z.$$

  $(K^Z, +, \cdot)$ es un K-espacio vectorial.
- $K[X]$ con la suma usual y la multiplicación usual de polinomios por una constante es un K-espacio vectorial.

Propiedades.

Sea V un K-espacio vectorial. Entonces:

1. $0 \cdot v = \mathbb{O} \;\; \forall v \in V$.
   ($\mathbb{O}$ denota el vector nulo, elemento neutro de $+$ en V)
2. $(-1) \cdot v = -v$ para todo $v \in V$.
   ($-v$ denota al inverso aditivo de v)

Demostración.

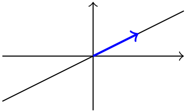
1. $0 \cdot v = (0 + 0) \cdot v = 0 \cdot v + 0 \cdot v$.
   Si w es el inverso aditivo de $0 \cdot v$,
   $\mathbb{O} = 0 \cdot v + w = (0 \cdot v + 0 \cdot v) + w = 0 \cdot v + (0 \cdot v + w) =$
   $0 \cdot v + \mathbb{O} = 0 \cdot v$.
2. $(-1) \cdot v + v = (-1) \cdot v + 1 \cdot v = (-1 + 1) \cdot v = 0 \cdot v = \mathbb{O}$.
   $\Rightarrow (-1) \cdot v = -v$.

Subespacios

Definición.
Sea V un K-espacio vectorial. Un subconjunto $S \subseteq V$ no vacío se dice un subespacio de V si la suma y el producto por escalares (de V) son una operación en S y una acción de K en S que lo convierten en un K-espacio vectorial.

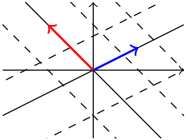
Ejemplo. Subespacios de $\mathbb{R}^2$:

- $S = \{(0,0)\}$ es un subespacio.
- Si $S \neq \{(0,0)\}$, $\exists v \in S$ no nulo $\Rightarrow \forall \lambda \in \mathbb{R}$, $\lambda . v \in S$.



$S = \{\lambda v, \lambda \in \mathbb{R}\}$ es subespacio.

- Si $\exists v, w \in S$ no nulos, $w \neq \lambda v$:



$L = \{\lambda \cdot v, \lambda \in \mathbb{R}\} \subset S$
$L' = \{\mu \cdot w, \mu \in \mathbb{R}\} \subset S$
$\Rightarrow \lambda \cdot v + \mu \cdot w \in S \ \forall \lambda, \mu \in \mathbb{R}$
$S = \mathbb{R}^2$.

Proposición.

Sea V un K-espacio vectorial y sea $S \subseteq V$. Entonces S es un subespacio de V si y sólo si valen las siguientes condiciones:

i) $0 \in S$

ii) $v, w \in S \Rightarrow v + w \in S$

iii) $\lambda \in K, v \in S \Rightarrow \lambda \cdot v \in S$

Ejemplos. Sea V un K-espacio vectorial.

- $\{0\}$ es un subespacio de V.
- V es un subespacio de V.
- Si $v \in V$, $S = \{\lambda \cdot v \,/\, \lambda \in K\}$ es un subespacio de V:
  i) $0 = 0 \cdot v \in S$.
  ii) Si $\lambda \cdot v$, $\mu \cdot v \in S$, entonces $\lambda \cdot v + \mu \cdot v = (\lambda + \mu) \cdot v \in S$.
  iii) Si $\lambda \cdot v \in S$ y $\alpha \in K$, entonces $\alpha \cdot (\lambda \cdot v) = (\alpha \cdot \lambda) \cdot v \in S$.

  S se llama el subespacio generado por v y se nota $S = < v >$.

- Dados $v_1, \ldots, v_n \in V$,
  $S = \{\alpha_1.v_1 + \cdots + \alpha_n.v_n \mid \alpha_i \in K,\ 1 \leq i \leq n\}$ es un subespacio de V:
  - i) $0 = 0.v_1 + \cdots + 0.v_n \in S$.
  - ii) $v, w \in S$, $v = \alpha_1.v_1 + \cdots + \alpha_n.v_n$, $w = \beta_1.v_1 + \cdots + \beta_n.v_n$,
    $\Rightarrow v + w = (\alpha_1 + \beta_1).v_1 + \cdots + (\alpha_n + \beta_n).v_n \in S$.
  - iii) $\lambda \in K$ y $v = \alpha_1.v_1 + \cdots + \alpha_n.v_n \in S$
    $\Rightarrow \lambda.v = (\lambda.\alpha_1).v_1 + \cdots + (\lambda.\alpha_n).v_n \in S$.

  S se llama el subespacio generado por $v_1, \ldots, v_n$ y se nota $S = < v_1, \ldots, v_n >$.

- Sean $a_1, \ldots, a_n \in K$ fijos.
  $S = \{(x_1, \ldots, x_n) \in K^n \mid a_1x_1 + \cdots + a_nx_n = 0\}$ es un subespacio de K^n:
  - i) $0 \in S$ ✓
  - ii) $\mathrm{x} = (x_1, \ldots, x_n) \in S$ y $\mathrm{x}' = (x_1', \ldots, x_n') \in S$
    $\Rightarrow \mathrm{x} + \mathrm{x}' = (x_1 + x_1', \ldots, x_n + x_n') \in S$ ya que
    $a_1(x_1 + x_1') + \cdots + a_n(x_n + x_n') = (a_1x_1 + a_1x_1') + \cdots + (a_nx_n + a_nx_n') = (a_1x_1 + \cdots + a_nx_n) + (a_1x_1' + \cdots + a_nx_n') = 0 + 0 = 0$.
  - iii) Ejercicio.