Joaquín Pérez Muñoz

Geometría I

Índice general

Introducción

Estos son los apuntes de la asignatura **Geometría I,** obligatoria de 6 créditos en el primer cuatrimestre del primer curso del Grado en Matemáticas de la Universidad de Granada. Son de libre distribución, y están basados unos apuntes de Álgebra Lineal y Geometría del profesor Miguel Sánchez a quien agradezco su trabajo previo.

En estas notas se pueden encontrar los enunciados y demostraciones de los resultados contenidos en el programa de la asignatura, distribuidos por temas tal y como ésta se estructura en la Guía Docente. Algunas veces, las demostraciones están resumidas y dejan que el lector compruebe los detalles como ejercicio. Además de éstos, al final de cada tema hay una relación de ejercicios propuestos.

Como siempre en estos casos, los apuntes no estarán libres de errores, y es labor conjunta del autor y de los lectores mejorarlos, un trabajo que nunca se termina. Si encuentras algún error, por favor envía un e-mail a la dirección de correo electrónico `jperez@ugr.es` Todo lo que se dice en los apuntes puede encontrarse, a menudo explicado con más profundidad, en numerosos textos básicos, como los que aparecen relacionados en la Guía Docente.

Granada, agosto de 2024
Joaquín Pérez Muñoz

Capítulo 0

Preliminares

0.1. Fundamentos de lógica, conjuntos y aplicaciones

0.1.1. Proposiciones verdaderas y falsas; implicaciones

En esta sección veremos el lenguaje básico que es común a todas las áreas de las Matemáticas, por lo que normalmente se verán también en otras asignaturas.

La Lógica, que subyace en los fundamentos de cualquier ciencia, estudia las reglas que permiten hacer razonamientos válidos. Nos restringiremos aquí a algunas ideas y su lenguaje básico.

Un *axioma* es una afirmación que se acepta de entrada, sin demostración. Habitualmente expresa un principio claro y evidente (esto es mucho más discutible de lo que pudiera parecer a primera vista, como pone de manifiesto el famoso quinto postulado de Euclides). Una *proposición* es un enunciado que puede ser verdadero o falso. Dicho enunciado siempre tendrá dos partes: la hipótesis, que consiste en las condiciones que asumimos, y la tesis, que es la afirmación que se hace bajo esas condiciones:

$$\text{Si } p \text{, entonces } q \qquad (p \Rightarrow q).$$

En el ejemplo anterior, p es la tesis y q la hipótesis. Habitualmente usamos el *lenguaje matemático* para simplificar los enunciados, que es como la taquigrafía al lenguaje común. Según la importancia que le demos a ese enunciado en una teoría le asignaremos las categorías *lema, proposición, teorema, corolario*..., pero esto es puramente subjetivo.

Para que una proposición sea cierta, debemos dar una demostración lógica de la misma partiendo de proposiciones previamente demostradas o de axiomas. Si la proposición afecta una propiedad general, su demostración no podrá reducirse a un caso particular.

Partiendo de dos proposiciones p, q, podemos formar otras proposiciones más complejas usando operaciones lógicas; la verdad o falsedad de cada nueva proposición dependerá de la de p y q, así como de la operación lógica. Concretamente:

- Conjunción: $p \wedge q$ (que se lee "p y q").

  Esta proposición es verdadera cuando lo son simultáneamente p y q, y falsa en caso contrario, esto es, cuando es falsa al menos una de las proposiciones p, q.

- Disyunción: $p \vee q$ ("p ó q").

  Esta proposición es verdadera cuando lo es al menos una de los dos proposiciones p, q y falsa en caso contrario, esto es, cuando son falsas tanto p como q.

- Negación $\neg p$ ("no p").

  Este enunciado es verdadero cuando p es falso, y es falso cuando p es verdadero.

Si una proposición es verdadera, entonces su negación es falsa (y viceversa). De hecho, se tiene

$$\neg(\neg p) = p.$$

Si hemos usado la lógica correctamente y los axiomas aceptados no son contradictorios, entonces no puede existir una proposición p tal que tanto p como $\neg p$ sean ciertas (o falsas) simultáneamente. Esto tiene que ver con el llamado *principio de explosión*[1]: si existiera una proposición p tal que p y $\neg p$ son ciertas, entonces cualquier otra proposición q sería cierta también.

A las tres operaciones lógicas anteriores se añade otra que ya habíamos visto:

- Condicional: $p \Rightarrow q$, que se puede leer de varias formas: "si p entonces q", "p implica q", "p es suficiente (o condición suficiente) para q", "q es necesario (o condición necesaria) para p", "q se deduce de p". Cuando se den las dos implicaciones $p \Rightarrow q$ y $q \Rightarrow p$, entonces hablamos de proposiciones *equivalentes,* y se denota $p \Leftrightarrow q$ (y se lee "si y sólo si").

Imaginemos que tenemos dos proposiciones p y q, de las cuales no sabemos si son verdaderas o falsas. Supongamos también que la proposición $p \Rightarrow q$ es verdadera. Entonces podemos deducir tres cosas:

(a) Si p es verdadera, entonces q también lo es. Es decir, se razona *directamente.*

(b) Si q es falsa, entonces p también es falsa. Esto es razonar por *contrarrecíproco.*

(c) De los dos puntos anteriores, de deduce que $p \Rightarrow q$ es verdadera si y sólo si lo es $\neg q \Rightarrow \neg p$.

[1]En terminología clásica, *ex contradictione quodlibet* (o *ex falso quodlibet*): de la contradicción (se sigue) lo que se quiera.

Para probar que una proposición general es falsa, basta dar un *contraejemplo*. Sin embargo, como hemos dicho antes, para probar que una proposición general es verdadera no podemos reducirnos a un caso particular: hay que probarlo en general.

Otro hecho que debemos cuidar es que si tenemos que la proposición $p \Rightarrow q$, entonces no podemos concluir que $q \Rightarrow p$. Un ejemplo evidente de esto: tomemos p como la proposición "llueve" y como q la proposición "la calle está mojada". Está claro que $p \Rightarrow q$, es decir, si llueve la calle se moja. Pero si la calle está mojada, no podemos deducir que sea porque llueve ni porque haya llovido: podría ser por cualquier otra causa. Sin embargo, sí podemos deducir que si la calle está seca entonces no llueve (contrarrecíproco).

A veces denotaremos $p \Leftarrow q$, pero esto no es más que una notación alternativa para $q \Rightarrow p$.

0.1.2. Conjuntos

De manera intuitiva suficiente para nuestros objetivos (aunque lo que sigue tiene más sutilezas, entenderemos por *conjunto* una colección cualquiera de objetos; de cada uno de estos objetos se dirá que es un *elemento* del conjunto.

Si X es un conjunto, de cualquiera de sus elementos diremos que *pertenece* a X, lo cual se denota $x \in X$ (equivalentemente, se dice que X *contiene* a x, y se denota $X \ni x$).

Para definir los conjuntos, implícitamente se ha supuesto una clase de objetos preexistente. Algunos de estos objetos podrían ser conjuntos previamente definidos, pero no se permite que un conjunto sea elemento de sí mismo, pues no estaría entre los objetos preexistentes, ni otras construcciones autorreferentes similares. Lo contrario daría lugar a la conocida *paradoja del barbero*[2] de Bertrand Rusell:

> *Si a los conjuntos se les permitiera contenerse a sí mismos, entonces podríamos construir el conjunto X de todos los conjuntos que no son elementos de sí mismos; se llega entonces a un absurdo al tratar de determinar si X es un elemento de sí mismo o no, porque encontraríamos una proposición verdadera y falsa simultáneamente.*

Un conjunto X está *contenido* en otro Y ($X \subset Y$, X es subconjunto de Y) cuando todo elemento de X también lo es de Y, es decir:

$$\forall x \in X, x \in Y \qquad \text{o, igualmente,} \qquad x \in X \Rightarrow x \in Y.$$

Si $X \subset Y$ e $Y \subset X$, entonces decimos que los conjuntos X, Y son iguales ($X = Y$); esto equivale a:

$$(\forall x \in X, x \in Y) \wedge (\forall y \in Y, y \in X).$$

[2] `https://es.wikipedia.org/wiki/Paradoja_de_Russell`

A veces denotaremos $X \subset Y$ por $X \subseteq Y$. El símbolo $\subsetneq$ denota que se da la inclusión pero no la igualdad (esto es, que la inclusión es *estricta*).

