Algebra lineal III

15 Abril 2026

Empezamos con el estudio de espacios vectoriales y módulos, pues el álgebra lineal no es otra cosa que el estudio de módulos (esp. vectoriales) y matrices.

Repasemos algunas definiciones algebraicas.

Decimos que $(R, +, \cdot, 0, 1)$ es un anillo con unidad si el conjunto R admite dos operaciones binarias, la suma $+$ y la multiplicación $\cdot$ que satisfacen lo siguiente

i) La estructura $(R, +, 0)$ es un grupo abeliano

- La operación binaria $+$ (adición) es asociativa

  – $\forall x, y, z \ ((x+y)+z = x+(y+z))$

- El elemento 0 es la identidad aditiva

  – $\forall x \ (x+0 = 0+x = x)$

- Todo elemento en R tiene inverso aditivo

- $\forall x \exists y (x+y=y+x=0)$
donde y se denota $-x$
- La operación $+$ es conmutativa
$\forall x,y (x+y=y+x)$

Los tres primeros axiomas determinan un grupo, y cuando el grupo es conmutativo se le llama abeliano

---

ii) La estructura $(R, \cdot, 1)$ es un monoide cuando ocurre lo siguiente.
- La operación binaria $\cdot$ (multiplicación) es asociativa
$\forall x,y,z (x\cdot(y\cdot z)=(x\cdot y)\cdot z)$
- El elemento 1 es la identidad multiplicativa
$\forall x (x\cdot 1=1\cdot x=x)$

iii) La multiplicación $\cdot$ es distributiva respecto a $+$
- $\forall a,b,c ((a+b)\cdot c=a\cdot c+b\cdot c)$
- $\forall a,b,c (a\cdot(b+c)=a\cdot b+a\cdot c)$

Por lo general, el producto $a\cdot b$ se escribe simplemente como ab

La identidad multiplicativa 1 se llama unidad de R. Si bien los anillos que tratamos nosotros siempre tienen 1, en la literatura no siempre se piensa que los anillos necesariamente 1

Nota que no se pide que la multiplicación sea una operación conmutativa

Cuando $\cdot$ es conmutativa, el anillo se llama

anillo conmutativo

Igualmente, nosotros sólo consideraremos anillos conmutativos, pero debe quedar claro que la teoría con anillos no conmutativos es extraordinariamente importante.

Nota: Nuestros anillos son anillos con unidad y conmutativos. Siempre que escribamos "anillo" pensaremos que tiene tales propiedades, a menos que se indique lo contrario

Si un anillo F tiene la propiedad de que

$$\forall x (x \neq 0 \to \exists y (xy = 1))$$

es decir, cualquier elemento de F distinto de cero tiene inverso multiplicativo, diremos que F es un campo.

Así, en un campo se puede sumar, multiplicar, restar y dividir. (por elementos distintos de cero).

Ejemplos

- Anillos: $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$
- campos: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_7$

Ahora nos interesa introducir los módulos

<u>Def</u> Sea R un anillo. Decimos que M, formalmente $(M, +, \cdot)$, es un R-módulo si M es un grupo abeliano y existe una aplicación

$$\begin{aligned} R \times M &\longrightarrow M \\ (a, m) &\longmapsto a \cdot m \end{aligned}$$

con las siguientes propiedades

i) $\forall m\ (1\cdot m = m)$

ii) Para cada $a\in R$ $\forall m,n\ (a\cdot(m+n) = a\cdot m + a\cdot n)$

iii) Para cualesquiera $a,b\in R$ $\forall m\ ((a+b)\cdot m = a\cdot m + b\cdot m)$

iv) Para cualesquier $a,b\in R$ $\forall m\ (a\cdot(b\cdot m) = (ab)\cdot m)$

Cuando R es un campo, M es un R-espacio vectorial ó un espacio vectorial sobre R, los elementos de R se llaman escalares y los elementos de M vectores, la operación $+$ es adición vectorial, el producto $\cdot$ es la multiplicación escalar.

Parte de esta notación se usa aun en el caso en que R es un anillo, no un campo

---

Ejemplos

1) El grupo trivial $\{0\}$ es un R-módulo para cualquier anillo R

Pues $r\cdot 0 = 0 \in \{0\}$ para todo $r \in R$

2) Sea R un anillo. El producto cartesiano

$$R\times R = R^2$$

Consiste en parejas (a,b) con $a,b\in R$

En general

$$R\times \dots \times R = R^n$$

Consiste en n-adas de elementos de R

$$(r_1,\dots,r_n) \qquad r_i \in R$$

Notemos que

$(R^n,+)$ es un grupo abeliano

con la operación

$$(r_1,\dots,r_n)+(s_1,\dots,s_n) = (r_1+s_1,\dots,r_n+s_n)$$

(El alumno debe convencerse de que se cumplen los axiomas de grupo abeliano)

Ahora, sea $(r_1,\dots,r_n)\in R^n$ y $a\in R$

definimos

$$a(r_1,\dots,r_n) = (ar_1,\dots,ar_n)$$

que resulta un elemento de R^n

El ~~de~~ alumno debe verificar que se cumplen los axiomas que convierten a $(R^n,+,\underline{1},\underline{0},\cdot)$

en un R-módulo, donde

$$\underline{1}=(1,\dots,1)\in R^n$$

$$\underline{0}=(0,\dots,0)\in R^n$$

Si R es un campo F, obtenemos un F-espacio vectorial.

