Algebra Lineal: Aplicaciones a la Física, Curso 2012

0. Repaso de estructuras algebraicas básicas

Un sistema algebraico es un conjunto no vacío de elementos, A, junto con un conjunto de operaciones **cerradas** sobre A que satisfacen ciertas propiedades.

Un **monoide** es un sistema algebraico $\{A, *\}$ formado por un conjunto A y una operación binaria cerrada $*: A \times A \to A$ (también llamada ley de composición interna).
Ejemplos bien conocidos son $\{\mathbb{R}, +\}$ (el conj. de num. reales con la suma), $\{\mathbb{R}, \cdot\}$ (los reales con el prod.) $\{\mathbb{R}_+, \cdot\}$ (los reales positivos con el producto). En cambio, $\{\mathbb{R}_-, \cdot\}$, donde $\mathbb{R}_-$ denota los reales negativos, no es un monoide pues la operación no es cerrada.

Un **grupo** es un monoide $\{A, *\}$ donde A y la operación $*$ satisfacen
1) Asociatividad: $a * (b * c) = (a * b) * c \ \forall\ a, b, c \in A$
2) Existencia de elemento identidad: $\exists\ I \in A$ t.q. $\forall\ a \in A$, $a * I = I * a = a$
3) Existencia de elemento inverso: $\forall\ a \in A\ \exists\ a^{-1} \in A$ t.q. $a * a^{-1} = a^{-1} * a = I$
Un **semigrupo** es un monoide $\{A, *\}$ que satisface la prop. 1), aunque no necesariamente 2) y 3).

Recordemos la *unicidad* de la identidad y de la inversa:
i) La identidad I, si existe, es única: Supongamos que $\exists\ I$, I' t.q. $I * a = a$, $a * I' = a\ \forall\ a \in A$. Entonces $I * I' = I'$ (caso $a = I'$) y $I * I' = I$ (caso $a = I$) por lo que $I' = I$. Esto muestra también que si existe una identidad a izquierda I y una identidad a derecha I', necesariamente son coincidentes!
ii) La inversa $b = a^{-1}$ de a, si existe, es única: Supongamos que $\exists$ otra inversa b'. Entonces $b * (a * b') = b * I = b$, pero por asociatividad, $b * (a * b') = (b * a) * b' = I * b' = b'$, de donde $b = b'$.
Esto muestra también que si $\exists$ una inversa a izquierda b y una inversa a derecha b' necesariamente son coincidentes. Puede ocurrir, no obstante, que exista inversa a izquierda pero no a derecha, y viceversa, en cuyo caso pueden no ser únicas, como veremos posteriormente.
Si la operación binaria satisface $a * a' = a' * a\ \forall\ a, a' \in A$, se dice que es *conmutativa*. En tal caso, el grupo se denomina conmutativo o *abeliano*. En caso contrario el grupo es no abeliano o no conmutativo.

Ejemplos de grupos abelianos son:
1) $\{\mathbb{R}, +\}$, donde la identidad es el 0 y el inverso de $a \in \mathbb{R}$ el opuesto $-a$
2) $\{\mathbb{R}_0, \cdot\}$, donde $\mathbb{R}_0$ denota los reales sin el 0, la identidad es el 1 y el elemento inverso $a^{-1} = 1/a$
3)$\{\mathbb{R}^2, +\}$, donde la identidad es el vector nulo $(0, 0)$ y el inverso de $a = (x, y)$ el vector opuesto $(-x, -y)$
4) $\{\mathbb{R}^{2\times 2}, +\}$, donde la identidad es la matriz nula $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ y el inverso de $a = \left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right)$ la matriz opuesta $\left(\begin{smallmatrix} -x & -y \\ -z & -t \end{smallmatrix}\right)$.
Nótese en cambio que $\{\mathbb{R}^3, \times\}$, donde $\times$ denota el producto vectorial, es un monoide pero no es grupo ni semigrupo pues el producto vectorial no es asociatvo (por ej., $\vec{i} \times (\vec{i} \times \vec{j}) = \vec{i} \times \vec{k} = -\vec{j} \neq (\vec{i} \times \vec{i}) \times \vec{j} = \vec{0}$).

Ejemplos de grupos no abelianos son:
1) $GL(n)$: $\{M, \cdot\}$, donde $M = \{A \in \mathbb{R}^{n\times n}, \mathrm{Det}[A] \neq 0\}$ es el conjunto de matrices reales de $n \times n$ de determinante no nulo y $\cdot$ la operación de multiplicación matricial usual (Grupo gral. lineal). En efecto,
i) la operación $\cdot$ es cerrada en el conjunto pues si $A, B \in M$, $A.B \in \mathbb{R}^{n\times n}$ y $\mathrm{Det}[A \cdot B] = \mathrm{Det}[A]\mathrm{Det}[B] \neq 0$
ii) el producto matricial es asociativo
iii) La identidad $I \in M$ ($\mathrm{Det}[I] = 1 \neq 0$)
iv) Si $A \in M \Rightarrow \mathrm{Det}\, A \neq 0$ y por lo tanto $\exists$ la matriz inversa A^{-1} t.q. $A \cdot A^{-1} = A^{-1} \cdot A = I$. Por su puesto, $A^{-1} \in M$ pues $\mathrm{Det}[A^{-1}] = 1/\mathrm{Det}[A] \neq 0$.
Ejercicio: Explicar, considerando la multiplicación matricial usual, por qué
1a) el conjunto de matrices reales de 2×2 de determinante 2 no es un grupo.
1b) el conjunto de todas las matrices reales de 2×2 sin la matriz nula $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, tampoco es grupo.
1c) el conjunto de matrices reales de 2×2 de determinante 1 si es un grupo.