Dados dos conjuntos X, Y, definimos su *intersección* $X \cap Y$ como el conjunto cuyos elementos son los comunes a X y a Y; y su *unión* $X \cup Y$ como el conjunto cuyos elementos son los de X y los de Y. Claramente,

$$X \cap Y \subset X \subset X \cup Y.$$

Los elementos de un conjunto pueden determinarse por *extensión,* es decir, enumerando todos y cada uno de ellos, como

$$X = \{a, b, c\}$$

o por *comprensión,* que consiste en enunciar una propiedad que los caracterice. Para esta modalidad necesitamos el símbolos "tal que", que se denota "\" o también ":". También necesitaremos los *cuantificadores:*

- Cuantificador universal $\forall$, que se lee "para todo". Indica que lo que viene detrás del símbolo se aplicará a todos los elementos de un conjunto dado.

- Cuantificador existencial $\exists$, que se lee "existe" Indica que lo que viene detrás del símbolo se aplica a al menos un elemento de un conjunto dado.

- Cuantificador existencial único, que se escribe $\exists!$ y se lee "existe un único". Indica que lo que viene detrás del símbolo se aplica a exactamente un elemento de un conjunto dado.

Con todo esto, ya podemos dar algunos conjuntos sencillos:

- $\mathbb{N} = \{1, 2, 3, \ldots\}$ es el conjunto de los números naturales. Notemos que 0 no es un número natural.

- $\mathbb{Z} = \{a \mid (a \in \mathbb{N}) \wedge (-a \in \mathbb{N})\} \cup \{0\}$ es el conjunto de los números enteros.

- $\mathbb{Q} = \{a/b \mid a \in \mathbb{Z}, b \in \mathbb{N}\}$ es el conjunto de los números racionales.

- $\mathbb{R} = \{x = \lim_{n\to\infty} x_n \mid \{x_n\}_n\} \in \mathbb{Q}$ es una sucesión convergente$\}$ es el conjunto de los números reales.

- $\mathbb{C} = \{a + b\,i \mid a, b \in \mathbb{R}\}$ es el conjunto de los números complejos (aquí i es la unidad imaginaria, $i = \sqrt{-1}$).

Operaciones entre conjuntos

Todo conjunto X admite dos subconconjuntos a los que llamaremos *impropios*: el propio conjunto X y el conjunto vacío $\varnothing$ (el que no tiene ningún elemento); este último se puede admitir sin incurrir en ninguna contradicción y resulta útil desde el punto de vista lógico para poder definir ciertas operaciones entre subconjuntos. Por ejemplo, el conjunto $X = \{a\}$ sólo tiene como subconjuntos a los impropios. A cualquier subconjunto que no sea impropio de un conjunto X le llamaremos *propio*.

Dado un conjunto X, al conjunto cuyos elementos son todos los subconjuntos de X le llamaremos *conjunto de las partes de* X, y lo denotaremos $\mathcal{P}(X)$. Es decir:

$$A \in \mathcal{P}(X) \;\Leftrightarrow\; A \subset X.$$

Según hemos visto, dados $A, B \in \mathcal{P}(X)$, se tiene que $A \cap B$ y $A \cup B$ son subconjuntos de X, es decir, $A \cap B, A \cup B \in \mathcal{P}(X)$ (la unión y la intersección son *operaciones* en $\mathcal{P}(X)$). Además:

Hay una tercera operación en en $\mathcal{P}(X)$), llamada *diferencia:*

$$A \setminus B = A - B := \{x \in X \mid (x \in A) \wedge (x \notin B)\}.$$

A la diferencia $X \setminus A$ se le llama el *complementario de* A *en* X.

A partir de las definiciones anteriores no es difícil definir la intersección o la unión de una colección finita, o incluso infinita, de subconjuntos de un conjunto X.

Producto cartesiano

Dados dos conjuntos X, Y se define su *producto cartesiano* $X \times Y$ como

$$X \times Y : \{(x, y) : (x \in X) \wedge (y \in Y)\}.$$

A cada elemento $(x, y) \in X \times Y$ se le llama *par ordenado,* y sus componentes son x, y. No es lo mismo (x, y) que (y, x).

A partir de lo anterior, es fácil definir el producto cartesiano de cualquier cantidad finita de conjuntos. A sus elementos ya no se les llama pares ordenados, sino ternas, cuadruplas, quintuplas o, en general, n-uplas, según tengan 3, 4, 5 ó $n \in \mathbb{N}$ elementos, respectivamente. Por ejemplo,

$$\mathbb{R}^n := \mathbb{R} \times \overset{(n)}{\cdots} \times \mathbb{R}.$$

Incluso es posible definir el producto cartesiano de cualquier cantidad infinita de conjuntos, pero eso es más complicado y lo omitiremos por el momento.

Relaciones binarias

Llamaremos *relación binaria* en un conjunto X a cualquier subconjunto $\mathcal{R}$ de $X \times X$. Cuando un par $(x, y) \in X \times X$ pertenezca a X diremos: "x está relacionado con y", y escribiremos $x\mathcal{R}y$.

Las relaciones binarias que nos interesan más son aquellas que cumplen ciertas propiedades, como las siguientes:

- *Reflexiva*: $\forall x \in X$, $x\mathcal{R}x$ (todo elemento está relacionado consigo mismo).
- *Simétrica*: Si $x\mathcal{R}y \Rightarrow y\mathcal{R}x$.
- *Transitiva*: $(x\mathcal{R}y) \wedge (y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.
- *Antisimétrica:* $(x\mathcal{R}y) \wedge (y\mathcal{R}x) \Rightarrow x = y$.

Cuando X es finito, las propiedades anteriores se traducen en ciertas propiedades geométricas de la representación de $\mathcal{R}$ como subconjunto del producto cartesiano $X \times X$.

Dentro de las relaciones binarias, las que más aparecen en Matemáticas son las relaciones de orden y las de equivalencia; las primeras se estudian principalmente en Cálculo (porque aparecen de forma natural al estudiar los números reales), y las segundas aparecen en muchas más situaciones como el Algebra o la Geometría, además del Análisis.

Una relación binaria $\mathcal{R}$ se dice que es *de orden* si verifica las propiedades reflexiva, antisimétrica y transitiva. Si en una relación de orden se verifica además:

$$\forall x, y \in X, \quad (x\mathcal{R}y) \vee (y\mathcal{R}x)$$

la relación se llama *de orden total*.

Relaciones de equivalencia

Definición 0.1.1 Dado un conjunto X y una relación binaria $\mathcal{R} \subset X \times X$, diremos que $\mathcal{R}$ es *de equivalencia* si satisface las propiedades reflexiva, simétrica y transitiva. En este caso, el símbolo $\mathcal{R}$ se suele reemplazar por $\sim$.

Sea $(X, \sim)$ un conjunto dotado con una relación de equivalencia.

Definición 0.1.2 Para cada $x \in X$ se define la *clase de equivalencia* de x mediante

$$C(x) = [x] := \{y \in X : y \sim x\}.$$

(notemos que gracias a la propiedad simétrica, no importa si escribimos $x \sim y$ ó $y \sim x$ en la definición de $[x]$). Llamaremos *conjunto cociente* al conjunto cuyos elementos son las clases de equivalencia:

$$X/_\sim := \{[x] \mid x \in X\}.$$

Cada clase $[x]$ es a la vez un subconjunto de X y un elemento de $X/_\sim$. Además, $X/_\sim$ es un subconjunto de $\mathcal{P}(X)$.