Note que si $n=1$, $R^1=R$ es un R-módulo y si $R=F$ es campo, F mismo es un espacio vectorial sobre F.

3) Sea G un grupo abeliano $(G,+)$ es el grupo. Podemos ver a G como un $\mathbb{Z}$-módulo, si hacemos

$$0_{\mathbb{Z}}\cdot a=0_G$$

$$k\cdot a=\underbrace{a+\dots+a}_{k \text{ veces}}$$

$$(-k)a=-(k\cdot a)=\underbrace{(-a)+\dots+(-a)}_{k \text{ veces}}$$

para todo $a\in G$, para cada $k\in\mathbb{Z}$, $k\neq 0$.

Así, cualquier grupo abeliano G es a la vez

Un $\mathbb{Z}$-módulo

---

5) Supongamos que $f, g, h : I \to \mathbb{R}$
I un intervalo en $\mathbb{R}$, f, g, h continuas
Sea V la colección de todas estas funciones.
Note que podemos hacer
$$(f+g)(x) = f(x) + g(x)$$
para cualquier $f, g \in V$
Si $a \in \mathbb{R}$,
$$(af)(x) = af(x)$$
Sabemos que $f+g$ y af son funciones continuas, cuando $f, g \in V$
Por tanto V es un espacio vectorial sobre $\mathbb{R}$.
En forma análoga, si V consiste en funciones $f : I \to \mathbb{R}$ continuas y diferenciables (integrables), V resulta ser un $\mathbb{R}$-espacio vectorial.

6) El conjunto $\mathbb{C}^n$ es un espacio vectorial sobre $\mathbb{C}$ como vimos antes, pero también $\mathbb{C}^n$ también es un espacio vectorial sobre $\mathbb{R}$ o sobre $\mathbb{Q}$

si $(z_1, \dots, z_n) \in \mathbb{C}^n$

y $a \in \mathbb{R}$

$$a(z_1, \dots, z_n) = (az_1, \dots, az_n) \in \mathbb{C}^n$$

o algo correspondiente para $a \in \mathbb{Q}$.

En general cuando K es un campo y F un subcampo de K,

Si V es un espacio vectorial sobre K también se puede convertir en un espacio vectorial sobre F

Si M es un R-módulo y S es un subanillo de R, M se puede convertir en un S-módulo.

Usaremos la notación $(a_{ij})_{m \times n}$ para denotar una matriz de m renglones y n columnas

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

a_{ij} es una entrada de la matriz. Si las entradas pertenecen a un anillo R decimos que es una matriz de $m \times n$ sobre R

$M_{m\times n}(R)$ denota el conjunto de matrices sobre R.

Si $m=n$ hablamos de una matriz cuadrada y su colección se representa como $M_n(R)$

I_n representa la matriz identidad de tamaño n

$$\begin{pmatrix} 1 & \cdots & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 1 \end{pmatrix}$$

Con 1 en la diagonal. Así

$$a_{ij} = \delta_{ij} = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{si } i = j \end{cases}$$

$0_{m\times n}$ o simplemente 0 cuando m, n queden claros, denota a la matriz de $m\times n$ cuyas entradas son 0.
Es la matriz trivial o cero.

En $M_{m\times n}(R)$ podemos definir suma y producto escalar

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$$

$$r(a_{ij}) = (r a_{ij})$$

Estas operaciones convierten a $M_{m\times n}$ en un R-módulo, algo que el alumno debe verificar.

Si U, V son conjuntos, se acostumbra escribir U^V para el conjunto de funciones de V en U

$$U^V = \{ f \mid dom(f) = V,\ ran(f) \subseteq U \}$$

Sean R un anillo y S un conjunto
Sean $f, g \in R^S$. Definimos la función

$f+g \in R^S$ mediante la prescripción

$$(f+g)s = f(s)+g(s) \text{ para todo } s \in S$$

Si $a \in R$, $af \in R^S$, donde

$$(af)(s) = af(s) \text{ para cualquier } s \in S$$

Otra vez, el estudiante debe verificar que de esta forma R^S es un R-módulo

Note que el 0 de R^S es la función

$$0(s) = 0_R \text{ para cualquier } s \in S.$$

Como ilustración considere $S = \{a, b\}$

La siguiente tabla procura expresar $\mathbb{Z}_3^S$ es decir, funciones de S en $\mathbb{Z}_3$

$\mathbb{Z}_3$	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9
a	0	0	0	1	1	1	2	2	2
b	0	1	2	0	1	2	0	1	2

así $f_6(a) = 1$

$f_6(b) = 2$

Dado que $\mathbb{Z}_3$ es un campo, $\mathbb{Z}_3^S$ es un espacio vectorial de 9 elementos. La función f_1 es la trivial en $\mathbb{Z}_3^S$. Note que

$$(f_5 + f_6)(a) = 2$$
$$(f_5 + f_6)(b) = 3 = 0$$
$$f_5 + f_6 = f_7$$
$$2f_8(a) = 4 = 1$$
$$2f_8(b) = 2$$

de modo que $2f_8 = f_6$

Sea R un anillo. Sea I un subgrupo de R (no necesariamente subanillo). Decimos que I es un ideal de R cuando $ra \in I$ para cada $r \in R$, toda $a \in I$.

Entonces, I se convierte en un R-módulo