2) $O(n)$: Grupo de matrices reales ortogonales de $n \times n$ (con la multiplicación matricial usual), donde ortogonal significa que $A^{-1} = A^t$ (matriz traspuesta), es decir, $AA^t = A^tA = I$. En efecto,
i) Si $A, B \in O(n)$, $(AB)^{-1} = B^{-1}A^{-1} = B^tA^t = (AB)^t$, por lo que $AB \in O(n)$
ii) El producto matricial es asociativo
iii) $I \in A$, ya que $I^{-1} = I = I^t$. Aquí I denota la matriz identidad, de elementos $I_{ij} = \delta_{ij} = \{^{1,\ i=j}_{0,\ i\neq j}$.
iv) si $A \in O(n) \Rightarrow A^{-1} = A^t \in O(n)$ pues $(A^{-1})^{-1} = (A^t)^{-1} = (A^{-1})^t$.

Notemos que si $AA^t = I \Rightarrow \mathrm{Det}[AA^t] = \mathrm{Det}[A]^2 = \mathrm{Det}[I] = 1$, por lo que $\mathrm{Det}[A] = \pm 1$.

3) $SO(n)$: grupo de matrices reales ortogonales de $n \times n$ de determinante 1.
Este subconjunto de $O(n)$ es también un grupo, pues
i) Si $A, B \in SO(n)$, $\mathrm{Det}[AB] = \mathrm{Det}[A]\mathrm{Det}[B] = 1$
iii) $I \in SO(n)$ pues $\mathrm{Det}[I] = 1$
iv) $A^{-1} \in SO(n)$ pues $\mathrm{Det}[A^{-1}] = 1/\mathrm{Det}[A] = 1$.
Veremos luego que $SO(n)$ es el grupo de rotaciones en $\mathbb{R}^n$ (rotaciones alrededor de ejes que pasen por el origen, es decir, que dejan el origen fijo).

4) $U(n)$: Grupo de matrices complejas unitarias de $n \times n$, con la operación de multiplicación matricial usual, donde unitario significa que $A^{-1} = A^\dagger$, siendo $A^\dagger \equiv (A^t)^*$ (matriz traspuesta conjugada).
Se deja como ejercicio mostrar que es grupo.
5) $SU(n)$: Grupo de matrices complejas unitarias de $n \times n$ de determinante 1.
Se deja también como ejercicio mostrar que es grupo.

Los grupos anteriores constan de un número infinito de elementos. Un grupo puede también constar de un número finito de elementos (grupo finito). Por ejemplo, $\{\{1, -1\}, .\}$ es un grupo con el producto usual, y también lo es $\{\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}-1&0\\0&-1\end{pmatrix}\}, \cdot\}$ con el producto matricial usual.

Dado que el conjunto de operaciones geométricas (rotaciones, reflexiones, etc.) que dejan invariante un cierto sistema físico forma un grupo con respecto a la operación de composición, los grupos juegan un rol fundamental en Física, especialmente en Mecánica Cuántica, caracterizando las simetrías y determinando sus consecuencias.

Un **anillo** $\{A, +, *\}$ es un conjunto A munido de dos operaciones binarias que satisface :
1) $\{A, +\}$ es un grupo abeliano
2) $a * (b * c) = (a * b) * c\ \forall\ a, b, c \in A$ (Asociatividad de $*$)
3) $a * (b + c) = a * b + a * c$, $\ (b + c) * a = b * a + c * a$ (Distributividad)
Si además $a * b = b * a\ \forall\ a, b \in A$ el anillo es conmutativo.
Ej.: $\{\mathbb{Z}, +, \cdot\}$ es anillo conmutativo.
El inverso respecto de $+$ se denomina opuesto, y la identidad respecto de $+$ elemento neutro o 0.

Un **cuerpo** o **campo** $\{F, +, *\}$ es un conjunto F munido de dos operaciones binarias $+, *$ que satisface:
1) $\{F, +\}$ es grupo abeliano
2) $\{F_0, *\}$ es grupo abeliano, donde F_0 es el conjunto de elementos de F distintos de 0 (elem. neutro)
3) $*$ es distributiva con respecto a $+$.
La identidad respecto de $*$ se denomina 1 (unidad). Un cuerpo es pues un anillo conmutativo con unidad donde $\forall\ a \in F_0\ \exists\ a^{-1} \in F_0$ tal que $a^{-1} * a = a * a^{-1} = 1$.