Proposición 0.1.1 *Sea X un conjunto y $\sim$ una relación de equivalencia en X. Entonces, las clases de equivalencia de $(X,\sim)$ verifican las siguientes propiedades:*

1. *$x \in [x]$. En particular, $[x] \neq \varnothing$ y $X = \bigcup_{x\in X}[x]$.*

2. *Si $y \in [x] \ \Rightarrow\ [x] = [y]$. Luego las clases de equivalencia son disjuntas dos a dos.*

Demostración. Por la propiedad reflexiva, $x \sim x$, y por tanto $x \in [x]$. Esto prueba el apartado 1. En cuanto al apartado 2, supongamos que $y \in [x]$. Dado $z \in [y]$ se tiene $z \sim y$. Como $y \sim x$ (por ser $y \in [x]$), entonces la propiedad transitiva implica que $z \sim x$, y por tanto $z \in [x]$. Esto prueba que $[y] \subset [x]$. Recíprocamente, si $w \in [x]$ entonces $w \sim x$. Como $x \sim y$ (porque $y \sim x$ y por la propiedad simétrica), de nuevo por transitividad tenemos $w \sim y$ luego $w \in [y]$ Esto demuestra que $[x] \subset [y]$. Finalmente, de $[y] \subset [x]$, $[x] \subset [y]$ deducimos que $[x] = [y]$. $\square$

A cada elemento y de un clase $[x]$ se le llama *representante de la clase*. El hecho de que si $y \in [x]$ entonces $[y] = [x]$ sugiere que todos los representantes de la clase son “igualmente buenos” a la hora de denotar esa clase.

Definición 0.1.3 Una *partición* P de un conjunto X es una colección de subconjuntos de X que satisfacen las propiedades

1. Cada subconjunto en P es no vacío.

2. La unión de los elementos de P es X.

3. Cada par de elementos de P tiene intersección vacía.

La Proposición 0.1.1 muestra que el conjunto cociente $X/\sim$ es una partición de X. El recíproco a esta propiedad es cierto (Ejercicio 13).

0.1.3. Aplicaciones entre conjuntos

Sean X, Y dos conjuntos. Una *aplicación* f de X a Y es una asociación a cada elemento de X de un único elemento de Y. La aplicación se representa $f\colon X \to Y$, y escribiremos $x \mapsto y$ o bien $f(x) = y$ si y es el único elemento de Y que se asocia a x mediante f. Al conjunto X se le llama *dominio* (o conjunto inicial) de la aplicación, a Y el *codominio* (o conjunto final) y a $f(x)$ *imagen por f de x*. A veces, a la asociación $x \mapsto y = f(x)$ se le llama la *ley* de f.

Por ejemplo, la asociación $x \mapsto \sqrt{x}$ no es una aplicación de $\mathbb{R}$ en $\mathbb{R}$, porque la raíz cuadrada de un número negativo no es un número real. Tampoco $f\colon [0,\infty) \to \mathbb{R}$, $f(x) = \sqrt{x}$ es una aplicación, porque dado $x \in [0,\infty)$, tienen sentido dos raíces cuadradas de x (es decir, dos números reales cuyo cuadrado es x). En cuanto elijamos una determinación para una de estas dos raíces cuadradas (por ejemplo, la no negativa), sí estaremos definiendo una aplicación. Es decir, $f\colon [0,\infty) \to [0,\infty)$, $f(x) = +\sqrt{x}$ sí es una aplicación.

Dejaremos la palabra *función* para el caso en que el codominio de una aplicación sea $\mathbb{R}$ ó $\mathbb{C}$.

Nota 0.1.1 El que para cada $x \in X$ tenga que existir un único $y \in Y$ tal que $f(x) = y$ tiene una lectura especial cuando la aplicación f está definida en un conjunto cociente $X/_\sim$. En este caso, podemos tener $[x] = [y]$ para dos elementos $x, y \in X$ distintos (esto se dará siempre que $x \sim y$). Para que $f\colon X/_\sim \to Y$ sea aplicación debe darse que $f(x) = f(y)$. Esto es lo que se llama que f *está bien definida* (o que no depende del representante):

$$\forall x, y \in X \text{ tales que } x \sim y, \text{ se tiene } f(x) = f(y).$$

Volvamos al caso general. Para que dos aplicaciones coincidan, han de coincidir sus dominios, codominios y leyes. Dos aplicaciones pueden ser distintas incluso si sus dominios y grafos coinciden; por ejemplo:

$$f\colon \mathbb{N} \to \mathbb{N}, \quad f(x) = x^2, \qquad g\colon \mathbb{N} \to \mathbb{R}, \quad g(x) = x^2, \qquad h\colon \mathbb{R} \to \mathbb{R}, \quad h(x) = x^2,$$

son tres aplicaciones distintas.

La aplicación más sencilla es la identidad, $1_X\colon X \to X$, $1_X(x) = x$, $\forall x \in X$.

Otros conjuntos asociados a cada aplicación $f\colon X \to Y$ son su imagen

$$\mathrm{Im}(f) := \{f(x) : x \in X\} = \{y \in Y \,|\, \exists x \in X : y = f(x)\} \subset Y,$$

y su *grafo* (o *gráfica*)

$$\mathrm{Grafo}(f) := \{(x, f(x)) \mid x \in X\} = \{(x,y) \in X \times Y \,|\, y = f(x)\}.$$

Proposición 0.1.2 *Sea $f\colon X \to Y$ una aplicación. Entonces, su grafo cumple*

$$\forall x \in X, \ \exists!\, y \in Y \mid (x,y) \in \mathrm{Grafo}(f).$$

Recíprocamente, si C es un subconjunto de $X \times Y$ tal que $\forall x \in X$, $\exists!\, y \in Y$ tal que $(x,y) \in C$, entonces existe una única aplicación $f\colon X \to Y$ cuyo grafo es C.

Demostración. Sea $x \in X$. Su imagen $f(x) \in Y$ cumple que $(x, f(x)) \in \mathrm{Grafo}(f)$, y si $y \in Y$ cumple $(x,y) \in \mathrm{Grafo}(f)$ entonces $y = f(x)$ por definición de aplicación.

Recíprocamente, supongamos que C es un subconjunto de $X \times Y$ tal que $\forall x \in X$, $\exists!\, y \in Y$ siendo $(x,y) \in C$. Definimos una aplicación $f\colon X \to Y$ mediante $x \mapsto f(x) :=$ el único $y \in Y$ tal que $(x,y) \in C$. La unicidad de f es obvia. $\square$

Definición 0.1.4 Dada una aplicación $f\colon X \to Y$ y un subconjunto $A \subset X$, se define la *restricción de f a A* mediante

$$f|_A\colon A \to Y, \qquad x \mapsto (f|_A)(x) = f(x).$$

Es decir, la ley de $f|_A$ asigna a cada elemento x de A su imagen por f. La diferencia entre f y $f|_A$ es que $f|_A$ aplica la ley de f sólo a los elementos de A.

La restricción de la identidad 1_X a un subconjunto $A \subset X$ se llama la *inclusión de A en X*:

$$i_A\colon A \to X, \quad i_A(x) = x.$$

Tambien podemos restringir una aplicación $f\colon X \to Y$ por la derecha: si $B \subset Y$ cumple $\mathrm{Im}(f) \subset B$, entonces podemos restringir f a $f|^B\colon X \to B$, $(f|^B)(x) = f(x)$, $\forall x \in X$.

Definición 0.1.5 Dada una aplicación $f\colon X \to Y$, se definen la *imagen directa*

$$f_*\colon \mathcal{P}(X) \to \mathcal{P}(Y), \qquad A \mapsto f_*(A) := \{f(x) : x \in A\}$$

y la *imagen inversa* (o recíproca)

$$f^*\colon \mathcal{P}(Y) \to \mathcal{P}(X), \qquad B \mapsto f^*(B) := \{x \in X : f(x) \in B\}.$$

En ocasiones se abusa de la notación escribiendo $f(A)$ en lugar de $f_*(A)$, y $f^{-1}(B)$ en lugar de $f^*(B)$. Esto no es formalmente correcto, y además puede llevar a confusión con el concepto de *aplicación inversa,* que veremos después (y qe no siempre existe para una aplicación $f\colon X \to Y$). Por tanto, intentaremos no hacer este abuso de notación, al menos mientras no tengamos la suficiente práctica como para entender inequívocamente lo que se está haciendo.

De la definición se deducen

1. $f_*(A) \subset Y$, por lo que $f_*(A) \in \mathcal{P}(Y)$.
2. $f^*(B) \subset X$, por lo que $f^*(B) \in \mathcal{P}(X)$.
3. $f_*(X) =\mathrm{Im}(f)$, $f^*(Y) = X$,
4. Si $B \subset Y$ cumple $B \cap \mathrm{Im}(f) = \varnothing$, entonces $f^*(B) = \varnothing$.

Definición 0.1.6 Sean $f\colon X \to Y$, $g\colon Y \to Z$ dos aplicaciones, en la que el codominio de f coincide con el dominio de g. Se define su *composición* $g \circ f\colon X \to Z$ mediante

$$(g \circ f)(x) := g(f(x)), \quad \forall x \in X.$$

Observemos que $g \circ f$ puede definirse también en el caso $f\colon X \to Y$, $g\colon Y' \to Z$ siempre que $\mathrm{Im}(f) \subset Y'$.

Proposición 0.1.3 *Se consideran tres aplicaciones $f\colon X \to Y$, $g\colon Y \to Z$, $h\colon Z \to W$. Entonces,*

$$(h \circ g) \circ f = h \circ (g \circ f). \tag{1}$$

Demostración. Claramente, ambos miembros de la igualdad están bien definidos como aplicaciones y tienen igual dominio y codominio. Queda ver que las leyes coinciden; dado $x \in X$,

$$[(h \circ g) \circ f](x) = (h \circ g)(f(x)) = h(g(f(x))) = h((g \circ f)(x)) = [h \circ (g \circ f)](x).$$

$\square$

La proposicion 0.1.3 nos dice que la composición de aplicaciones es *asociativa*; en particular, podemos usar la notación $h \circ g \circ f$. Pero la composición no es, en general, conmutativa.

Definición 0.1.7 Sea $f\colon X \to Y$ una aplicación.

- f es *inyectiva* si elementos distintos de X tienen imágenes distintas en Y:

  $$\text{Si } x, x' \in X \text{ cumplen } x \neq x', \text{ entonces } f(x) \neq f(x').$$

  Equivalentemente, cuando $f(x) = f(x') \Rightarrow x = x'$.

- f es *sobreyectiva* (suprayectiva) si todo elemento de Y es imagen de alguno de X:

  $$\forall y \in Y,\ \exists x \in X \text{ tal que } f(x) = y.$$

  (equivalentemente, si $\mathrm{Im}(f) = Y$).

- f es *biyectiva* si es inyectiva y sobreyectiva:

  $$\forall y \in Y,\ \exists! x \in X \text{ tal que } f(x) = y.$$

Una aplicación f no ha de ser inyectiva, ni sobreyectiva, ni biyectiva.

Definición 0.1.8 Cuando $f\colon X \to Y$ sea una aplicación biyectiva, tiene sentido definir la aplicación *inversa* de f:

$$f^{-1}\colon Y \to X, \quad f^{-1}(y) := \text{ el único } x \in X \text{ tal que } f(x) = y.$$

Por ejemplo, la inclusión i_A de un subconjunto $A \subset X$ en X es inyectiva, y la identidad 1_X es biyectiva (su inversa es 1_X). La proyección canónica $\pi\colon X \to X/_\sim$ sobre un conjunto cociente, definida como $\pi(x) := [x]\ \forall x \in X$, es sobreyectiva.

Es fácil comprobar que si $f\colon X \to Y$ es biyectiva, entonces $f^{-1} \circ f = 1_X$ y $f \circ f^{-1} = 1_Y$. Veremos más adelante que el recíproco es cierto.

Proposición 0.1.4 *La composición de dos aplicaciones inyectivas (resp. sobreyectivas, biyectivas) es inyectiva (resp. sobreyectiva, biyectiva).*

Demostración. Ejercicio. □

Lema 0.1.1 *Sean $f\colon X \to Y$, $g\colon Y \to Z$ dos aplicaciones.*

- *Si $g \circ f$ es inyectiva, entonces f es inyectiva.*
- *Si $g \circ f$ es sobreyectiva, entonces g es sobreyectiva.*
- *Si $g \circ f$ es biyectiva, entonces f es inyectiva y g es sobreyectiva.*

Demostración. Para la primera afirmación, si f no fuera inyectiva existirían $x, x' \in X$ tales que $x \neq x'$ y $f(x) = f(x')$. Por tanto, $(g \circ f)(x) = g(f(x)) = g(f(x')) = (g \circ f)(x')$, de donde deducimos que $g \circ f$ no es inyectiva.

Para la segunda, sea $z \in Z$. Como $g \circ f$ es sobreyectiva, existe $x \in X$ tal que $z = (g \circ f)(x) = g(f(x))$. Por tanto, z es la imagen por g de $f(x) \in Y$, luego g es sobreyectiva.

La tercera afirmación es consecuencia directa de la primera y la segunda. □

Proposición 0.1.5 *Sean $f\colon X \to Y$, $g\colon Y \to X$ dos aplicaciones tales que $g \circ f = 1_X$ y $f \circ g = 1_Y$. Entonces, f, g son biyectivas y $g = f^{-1}$.*

Demostración. Aplicando el Lema 0.1.1 a $g \circ f = 1_X$ se obtiene la inyectivdad de f y la sobreyectividad de g. Aplicándolo a $f \circ g = 1_Y$. se deduce la inyectividad de g y la sobreyectividad de f. Por tanto, ambas aplicaciones son biyectivas.

Claramente, g y f^{-1} tienen igual dominio y codominio. Sea $y \in Y$ y $x = f^{-1}(y)$, esto es, $f(x) = y$. Entonces,

$$g(y) = g(f(x)) = (g \circ f)(x) = 1_X(x) = x = f^{-1}(y),$$

por lo que g y f^{-1} coinciden. □

Decíamos arriba que aplicación arbitraria no tiene por qué ser inyectiva ni sobreyectiva. No obstante, toda aplicación se puede escribir como composición de una aplicación inyectiva, una biyectiva y otra sobreyectiva:

Teorema 0.1.1 (Descomposición canónica de una aplicación) *Sea $f\colon X \to Y$ una aplicación.*

1. *Se define la relación binaria en X: Dados $x, x' \in X$, diremos que $x \sim x'$ cuando $f(x) = f(x')$. Entonces, $\sim$ es una relación de equivalencia. Consideremos la proyección canónica $\pi\colon X \to X/_\sim$, que es sobreyectiva.*

2. *Definimos*
$$b\colon X/_\sim \to \mathrm{Im}(f), \quad b([x]) := f(x), \quad \forall x \in X.$$
Entonces, b es una aplicación bien definida (en el sentido de la Nota 0.1.1) y es biyectiva.

3. *Consideremos la inclusión $i = i_{Im(f)}\colon Im(f) \to Y$, que es inyectiva.*

Entonces, se cumple $f = i \circ b \circ \pi$.

Demostración. Que $\sim$ es una relación de equivalencia es trivial, (se cumplen las propiedades reflexiva, simétrica y transitiva), con lo que 1 está probado.

Para ver que b está bien definida, supongamos que $[x] = [y]$ para dos elementos $x, y \in X$. Entonces, $x \sim y$ luego $f(x) = f(y)$. Esto nos dice que $b([x]) = b([y])$ luego b está bien definida.

Veamos que b es inyectiva: si $b([x]) = b([y])$ entonces por definición de b tenemos $f(x) = f(y)$, luego por definición de $\sim$, se tiene $x \sim y$ y por tanto $[x] = [y]$.

Veamos que b es sobreyectiva: dado $z \in \mathrm{Im}(f)$, por definición de imagen de una aplicación existe $x \in X$ tal que $z = f(x)$. Por tanto, $b([x]) = z$, esto es, $z \in \mathrm{Im}(b)$. Esto termina de probar el apartado 2.