Ejemplos: $\{\mathbb{R}, +, \cdot\}$, $\{\mathbb{C}, +, \cdot\}$ son cuerpos. En cambio, $\{\mathbb{Z}, +, \cdot\}$ no es cuerpo pues la inversa de un entero no es necesariamente entero.
Los cuerpos pueden constar también de un número *finito* de elementos. El menor es $Z_2 = \{A = \{0, 1\}, +, \cdot\}$, donde $+$ y $\cdot$ denotan la suma y producto módulo 2 (el resto de dividir la suma y mult. ordinarias por 2): $0 + 0 = 0$, $0 + 1 = 1$, $1 + 1 = 0$, $0 \cdot 0 = 0 \cdot 1 = 0$, $1 \cdot 1 = 1$.
En general, $Z_p = \{(0, 1, \ldots, p - 1), +, \cdot\}$, con $+$ y $\cdot$ la suma y producto módulo p, es cuerpo para p primo. Esto puede demostrarse a partir del "pequeño teorema de Fermt": Si p es primo $\Rightarrow a^p = a \pmod p$ $\forall\ a$ entero.

1. Espacios vectoriales

Partiendo del concepto intuitivo de vectores de $\mathbb{R}^2$ o $\mathbb{R}^3$, extenderemos el concepto de vector a elementos de un sistema algebraico abstracto, llamado *espacio vectorial* (o *lineal*), en el que se cumplen propiedades análogas a las de $\mathbb{R}^2$ o $\mathbb{R}^3$ con respecto a la suma de vectores y a la multiplicación de un vector por un número real. Remarquemos que estas dos operaciones son **cerradas** en $\mathbb{R}^2$ y en $\mathbb{R}^3$.

Definición: Sea $\{K, +, \cdot\}$ un cuerpo, y sea $\{V, \oplus\}$ un grupo abeliano. Un espacio vectorial V sobre el cuerpo K, denotado por $V(K)$, es una estructura algebraica $\{K, +, \cdot, V, \oplus, *\}$ donde $* : V \times K \to V$ denota una multiplicación de elementos de K por elementos de V que da como resultado un elemento de V y que satistface: $\forall\ \alpha, \beta \in K$ y $\forall\ v, w \in V$:
1) $\alpha * (v \oplus w) = (\alpha * v) \oplus (\alpha * w)$
2) $(\alpha + \beta) * v = (\alpha * v) \oplus (\beta * v)$
3) $(\alpha \cdot \beta) * v = \alpha * (\beta * v)$
4) $1 * v = v$
donde 1 denota la identidad del cuerpo K respecto del producto.
Los elementos de V se denominan **vectores** y los de K **escalares**.

En el caso de $\mathbb{R}^2$, $\{V, \oplus\}$ es el grupo $\{\mathbb{R}^2, +\}$, con $\oplus = +$ la suma usual de vectores, y $\{K, +, \cdot\}$ el cuerpo de los reales $\{\mathbb{R}, +, \cdot\}$ con la suma y producto usual. La operación $*$ es el producto de un vector por un número real.
La definición general extiende pues $\{\mathbb{R}^2, +\}$ a un grupo abeliano arbitrario $\{V, \oplus\}$ y $\{\mathbb{R}, +, \cdot\}$ a un cuerpo arbitrario $\{K, +, \cdot\}$. Si este es el cuerpo de los reales $\{\mathbb{R}, +, \cdot\}$, el espacio vectorial se dice *real*, y si es el cuerpo de los complejos $\{\mathbb{C}, +, \cdot\}$, el espacio vectorial se dice *complejo*.

En los sucesivo, para aligerar la notación seguiremos la costumbre universal de denotar la operación $\oplus$ (suma de vectores) también con $+$ y de omitir los símbolos $\cdot$ y $*$, quedando la multiplicación de escalares y de escalares por vectores automáticamente asumida. Las 4 condiciones anteriores se reescriben como:
1) $\alpha(v + w) = \alpha v + \alpha w$
2) $(\alpha + \beta)v = \alpha v + \beta v$
3) $(\alpha\beta)v = \alpha(\beta v)$
4) $1v = v$

De la definición de espacio vectorial se desprende que si $v, w \in V$ y $\alpha, \beta \in K$, la *combinación lineal*

$$u = \alpha v + \beta w$$

queda automáticamente definida y *pertenece también* a V, para todo par de elementos α y β del cuerpo y v, w de V. Esta, podemos afirmar, es la característica principal de un espacio vectorial. Es decir, es posbile multiplicar un vector por un escalar, lo cual es siempre otro vector de V, y también es posible sumar dos vectores cualesquiera, siendo la suma también un vector de V.
En general, si $v_i \in V$, $\alpha_i \in K$, $i = 1, \ldots, n$,

$$v = \alpha_1 v_1 + \ldots + \alpha_n v_n$$

se denomina *combinación lineal* de los vectores $v_1, \ldots, v_n$, y es un vector $\in V$. Los escalares $\alpha_1, \ldots, \alpha_n$ se denominan los coeficientes de la combinación lineal.
Por ejemplo, el conjunto de todos los vectores del plano forma un espacio vectorial sobre $\mathbb{R}$ con la suma usual, pero el conjunto de los vectores del plano superior $\{(x, y) \in \mathbb{R}^2,\ y \geq 0\}$ NO es un espacio vectorial pues $-1 * (x, y) = (-x, -y)$ pertenece al plano inferior.