Por último, para el apartado 3 notemos que tanto f como $i \circ b \circ \pi$ tienen igual dominio y codominio. Por tanto, su igualdad se deducirá de

$$(i \circ b \circ \pi)(x) = i(b(\pi(x))) = i(b([x]) = i(f(x)) = f(x), \quad \forall x \in X.$$

□

Nota 0.1.2 Sea $f\colon X \to Y$ una aplicación. Con la notación de la descomposición canónica, tenemos que f es inyectiva si y sólo si π lo es, y que f es sobreyectiva si y sólo si i lo es.

0.2. Estructuras algebraicas

Aunque los conceptos de grupo, anillo y cuerpo se verán en más detalle en otras asignaturas, daremos aquí los fundamentos necesarios para lo que necesitaremos más adelante al hablar del grupo lineal general, el grupo ortogonal, el anillo de endomorfismos o de matrices cuadradas, etc. También es necesaria la estructura de cuerpo para hablar del cuerpo base de un espacio vectorial, pero en la práctica sólo desarrollaremos estos últimos cuando el cuerpo base son los números reales y los complejos, cuyas propiedades básicas se suponen conocidas de la enseñanza secundaria.

0.2.1. Grupos

Definición 0.2.1 Una *ley de composición interna* en un conjunto G es una aplicación $\cdot\colon G \times G \to G$. Usaremos la notación $x \cdot y := \cdot(x, y)$, pero no debemos pensar que $\cdot$ es un producto sino una operación abstracta (también usaremos los símbolos $\star, +$ con la misma idea).

Algunas posibles propiedades que puede cumplir una ley de composición interna $\cdot$ son:

1. *Asociativa*: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, $\forall x, y, z \in G$.
2. *Elemento neutro*: $\exists e \in G$ tal que $e \cdot x = x \cdot e = x$, $\forall x \in G$.

   El elemento neutro, si existe, es único (si $e, e' \in G$ son dos elementos neutros, entonces $e = e \cdot e' = e'$).
3. *Elemento simétrico*: Supongamos que existe el elemento neutro $e \in G$. Dado $x \in G$, $\exists \overline{x} \in G$ tal que $x \cdot \overline{x} = \overline{x} \cdot x = e$.

   En el caso de usar notación aditiva (resp. multiplicativa), al elemento simétrico se le llama *opuesto* y se le denota por $-x$ (resp. inverso, x^{-1}).
4. *Conmutativa*: $x \cdot y = y \cdot x$, $\forall x, y \in G$.

Definición 0.2.2 Un grupo es un par $(G, \cdot)$ formado por un conjunto G y una ley de composición interna $\cdot$ en G que verifica las propiedades asociativa, existencia de elemento neutro y de elemento simétrico. Si además verifica la propiedad conmutativa, el grupo se dice *conmutativo* o *abeliano*.

Proposición 0.2.1 *Sea $(G, \cdot)$ un grupo. Entonces:*

1. *(Leyes de simplificación) si $x, y, y' \in G$ y $x \cdot y = x \cdot y'$ o bien $y \cdot x = y' \cdot x \;\Rightarrow\; y = y'$.*
2. *El simétrico $\overline{x}$ de cada $x \in G$ es único.*

3. *Si $x, y \in G$ cumplen $x \cdot y = e$ entonces cada uno es el simétrico del otro.*

Demostración. Supongamos que $x \cdot y = x \cdot y'$. Operando ambos miembros por el simétrico $\overline{x}$ de x por la izquierda, tenemos $\overline{x} \cdot (x \cdot y) = \overline{x} \cdot (x \cdot y')$. Usando la propiedad asociativa, lo reescribimos como $(\overline{x} \cdot x) \cdot y = (\overline{x} \cdot x) \cdot y'$. Usando la propiedad del elemento simétrico, $e \cdot y = e \cdot y'$, y por último usando la propiedad del elemento neutro deducimos que $y = y'$. El argumento para probar que $y \cdot x = y' \cdot x \;\Rightarrow\; y = y'$ es análogo.

Para probar la unicidad del elemento simétrico, supongamos que $\overline{x}, x' \in G$ son simétricos de $x \in G$. Entonces, $\overline{x} = \overline{x} \cdot e = \overline{x} \cdot (x \cdot x') = (\overline{x} \cdot x) \cdot x' = e \cdot x' = x'$.

Por último, supongamos que $x \cdot y = e$. Entonces, $x \cdot y = e = x \cdot \overline{x}$, y aplicando el apartado 1, tenemos $y = \overline{x}$. □

Listamos a continuación algunos ejemplos de grupos:

- $(\mathbb{R}, +)$, abeliano. El neutro es $e = 0$, y el simétrico de cada $x \in \mathbb{R}$ es $-x$ (*opuesto* de x). Sin embargo, $(\mathbb{R}, \cdot)$ (producto de números reales) no es un grupo, ya que $0 \in \mathbb{R}$ no tiene simétrico.
- $(\mathbb{R} \setminus \{0\}, \cdot)$ (producto usual), abeliano. El neutro es $e = 1$, y el simétrico de cada $x \in \mathbb{R} \setminus \{0\}$ es $x^{-1} = 1/x$ (*inverso* de x).
- Sea $X \neq \varnothing$ un conjunto. Definimos

  $$S(X) = \{f : X \to X \mid f \text{ es biyectiva}\}.$$

  Por la Proposición 0.1.4, la composición $\circ$ es una ley de composición interna en $S(X)$. Es fácil comprobar que $(S(X), \circ)$ es un grupo cuyo elemento neutro es la aplicación identidad 1_X, y tal que el elemento simétrico de una biyección $f \in S(X)$ es su aplicación inversa f^{-1}. Salvo que el número de elementos de X sea 1 ó 2, $(S(X), \circ)$ no es abeliano.

Definición 0.2.3 Un *homomorfismo de grupos* es una aplicación $f : (G, \cdot) \to (G', \star)$ entre dos grupos que cumple $f(x \cdot y) = f(x) \star f(y)$, $\forall x, y \in G$.

Cuando f sea un homomorfismo de grupos inyectivo (resp. sobreyectivo, biyectivo), le llamaremos un *monomorfismo* (resp. *epimorfismo, isomorfismo*) de grupos.

0.2.2. Anillos

Definición 0.2.4 Un *anillo* es una terna $(A, +, \cdot)$ donde A es un conjunto no vacío, y $+, \cdot$ son dos leyes de composición interna en A que cumplen:

1. $(A, +)$ es un grupo abeliano. Denotaremos por $0 \in A$ al elemento neutro de esta estructura.

2. $(A, \cdot)$ verifica la propiedad asociativa.

3. *Propiedad distributiva:*

$$x \cdot (y+z) = x \cdot y + x \cdot z, \qquad (y+z) \cdot x = y \cdot x + z \cdot x, \qquad \forall x, y, z \in A.$$

Si además

- $(A, \cdot)$ tiene elemento neutro, llamaremos a $(A, +, \cdot)$ un *anillo unitario;* denotaremos por $1 \in A$ a este elemento neutro.

- $(A, \cdot)$ cumple la propiedad conmutativa, diremos que $(A, +, \cdot)$ es un anillo conmutativo (no se dice abeliano).

Nota 0.2.1 Tanto 0 como 1 son simplemente formas de denotar elementos abstractos en A; en particular, nada impide que pueda ser $1 = 0$, pero en este caso, se prueba fácilmente que $A = \{0\}$, que es el *anillo trivial.* Un *anillo unitario no trivial* es un anillo unitario en el que $1 \neq 0$.

Lema 0.2.1 *Sea $(A, +, \cdot)$ un anillo. Entonces,*

1. $\forall x \in A$, $0 \cdot x = x \cdot 0 = 0$.

2. Si $(A, +, \cdot)$ es unitario, entonces $(-1) \cdot x = -x$ y $(-1) \cdot (-x) = x$.

Demostración. Dado $x \in A$, $0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$, Simplificando tenemos $0 \cdot x = 0$.

Para la propiedad 2, supongamos que $(A, +, \cdot)$ es unitario y sea $x \in A$. Entonces, $x + (-1) \cdot x = 1 \cdot x + (-1) \cdot x = (1 + (-1)) \cdot x = 0 \cdot x = 0$, de donde $(-1) \cdot x = -x$. Aplicando esta igualdad a $-x$ tenemos $(-1) \cdot (-x) = -(-x) = x$. $\square$

Veamos algunos ejemplos de anillos:

- $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo unitario (no trivial); lo mismo le pasa a $(\mathbb{R}, +, \cdot)$ y a $(\mathbb{C}, +, \cdot)$.

- Sea $p \in \mathbb{N}$. El conjunto de los múltiplos de p,

$$p\mathbb{Z} := \{0, p, -p, 2p, -2p, ...\} = \{kp \mid k \in \mathbb{Z}\},$$

  es un anillo con la suma y producto restringidos de $\mathbb{Z}$. Para $p = 1$, tenemos $p\mathbb{Z} = \mathbb{Z}$ (unitario) pero si $p \neq 1$, $p\mathbb{Z}$ no es unitario.

- En $\mathbb{Z}$ se define la relación binaria *módulo* p: dados $x, y \in \mathbb{Z}$, diremos que $x \sim y$ (esto se escribe $x \equiv y \pmod{p}$) si $x - y \in p\mathbb{Z}$. Es fácil probar que $\sim$ es una relación de equivalencia en $\mathbb{Z}$, y por tanto define unas clases de equivalencia $[x]$, $x \in \mathbb{Z}$ y un conjunto cociente
$$\mathbb{Z}/p\mathbb{Z} = \{[x] \mid x \in \mathbb{Z}\} = \{[0], [1], \ldots, [p-1]\}.$$
Notemos que $[x]$ es el conjunto de los número enteros que producen el mismo resto al dividir por p que el resto producido por x. $\mathbb{Z}/pZ$ tiene una estructura natural de anillo unitario conmutativo, con las operaciones:
$$[x] + [y] := [x + y], \quad [x] \cdot [y] := [x \cdot y], \qquad \forall [x], [y] \in \mathbb{Z}/p\mathbb{Z}. \tag{2}$$
(que están definidas por el ejercicio 24).
- El conjunto $\mathcal{M}_n(\mathbb{R})$ de matrices cuadradas reales de orden $n \in \mathbb{N}$, con la suma y el producto habitual de matrices, es un anillo (en general, no conmutativo). Estudiaremos este ejemplo en más profundidad más adelante.

Sabemos que no toda matriz cuadrada tiene inversa. Así que no todos los elementos en $\mathcal{M}_n(\mathbb{R}) \setminus \{0\}$ son invertibles en el sentido de la siguiente proposición, pero aún así los elementos invertibles forman un grupo:

Proposición 0.2.2 *Sea* $(A, +, \cdot)$ *un anillo unitario no trivial. Definimos*
$$\mathrm{Inv}(A) = \{z \in A \mid \exists z^{-1} \in A \text{ tal que } z \cdot z^{-1} = z^{-1} \cdot z = 1\}.$$
Entonces, $(\mathrm{Inv}(A), \cdot)$ *es un grupo. En particular, el inverso de cada* $x \in \mathrm{Inv}(A)$ *es único.*

Demostración. Primero veamos que la restricción de $\cdot$ a $\mathrm{Inv}(A)$ es una ley de composición interna en $\mathrm{Inv}(A)$: dados $x, y \in \mathrm{Inv}(A)$, tenemos $x \cdot y \cdot (y^{-1} \cdot x^{-1}) = x \cdot (y \cdot y^{-1}) \cdot x^{-1} = x \cdot 1 \cdot x^{-1} = x \cdot x^{-1} = 1$, luego $x \cdot y \in \mathrm{Inv}(A)$ y
$$(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}.$$
La propiedad asociativa de $\cdot$ se cumple en $\mathrm{Inv}(A)$ porque se cumplía en A. La existencia de elemento neutro para $\cdot$ es trivial (este neutro es $1 \in \mathrm{Inv}(A)$), y la existencia de elemento simétrico se deduce de la definición de $\mathrm{Inv}(A)$. $\square$

Definición 0.2.5 Un *homomorfismo de anillos* es una aplicación $f\colon (A, +, \cdot) \to (A', +, \cdot)$ entre dos anillos que cumple $f(x + y) = f(x)'f(y)$, $f(x \cdot y) = f(x) \star f(y)$, $\forall x, y \in G$.

Cuando f sea un homomorfismo de anillos inyectivo (resp. sobreyectivo, biyectivo), le llamaremos un *monomorfismo* (resp. *epimorfismo, isomorfismo*) de anillos.

0.2.3. Cuerpos

Definición 0.2.6 Un *cuerpo* $(\mathbb{K}, +, \cdot)$ es un anillo unitario no trivial tal que $\mathrm{Inv}(\mathbb{K}) = \mathbb{K} \setminus \{0\}$. El cuerpo $(\mathbb{K}, +, \cdot)$ se dice *conmutativo* si el producto $\cdot$ verifica la propiedad conmutativa.

Algunos ejemplos de cuerpos son los siguientes:

- $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ son cuerpos conmutativos. $(\mathbb{Z}, +, \cdot)$ no es un cuerpo.
- Si p es primo, $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ es un cuerpo. Este es el primer ejemplo de cuerpo finito[3].
- **El cuerpo $\mathbb{C}$ de los números complejos**. Se supone que el lector ya conoce las propiedades fundamentales de $\mathbb{C}$. Las recopilamos aquí porque se usarán más adelante.

  Al igual que los números reales se definen como una extensión de los racionales para por ejemplo, poder hablar de soluciones de ecuaciones como $x^2 = 2$, los números complejos se definieron a partir de los reales para dotar de sentido a soluciones de ecuaciones del tipo $x^2 = -1$. Para ello, se introduce la *unidad imaginaria* i como solución abstracta de $x^2 = -1$, y se define

  $$\mathbb{C} = \{z = a + b\,i \mid a, b \in \mathbb{R}\}.$$

  Con la notación anterior, $a = \Re(z)$, $b = \Im(z)$ son la *parte real* y *parte imaginaria* del número complejo z. En particular, $\mathbb{R} \subset \mathbb{C}$.

  Las operaciones $+, \cdot$ se extienden de forma natural de $\mathbb{R}$ a $\mathbb{C}$:

  $$\begin{array}{rcl} (a + b\,i) + (a' + b'\,i) & := & (a + a') + (b + b')\,i \\ (a + b\,i) \cdot (a' + b'\,i) & := & (a \cdot a' - b \cdot b') + (a \cdot b' + b \cdot a')\,i. \end{array} \tag{3}$$

  y producen una estructura de cuerpo conmutativo en $(\mathbb{C}, +, \cdot)$. El inverso de $z = a + ib \in \mathbb{C} \setminus \{0\}$ es

  $$z^{-1} = \frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2}.$$

  Dado un complejo $z = a + b\,i$, su *conjugado* es $\overline{z} := a - b\,i$ y su *módulo* es

  $$|z| := \sqrt{a^2 + b^2} \; (= \sqrt{z \cdot \overline{z}}).$$

[3] Estos cuerpos finitos están relacionados con el concepto de *característica* de un cuerpo. En general, la *característica* de un cuerpo $\mathbb{K}$ es el menor natural p tal que al sumar p veces la unidad 1 consigo misma se obtiene 0: $1 + \overset{p)}{\ldots} + 1 = 0$; en caso de que esto no ocurra para ningún $p \in \mathbb{N}$ diremos que la característica de $\mathbb{K}$ es 0. Para p primo, los cuerpos $\mathbb{Z}/p\mathbb{Z}$ tienen característica p, mientras que los cuerpos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, con los que trabajaremos usualmente, tienen característica 0.