Debe destacarse además que el producto de vectores (escalar, vectorial u otro) no juega absolutamente ningún rol en la definición de espacio vectorial, y puede no estar definido en el mismo.

Demostremos ahora cuatro propiedades básicas válidas en cualquier espacio vectorial:
a) $0v = 0 \; \forall \; v \in V$
donde el primer 0 denota el 0 del cuerpo K (el elemento neutro respecto de la operación + para escalares) y el segundo el cero de V (la identidad respecto de la operación + para vectores).
En efecto, $0v = (0+0)v = 0v + 0v$ por (2). Sumando el inverso $-(0v)$ $(-(0v)+(0v) = 0)$ en ambos miembros obtenemos $0 = (0v) + 0 = 0v$, por lo que $0v = 0$.
b) $\alpha 0 = 0 \; \forall \; \alpha \in K$
donde 0 denota el cero de V. Tenemos $\alpha 0 = \alpha(0+0) = \alpha 0 + \alpha 0$, por 1). Sumando el inverso $-(\alpha 0)$ en ambos miembros se obtiene $0 = (\alpha 0) + 0 = \alpha 0$, por lo que $\alpha 0 = 0$.
c) $(-\alpha)v = -1(\alpha v) = -(\alpha v) = \alpha(-v)$
Tenemos, por 3), $(-\alpha)v = (-1\alpha)v = -1(\alpha v)$.
Además, $(-\alpha)v + \alpha v = (-\alpha + \alpha)v = 0v = 0$ por 2) y a), por lo que $(-\alpha)v = -(\alpha v)$ (opuesto de αv).
Finalmente, de b) y 1), $0 = \alpha 0 = \alpha(v + (-v)) = \alpha v + (\alpha(-v))$, por lo que $\alpha(-v)$ es también el opuesto de αv y por lo tanto coincide con $(-\alpha)v$ (unicidad del opuesto!).
d) Si $\alpha v = 0 \Rightarrow \alpha = 0$ o $v = 0$.
En efecto, por b), 3) y 4), si $\alpha \neq 0 \Rightarrow 0 = \alpha^{-1}0 = \alpha^{-1}(\alpha v) = (\alpha^{-1}\alpha)v = 1v = v$ por lo que $v = 0$. Por a), también se cumple si $\alpha = 0$.

Ejemplos de espacios vectoriales:
1) $K^n = \{(x_1, \ldots, x_n), x_i \in K, i = 1, \ldots, n\}$
Es el conjunto de n-uplas de elementos del cuerpo K. La suma de vectores se define como

$$(x_1, \ldots, x_n) + (x'_1, \ldots, x'_n) = (x_1 + x'_1, \ldots, x_n + x'_n)$$

y la multiplicación por un escalar $\alpha \in K$ como

$$\alpha(x_1, \ldots, x_n) = (\alpha x_1, \ldots, \alpha x_n)$$

El elemento neutro es $(0, \ldots, 0)$ y el opuesto de $(x_1, \ldots, x_n)$ es $-(x_1, \ldots, x_n) = (-x_1, \ldots, -x_n)$.
El caso $n = 1$ corresponde a tomar los elementos del cuerpo como vectores y escalares al mismo tiempo (es decir, como grupo abeliano $\{K, +\}$ y cuerpo $\{K, +, \cdot\}$).
El caso $K = \mathbb{R}$ con la suma y producto usual de números reales, se denomina espacio cartesiano. $\mathbb{R}^1$ consiste en tomar los reales como vectores y escalares al mismo tiempo, y corresponde geométricamente a una recta. $\mathbb{R}^2$ corresponde al plano y $\mathbb{R}^3$ al espacio cartesiano tridimensional.
Si $K = \mathbb{C}$, con + y $\cdot$ la suma y producto usual de números complejos, se obtiene el espacio $\mathbb{C}^n$, es decir, el conjunto de n-uplas complejas $\{(z_1, \ldots, z_n),\; z_i \in \mathbb{C}, i = 1, \ldots, n\}$, con escalares también complejos.
Se lo denota usualmente por $\mathbb{C}^n(\mathbb{C})$, para distinguirlo del espacio $\mathbb{C}^n(\mathbb{R})$, que es similar al anterior pero con los escalares restringidos a números reales, es decir, $\alpha_i \in \mathbb{R}$. Puede verse fácilmente que $\mathbb{C}^n(\mathbb{R})$ es también un espacio vectorial.
2) $\mathbb{K}^{m\times n}$. Es el conjunto de matrices A de $m \times n$ con elementos $A_{ij} = x_{ij}$ pertenecientes al cuerpo K, $i = 1, \ldots, m$, $j = 1, \ldots, n$, consideradas con la suma usual y el producto usual por un escalar. La suma se define por

$$\begin{pmatrix} x_{11} & \ldots & x_{1n} \\ & \ldots & \\ x_{m1} & \ldots & x_{mn} \end{pmatrix} + \begin{pmatrix} y_{11} & \ldots & y_{1n} \\ & \ldots & \\ y_{m1} & \ldots & y_{mn} \end{pmatrix} = \begin{pmatrix} x_{11}+y_{11} & \ldots & x_{1n}+y_{1n} \\ & \ldots & \\ x_{m1}+y_{m1} & \ldots & x_{mn}+y_{mn} \end{pmatrix}$$

y la multiplicación por un escalar como

$$\alpha \begin{pmatrix} x_{11} & \ldots & x_{1n} \\ & \ldots & \\ x_{m1} & \ldots & x_{mn} \end{pmatrix} = \begin{pmatrix} \alpha x_{11} & \ldots & \alpha x_{1n} \\ & \ldots & \\ \alpha x_{m1} & \ldots & \alpha_{mn} \end{pmatrix}$$

El elemento neutro es la matriz nula $0 = \begin{pmatrix} 0 & \ldots & 0 \\ & \ldots & \\ 0 & \ldots & 0 \end{pmatrix}$, y el opuesto de A es $-A = \begin{pmatrix} -x_{11} & \ldots & -x_{1n} \\ & \ldots & \\ -x_{m1} & \ldots & -x_{mn} \end{pmatrix}$.
Si $K = \mathbb{R}$ se obtiene el espacio de matrices reales de $m \times n$, y si $K = \mathbb{C}$, el de matrices complejas de $m \times n$. Este último puede considerarse con escalares complejos ($C^{m\times n}(\mathbb{C})$) o reales ($C^{m\times n}(\mathbb{R})$).

3) En general, si D es un conjunto no vacío, puede definirse el espacio vectorial

$$K^D = \{f \mid f \text{ es funcion de } D \text{ en } K\}$$

es decir, el conjunto de las funciones $f : D \to K$. La suma y producto de funciones se define como

$$(f+g)(x) = f(x) + g(x), \quad (\alpha f)(x) = \alpha f(x)$$

$\forall\, x \in D$, siendo el cero la función nula $0(x) = 0\ \forall\, x \in D$. Se verifican fácilmente que se satisfacen todas las condiciones de espacio vectorial. Por ejemplo,
$[\alpha(f+g)](x) = \alpha[(f+g)(x)] = \alpha(f(x)+g(x)) = \alpha f(x) + \alpha g(x) = (\alpha f + \alpha g)(x)$.
$[(\alpha+\beta)f](x) = (\alpha+\beta)f(x) = \alpha f(x) + \beta f(x) = (\alpha f + \beta f)(x)$
(verificación de las restantes a cargo del lector si lo considera necesario).

Así, si D es el conjunto $\{1, \ldots, n\}$, K^n es equivalente al espacio de n-uplas K^n anterior.

Si $K = D = \mathbb{R}$, se obtiene el espacio vectorial de funciones reales $\mathbb{R}^{\mathbb{R}} = \{f | f : \mathbb{R} \to \mathbb{R}\}$, y si $K = D = \mathbb{C}$, el espacio de funciones complejas $\mathbb{C}^{\mathbb{C}} = \{f | f : \mathbb{C} \to \mathbb{C}\}$.
Si $D = \mathbb{N}$, se obtiene el espacio vectorial de sucesiones de elementos de K, $\{x_n\} \equiv (x_1, x_2, \ldots)$.

2. Subespacios

Un subconjunto de vectores $S \subset V$ es un subespacio de V si es también un espacio vectorial.
Como consecuencia, un subconjunto de vectores $S \subset V$ *no vacío* es un subespacio si y sólo si S es *cerrado* bajo las operaciones de suma de vectores y multiplicación por escalar. Debe cumplirse entonces
0) $0 \in S$ (asegura que no sea vacío)
1) Si $v, w \in S \Rightarrow v + w \in S$
2) Si $v \in S$ y $\alpha \in K \Rightarrow \alpha v \in S$
Si se sabe que es no vacío bastan 1) y 2), pues si $\exists v \in S$, $0 = 0v \in S$ por 2).

Dem.: Es evidente que estas condiciones son necesarias. Para probar la suficiencia, podemos ver que por 1), la operación de suma es cerrada y asociativa en S, que por 0) o 2) $0 \in S$ y que $\forall\, v \in S\ \exists$ el elemento opuesto $-v = -1v \in S$ por 2), de modo que $\{S, +\}$ es grupo abeliano. Además, el producto de un vector de S por un escalar es siempre otro vector de S, por 2), por lo que la combinación lineal $\alpha v + \beta w$ pertence siempre a S. Las demás condiciones 1-4 se heredan de V, pues las operaciones son las mismas.
Cualquier espacio vectorial contiene siempre dos subespacios triviales: $S = V$ y $S = \{0\}$ (el vector nulo).