De esta forma, el módulo de un número complejo generaliza el valor absoluto en $\mathbb{R}$. En particular, $|z \cdot w| = |z| \cdot |w|$, $\forall z, w \in \mathbb{C}$. Además,

$$z^{-1} = \frac{1}{z} = \frac{\overline{z}}{z\overline{z}} = \frac{\overline{z}}{|z|^2}.$$

Es usual identificar $\mathbb{C}$ con $\mathbb{R}^2$, mediante la biyección

$$\mathbb{C} \to \mathbb{R}^2, \qquad a + b\,i \mapsto (a, b).$$

Esto permite hacer una definición formal de $\mathbb{C}$ sin basarnos en la unidad imaginaria i: simplemente se trasladan las operaciones de (3) a $\mathbb{R}^2$ y se comprueba que definen sobre $(\mathbb{R}^2, +, \cdot)$ una estructura de cuerpo conmutativo[4], y se define el cuerpo $\mathbb{C}$ como $(\mathbb{R}^2, +, \cdot)$ donde identificamos $z = a + b\,i$ con (a, b). En particular, la *unidad imaginaria* será $i := (0, 1)$. Esta biyección permite visualizar los números complejos como puntos de un plano.

Dado $z \in \mathbb{C} \setminus \{0\}$ con módulo $r = |z| > 0$, el número complejo z/r tiene módulo 1, es decir, cae en la circunferencia unidad de $\mathbb{R}^2 \equiv \mathbb{C}$. Por tanto existe un único $\theta \in [0, 2\pi)$ tal que $z/r = \cos\theta + i \operatorname{sen}\theta$, lo que produce la *representación polar* de z:

$$z = r(\cos\theta + i \operatorname{sen}\theta). \tag{4}$$

A θ se le llama el *argumento* de z. Dado un segundo número complejo expresado en forma polar $z' = r'(\cos\theta' + i \operatorname{sen}\theta')$, al multiplicar $z \cdot z'$, desarrollar los sumandos por dstributiva y aplicar las fórmulas del seno y coseno de la suma de dos ángulos, se deduce que el módulo del producto es el producto de módulos y el argumento del producto es la suma de los argumentos. Esto nos dice que $z^{-1} = r^{-1}(\cos(-\theta) + i \operatorname{sen}(-\theta))$.

Geométricamente:

- $\mathbb{R}$ puede verse dentro de $\mathbb{C}$ como el eje de abscisas dentro de $\mathbb{R}^2$ (por eso se llama *eje real* al eje de abscisas, y *eje imaginario* al eje de ordenadas).
- Multiplicar por i un complejo $z = a + b\,i$ equivale a rotar en $\mathbb{R}^2$ el punto (a, b) alrededor del origen un ángulo de $\pi/2$ radianes (90 grados) en el sentido opuesto al movimiento de las agujas del reloj.
- El complejo conjugado de $z \in \mathbb{Z}$ equivale al simétrico de z con respecto al eje de abscisas.
- El argumento de $z \in \mathbb{C} \setminus \{0\}$ se calcula como el ángulo del vector de posición de z con la dirección positiva del eje de abscisas, y el módulo es la distancia de z al origen.

[4]El producto componente a componente en $\mathbb{R}^2$ no define una estructura de cuerpo en $\mathbb{R}^2$.

Usando la *fórmula de Euler*[5],

$$e^{i\theta} = \cos\theta + i \operatorname{sen}\theta,$$

la ecuación (4) se simplifica

$$z = r\, e^{i\theta},$$

y dado $z' = r'\, e^{i\theta'}$, tenemos $z \cdot z' = (r \cdot r')\, e^{i(\theta+\theta')}$.

[5] Esta fórmula puede deducirse del desarrollo en serie de potencias de la exponencial, $e^w = \sum_{n=0}^{\infty} w^n/n!$, comparándolo con los desarrollos de las funciones seno y coseno.

0.3. Ejercicios.

1. Discutir si las siguientes afirmaciones son proposiciones y, en caso afirmativo, cuál es su negación en el lenguaje cotidiano:

   (a) Puede que llueva mañana.

   (b) Esta frase tiene cinco palabras.

2. **(Principio de inducción)** Este principio es muy útil para probar propiedades que dependan de índices en $\mathbb{N}$. Sea basa en la siguiente propiedad:

   > "Sea $A \subset \mathbb{N}$ tal que
   > - $1 \in A$.
   > - Si $n \in A$, entonces $n+1 \in A$.
   >
   > Entonces, $A = \mathbb{N}$".

   Usar el principio de inducción para demostrar que $\forall n \in \mathbb{N}$,

   a) $\displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

   b) Dados $a, b \in \mathbb{R}$, $(a+b)^n = \displaystyle\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$.

3. Dado $n \in \mathbb{N}$, se define el conjunto $X_n = \{1, 2, \ldots, n\}$.

   (a) Construir $\mathcal{P}(X_n)$ explícitamente para $n = 1, 2, 3$. ¿Cuántos elementos tiene?

   (b) ¿Cuántos elementos tiene $\mathcal{P}(X_n)$ para cualquier valor de n?

   (c) Construir $\mathcal{P}(\mathcal{P}(X_2))$.

4. Sean A, B subconjuntos de un conjunto X. Representar los conjuntos $A \cup B$, $A \cap B$, $A \setminus B$ usando diagramas de Venn.

5. Explica la diferencia existente entre los objetos que aparecen en cada caso:

   (a) x, $\{x\}$, (x, x).

   (b) $\{x, y\}$, $\{y, x\}$.

   (c) (x, y), (y, x).

6. Si X e Y son conjuntos finitos con n y m respectivamente, ¿cuántos elementos tiene $X \times Y$?

7. Dar ejemplos de dos relaciones binarias en un conjunto X que sean a la vez simétricas y antisimétricas, una de ellas que verifique además la propiedad reflexiva, y la otra que no la verifique.

8. ¿Dónde está el fallo en el siguiente razonamiento? Sea $X \neq \varnothing$ y $R \subset X \times X$ una relación binaria simétrica y transitiva. Si xRy, entonces yRx por ser R simétrica. Como xRy e yRx, por ser R transitiva se tiene xRx. Por tanto, R es reflexiva.

9. Comprobar que las siguientes relaciones binarias son relaciones de orden:

   (a) En $\mathbb{R}$, la relación "ser menor o igual a" (esto es, $\mathcal{R}$ es la relación $\leq$).

   (b) En el conjunto $\mathcal{P}(X)$ de las partes de un conjunto X, la relación 'estar incluido en" (esto es, $\mathcal{R}$ es la relación $\subset$). Además, probar que

   - $A \cap B$ es el mayor subconjunto de X que está contenido a la vez en A y B.
   - $A \cup B$ es el menor subconjunto de X que contiene a la vez a A y B.

   (c) ¿Es alguna de estas dos relaciones de orden total?

10. Se considera en $X = \{1, 2, 3, 4, 5, 6\}$ la relación binaria $\mathcal{R} = \{(1, 1), (1, 2), (3, 5), (6, 5)\}$. Completar $\mathcal{R}$ hasta una relación de equivalencia, es decir, hallar la única relación binaria $\mathcal{R}'$ que verifica las siguientes propiedades: (a) $\mathcal{R} \subset \mathcal{R}'$, (b) $\mathcal{R}'$ es de equivalencia, y (c) si $\mathcal{R}''$ es otra relación binaria que verifica (a) y (b), entonces $\mathcal{R}' \subset \mathcal{R}''$.

11. Discutir si, dado un conjunto arbitrario X y una relación binaria $\mathcal{R}$ cualquiera en X, existe una relación binaria $\mathcal{R}'$ que complete $\mathcal{R}$ hasta una relación de equivalencia.

12. Se considera en $\mathbb{R}^3$ la relación de equivalencia "estar a la misma distancia del origen". Determinar el conjunto cociente.

13. Sea P una partición de un conjunto X. Se considera la siguiente relación binaria $\mathcal{R}$ en X: Dados $x, y \in X$ diremos que $x\mathcal{R}y$ si x, y pertenecen al mismo elemento de P. Demostrar que $\mathcal{R}$ es una relación de equivalencia y que su conjunto cociente coincide con P.

14. ¿Cuáles de los siguientes conjuntos son grafos de aplicaciones $f \colon \mathbb{R} \to \mathbb{R}$?

   (a) $G_1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 16\}$.

   (b) $G_2 = \{(x, y) \in \mathbb{R}^2 \mid x = y^2\}$.