Ejemplos:
1) Si $V = \mathbb{R}^2$, $S = \{(x,y) \mid ax + by = 0,\ a, b \in \mathbb{R},\ a \neq 0 \text{ o } b \neq 0\}$ es siempre un subespacio de $\mathbb{R}^2$, que representa geométricamente una recta que pasa el origen. En efecto, si $(x,y), (x',y') \in S$, $(x,y) + (x',y') = (x+x', y+y') \in S$ pues $a(x+x') + b(y+y') = (ax+by) + (ax'+by') = 0 + 0 = 0$, y $\alpha(x,y) = (\alpha x, \alpha y) \in S$ pues $a\alpha x + b\alpha y = \alpha(ax+by) = 0$.
Geométricamente, los subespacios no triviales de $\mathbb{R}^2$ son pues rectas que pasan por el origen.
2) Si $V = \mathbb{R}^3$, se prueba en forma análoga que los subespacios no triviales son planos o rectas que pasan por el origen, es decir, $S = \{(x,y,z) \mid ax + by + cz = 0, \text{ con } (a,b,c) \text{ vector no nulo}\}$ (plano $\perp$ a (a,b,c)) o
$S = \{(x,y,z) \mid ax + by + cz = 0,\ dx + ey + fz = 0, \text{ con } (a,b,c),\ (d,e,f) \text{ vectores no nulos y no paralelos}\}$ (rectas).
Por ejemplo, $S = \{(x,y,z) \,|\, x+y+z = 0\}$ es un subespacio de $\mathbb{R}^3$ que representa geométricamente un plano ($\perp$ a $(1,1,1)$) que contiene al origen, $S = \{(x,y,z) \,|\, x+y+z = 0,\ x-y = 0\}$ es un subespacio que representa a una recta que pasa por el origen ($\parallel$ a $(1,1,-2)$) pero $C = \{(x,y,z) \,|\, x+y+z = 1\}$, $D = \{(x,y,z) \,|\, x \geq 0\}$, y $E = \{(x,y,z) \,|\, x^2 + y = 0\}$ NO son subespacios (probar!).
En general, si $V = \mathbb{K}^n$, $S = \{(x_1, \ldots, x_n) \,|\, a_{i1}x_1 + \ldots + a_{in}x_n = 0, i = 1, \ldots, m,\ a_{in} \in K\}$ es siempre un subespacio de V (que puede ser $\{0\}$ si la única solución al sistema es $x_i = 0$ para $i = 1, \ldots, n$, o V si todos los coeficientes a_{ij} son nulos). Corresponde en general a un hiperplano que pasa por el origen. Se prueba de la misma manera anterior (hecho en clase y se deja como ejercicio).

3) Si $V=\mathbb{R}^{n\times n}$, son subespacios:
El conjunto de matrices diagonales ($A_{ij}=0$ si $i\neq j$)
El conjunto de matrices simétricas ($A_{ij}=A_{ji}\ \forall\ i,j$)
El conjunto de matrices antisimétricas ($A_{ij}=-A_{ji}\ \forall\ i,j$)
El conjunto de matrices donde los coeficientes satisfacen un conjunto de ecuaciones lineales homogéneas $\sum_{i,j}a_{kij}A_{ij}=0$, $k=1,\ldots,p$, que incluye como casos particulares todos los anteriores.

4) Si $V=\mathbb{R}^{\mathbb{R}}$ (funciones reales de $\mathbb{R}$ en $\mathbb{R}$), el conjunto de los polinomios, es decir, de las funciones

$$f(x)=a_0+a_1x+\ldots+a_nx^n$$

con $a_i\in\mathbb{R}$, es un subespacio de V. Es claro que la suma es también un polinomio, que la función nula 0 es un polinomio (de grado 0) y que el producto de un polinomio por un escalar es un polinomio.
En cambio, el conjunto de los polinomios de grado fijo $n>0$ NO es un subespacio, ya que en particular 0 no pertenece al mismo (y la suma no es cerrada).
El conjunto de polinomios de grado $\leq n$ si es en cambio un subespacio.
También lo son, por ejemplo (probarlo como ejercicio):
i) el conjunto de funciones reales continuas
ii) el i) el conjunto de funciones reales derivables
iii) el de funciones que satisfacen $f(a)=0$ para un cierto $a\in\mathbb{R}$ (o en general, $\sum_{i=1}^m\alpha_if(a_i)=0$)
iv) el conjunto de funciones de período L ($f(x+L)=f(x)\ \forall\ x\in\mathbb{R}$).
v) el conjunto de funciones pares ($f(x)=f(-x)$) y el de funciones impares ($f(x)=-f(-x)$).

Subespacio generado por un conjunto de vectores

Dado un conjunto $M=\{v_1,\ldots,v_m\}$ de vectores $\subset V$, el conjunto de combinaciones lineales

$$\overline{M}=\{\alpha_1v_1+\ldots+\alpha_mv_m,\ \ \alpha_i\in K,\ i=1,\ldots,m\}$$

es un subespacio de V denominado subespacio generado por M. Es fácil ver que es un subespacio, ya que
0) $0=0v_1+\ldots 0v_m\in\overline{M}$
1) $(\alpha_1v_1+\ldots+\alpha_mv_m)+(\alpha'_1v_1+\ldots+\alpha'_mv_m)=(\alpha_1+\alpha'_1)v_1+\ldots+(\alpha_m+\alpha'_m)v_m\in\overline{M}$
2) $\beta(\alpha_1v_1+\ldots+\alpha_mv_m)=(\beta\alpha_1)v_1+\ldots+(\beta\alpha_m)v_m\in\overline{M}$
donde, para $i=1,\ldots,m$, $\alpha_i,\alpha'_i,\beta\in K$.
Los vectores de M se denominan *generadores* de $\overline{M}$.
En general, para un conjunto aribtrario $M\subset V$, podemos definir $\overline{M}$ como el conjunto de todas las combinaciones lineales finitas de vectores de M. En particular, si S es un subespacio $\Rightarrow\overline{S}=S$, pues un subespacio debe contener todas las combinaciones lineales de sus vectores.
Como consecuencia, $\overline{M}$ es el *menor* subespacio que contiene a M: Si S es un subespacio y $M\subset S\Rightarrow\overline{M}\subset S$, ya que S debe contener a toda combinación lineal de sus elementos.
Ejemplo: En $V=\mathbb{R}^3$, si $M=\{(1,0,0),(1,1,0)\}\Rightarrow\overline{M}=\{(x+y,y,0)|\,x,y\in\mathbb{R}\}$ es el plano determinado por los vectores de M.

Un espacio vectorial V se llama **finitamente generado** si existe un conjunto finito de vectores M tal que $\overline{M}=V$.
Por ejemplo, $\mathbb{R}^2$ puede ser generado por los vectores $(1,0)$ y $(0,1)$, ya que $(x,y)=x(1,0)+y(0,1)$, y también por los vectores $(1,1)$ y $(0,1)$, ya que $(x,y)=x(1,1)+(y-x)(0,1)$. También puede ser generado por los vectores $(1,0)$, $(0,1)$ y $(1,1)$, ya que $(x,y)=(x-z)(1,0)+(y-z)(0,1)+z(1,1)$, con z arbitrario.
El espacio $\mathbb{R}^{\mathbb{R}}$ de funciones reales $f:\mathbb{R}\to\mathbb{R}$ no puede ser en cambio generado por conjunto finito de vectores.

Intersección, Unión y Suma de subespacios

1) La **Intersección** $S=S_1\cap S_2$ de dos subespacios S_1, S_2, es un subespacio.
En efecto, $0\in S_1$ y $0\in S_2$, por lo que $0\in S_1\cap S_2$. Además, si $u,v,\in S$, $u,v\in S_1$ y $u,v,\in S_2$, por lo que $u+v\in S_1$ y $u+v\in S_2$, y por lo tanto $u+v\in S$. Análogamente, $\alpha u\in S_1$ y $\alpha u\in S_2$, de modo que $\alpha u\in S$.
Por ejemplo, en $V=\mathbb{R}^2$, si $S_1=\{(x,y),x+y=0\}$ y $S_2=\{(x,y),x-y=0\}\Rightarrow S_1\cap S_2=\{(0,0)\}$

(Geométricamente la intersección de dos rectas distintas que pasan por el origen es $(0,0)$).
Y en $V=\mathbb{R}^3$, si $S_1=\{(x,y,z)|x+y+z=0\}$ y $S_2=\{(x,y,z)|x-y-z=0\}\Rightarrow S_1\cap S_2=\{(0,y,z)|y+z=0\}$ (Geométricamente la intersección de dos planos distintos que pasan por el origen es una recta).

2) La **Unión** de dos subespacios No es en general un subespacio. Por ejemplo, en el caso pre-anterior, $S_1\cup S_2=\{(x,y)\,|\,y=\pm|x|\}$ no es un subespacio, ya que no es cerrado por la operación de suma de vectores (aunque sí lo es por el producto por escalares!).

3) La **Suma** de subespacios $S=S_1+S_2$, definida por

$$S_1+S_2=\{v=v_1+v_2,\ v_1\in S_1,\ v_2\in S_2\}$$

es un subespacio. En efecto, 1) $0=0+0\in S$, 2) si $v=v_1+v_2$ y $u=u_1+u_2$, con $u_i,v_i\in S_i\Rightarrow v+u=(v_1+v_2)+(u_1+u_2)=(v_1+u_1)+(v_2+u_2)\in S$, y 3) si $v=v_1+v_2$, $\alpha v=\alpha v_1+\alpha v_2\in S$.
Obviamente $S_1\cup S_2\subset S_1+S_2$ pues $v_1=v_1+0$, $v_2=0+v_2$.

En realidad, es fácil demostrar que $S_1+S_2=\overline{S_1\cup S_2}$ (probarlo!).

En el ejemplo anterior, $S_1+S_2=\{(x+x',y+y')\,|\,x+y=0,x'-y'=0\}=\{(x+x',x'-x),x,x'\in\mathbb{R}\}=\mathbb{R}^2$.

Suma directa: Si $S_1\cap S_2=\{0\}$, se dice que la suma S_1+S_2 es *directa* y se la escribe como $S_1\oplus S_2$.
Si $S_1\cap S_2=\{0\}$, todo vector $v\in S_1+S_2$ puede escribirse de manera **única** como suma de un vector de S_1 y un vector de S_2, y viceversa. En efecto, si

$$\begin{aligned} v &= v_1+v_2\\ &= v_1'+v_2'\end{aligned}$$

con $v_i,v_i'\in S_i\Rightarrow 0=(v_1-v_1')+(v_2-v_2')$, por lo que $(v_1-v_1')=-(v_2-v_2')$, lo que implica, como $v_2-v_2'\in S_2$, que $v_1-v_1'\in$ también a S_2 y por lo tanto a $S_1\cap S_2$. Si $S_1\cap S_2=\{0\}\Rightarrow v_1-v_1'=0=v_2-v_2'$, por lo que $v_1=v_1'$, $v_2=v_2'$.
Análogamente, si todo vector $v\in S_1+S_2$ puede escribirse de manera única como v_1+v_2 y $v\in S_1\cap S_2\Rightarrow v=v+0=0+v$, por lo que la única posibilidad es $v=0$.
Demotraremos luego que dado un subespacio $S_1\subset V$, siempre existe un subespacio $S_2\subset V$ tal que $V=S_1\oplus S_2$ (se demostrará luego de introducir bases).
Ejemplos:
1) $\mathbb{R}^2=S_1\oplus S_2$, donde $S_1=\{(x,0)|x\in\mathbb{R}\}$ y $S_2=\{(0,y),|y\in\mathbb{R}\}$. En efecto, $S_1\cap S_2=\{0\}$ y $\forall\ v\in\mathbb{R}^2$ se cumple $v=(x,y)=v_1+v_2$, donde $v_1=(x,0)\in S_1$, $v_2=(0,y)\in S_2$.
Notemos, sin embargo, que también $\mathbb{R}^2=S_1\oplus S_2'$, donde nuevamente $S_1=\{(x,0)|x\in\mathbb{R}\}$ pero $S_2'=\{(x,x)|x\in\mathbb{R}\}$. En efecto, $S_1\cap S_2'=\{0\}$ y $\forall\ v\in V$ se cumple $v=(x,y)=v_1+v_2'$, donde $v_1=(x-y,0)\in S_1$ y $v_2=(y,y)\in S_2'$.

2) $\mathbb{R}^{n\times n}=\mathbb{R}^{n\times n}_s\oplus\mathbb{R}^{n\times n}_a$, donde $\mathbb{R}^{n\times n}_s$, $\mathbb{R}^{n\times n}_a$ denotan los subespacios de matrices simétricas y antisimétricas respectivamente. En efecto, $\mathbb{R}^{n\times n}_s\cap\mathbb{R}^{n\times n}_a=\{0\}$ (pues si $A\in\mathbb{R}^{n\times n}_s$ y $A\in\mathbb{R}^{n\times n}_a\Rightarrow A_{ij}=A_{ji}=-A_{ji}\ \forall i,j$, por lo que $A_{ij}=0\ \forall\ i,j$). Además, toda matriz A puede escribirse como

$$A=A_s+A_a,\ \ A_s=\frac{1}{2}(A+A^t)\in\mathbb{R}^{n\times n}_s,\ \ \ A_a=\frac{1}{2}(A-A^t)\in\mathbb{R}^{n\times n}_a$$

donde A^t es la matriz traspuesta, de modo que $\mathbb{R}^{n\times n}_s\oplus\mathbb{R}^{n\times n}_a=\mathbb{R}^{n\times n}$.

3) $\mathbb{R}^{\mathbb{R}}=\mathbb{R}^{\mathbb{R}}_p\oplus\mathbb{R}^{\mathbb{R}}_i$, donde $\mathbb{R}^{\mathbb{R}}_p$, $\mathbb{R}^{\mathbb{R}}_i$ denotan los subespacios de funciones pares e impares. En efecto, si $f(x)=f(-x)=-f(-x)\ \forall\ x\Rightarrow f(x)=0\ \forall\ x$. Además, toda función puede escribirse como

$$f(x)=f_p(x)+f_i(x),\ \ f_p(x)=\frac{1}{2}(f(x)+f(-x))\in\mathbb{R}^{\mathbb{R}}_p,\ \ f_i(x)=\frac{1}{2}(f(x)-f(-x))\in\mathbb{R}^{\mathbb{R}}_i$$

Los desarrollos de Taylor alrededor del origen de f_p y f_i, si existen, contienen sólo potencias pares o impares respect. Por ejemplo, si $f(x)=e^x$, $f_p(x)=\cosh(x)$, $f_i(x)=\sinh(x)$.