   (c) $G_3 = \{(x, y) \in \mathbb{R}^2 \mid x^2 = y\}$.

   (d) $G_4 = \{(x, y) \in \mathbb{R}^2 \mid x + y = 0\}$.

15. Sean $f, g \colon \mathbb{R} \to \mathbb{R}$ las aplicaciones definidas por
$$f(x) = x^2 + 1, \qquad g(x) = e^x, \qquad \forall x \in \mathbb{R}.$$
Calcular $g \circ f$ y $f \circ g$.

16. Sean $f \colon X \to Y$ y $g \colon X' \to Y'$ dos aplicaciones. Supongamos que se puede definir $g \circ f$. ¿Cuándo se puede definir también $f \circ g$?

17. Sea $f \colon D \to \mathbb{R}$ cada una de las siguientes cuatro funciones elementales: $x \mapsto x^2, e^x, \sqrt{x}$, $\ln x$, siendo en cada caso $D \subset \mathbb{R}$ su dominio natural. Determinar cuáles de estas aplicaciones son inyectivas, sobreyectivas o biyectivas. ¿Es alguna de estas aplicaciones la inversa de otra?

18. Sea $f \colon X \to X$ una aplicación. Probar que
    (a) f es inyectiva si y solo si $\forall g, h \colon X \to X$ tales que $f \circ g = f \circ h$, se tiene $g = h$.
    (b) f es sobreyectiva si y solo si $\forall g, h \colon X \to X$ tales que $g \circ f = h \circ f$, se tiene $g = h$.

19. Sea X, Y conjuntos no vacíos, y $\sim, \sim'$ relaciones de equivalencia en X, Y respectivamente. Una aplicación $f \colon X \to Y$ se dice *compatible con* $\sim, \sim'$ si cumple:
$$\text{Si } x, x' \in X \text{ cumplen } x \sim x', \text{ entonces } f(x) \sim' f(x')$$
Demostrar que si una aplicación $f \colon X \to Y$ es compatible con $\sim, \sim'$, entonces existe una única aplicación $\widetilde{f} \colon X/_\sim \to Y/_{\sim'}$ tal que $\widetilde{f} \circ \pi = \pi' \circ f$, donde $\pi \colon X \to X/_\sim$, $\pi' \colon Y \to Y/_{\sim'}$ son las respectivas proyecciones canónicas. ¿Cuándo es $\widetilde{f}$ biyectiva?

20. Probar la Proposición 0.1.4.

21. Sea $\mathbb{R}_2[x]$ el conjunto de todos los polinomios con coeficientes reales con grado ≤ 2. Definimos
$$D \colon \mathbb{R}_2[x] \to \mathbb{R}_2[x], \quad D(p(x)) = p'(x), \qquad E \colon \mathbb{R}_2[x] \to \mathbb{R}, \quad E(p(x)) = p(1).$$
    (a) Probar que D no es inyectiva ni sobreyectiva.
    (b) Demostrar que E es sobreyectiva y no inyectiva.
    (c) Probar que $E \circ D = 0$.
    (d) Aplicar la descomposición canónica a D, produciendo una relación de equivalencia $\sim$ en $\mathbb{R}_2[x]$ y una biyección $\widetilde{D}$ de $\mathbb{R}_2[x]/_\sim$ en $\mathrm{Im}(D)$. Interpretar $\widetilde{D}^{-1}$.

22. Demostrar que, en todo grupo $(G, \cdot)$ se verifica:
$$\overline{xy} = \overline{yx}, \qquad \forall x, y \in G.$$
¿qué ocurre si el grupo es abeliano?

23. Sea $(A, +, \cdot)$ un anillo unitario. Probar que si $x, y \in A$ cumplen $x \neq 0 \neq y$ pero $x \cdot y = 0$ (0 admite divisores), entonces $x, y \notin \mathrm{Inv}(A)$.

24. Probar que las operaciones definidas en (2) están bien definidas, es decir, no dependen de los representantes elegidos en sus clases en $\mathbb{Z}/p\mathbb{Z}$.

25. Demostrar que dado $n \in \mathbb{N}$, las n soluciones complejas de la ecuación $z^n = 1$ (*raíces n-ésimas de la unidad*) son $\{e^{i2\pi k/n} : k = 0, 1, \ldots n-1\}$. ¿Qué interpretación geométrica tienen estas raíces?

26. De un modo similar a como se construyen los números complejos a partir de los reales, se puede definir otro cuerpo que "contiene" a $\mathbb{C}$ llamado los *cuaternios* (cuaterniones o números *cuaterniónicos*), que se usa mucho en Física. El conjunto base es $\mathbb{R}^4$, pero en lugar de tener una sola unidad imaginaria tenemos tres en diferentes direcciones:

$$i := (0,1,0,0),\ j := (0,0,1,0),\ k := (0,0,0,1).$$

Así que podemos reescribir cada $(x, y, z, t) \in \mathbb{R}^4$ como

$$(x, y, z, t) = x + iy + jz + kt.$$

Se define la suma usual, componente a componente, mientras que para el producto se opera de manera natural imponiendo las relaciones:

$$i^2 = j^2 = k^2 = ijk = -1.$$

(a) Probar que $ij = k$, $ji = -k$, $jk = i$, $kj = -i$, $ki = j$, $ik = -j$.

(b) Demostrar que las operaciones $+$, $\cdot$ dotan a $\mathbb{R}^4$ de una estructura de cuerpo *no conmutativo*, al que suele denotarse por $\mathbb{H} := (\mathbb{R}^4, +, \cdot)$.

(c) Probar que $\mathbb{H}$ también se puede construir a partir de $\mathbb{C}$ de un modo análogo a como se construye $\mathbb{C}$ a partir de $\mathbb{R}$ (esto es, $\mathbb{H}$ son los "complejos de los números complejos"): denotamos $z+jw$ al par de complejos $(z, w) \in \mathbb{C}\times\mathbb{C}$ y consideramos la suma componente a componente. Introducimos el siguiente producto (que extiende al de $\mathbb{C}$):

$$(z_1 + jw_1) \cdot (z_2 + jw_2) := (z_1 z_2 - \overline{w_1} w_2) + j(\overline{z_1} w_2 + w_1 z_2)$$

Denotando por k a $i \cdot j$, probar que obtenemos de nuevo $\mathbb{H}$.

Capítulo 1

Matrices, determinantes y SEL

1.1. Matrices

Definición 1.1.1 Sea $\mathbb{K}$ un cuerpo *conmutativo* y $m, n \in \mathbb{N}$. Una *matriz de orden* $m \times n$ con coeficientes en $\mathbb{K}$ es un rectángulo de $m \cdot n$ elementos de $\mathbb{K}$ dispuestos en m filas y n columnas. Denotaremos a las matrices por letras mayúsculas, y a sus elementos (entradas) con letras minúsculas y subíndices $a_{ij} \in \mathbb{K}$:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} = (a_{ij})_{\substack{i=1,\dots,m \\ j=1,\dots,n}} = (a_{ij})_{i,j}\,.$$

Al conjunto de matrices de orden $m \times n$ sobre $\mathbb{K}$ se le denotará por $\mathcal{M}_{m\times n}(\mathbb{K})$.

- Dos matrices $A = (a_{ij})_{i,j}, B = (b_{ij})_{i,j} \in \mathcal{M}_{m\times n}(\mathbb{K})$ son iguales si $a_{ij} = b_{ij}$ $\forall i = 1, \dots, m$ y $\forall j = 1, \dots, n$.

- Dada $A \in \mathcal{M}_{m\times n}(\mathbb{K})$, su matriz *traspuesta* $A^t \in \mathcal{M}_{n\times m}(\mathbb{K})$ es la que se obtiene cambiando las filas de A por columnas, esto es $(A^t)_{ji} = a_{ij}$.

- La *matriz nula* $0 \in \mathcal{M}_{n\times m}(\mathbb{K})$ es la matriz cuyos elementos son todos $0 \in \mathbb{K}$.

- Una matriz con una sola fila ($m = 1$) se llama *matriz fila*, o *vector fila*. Una matriz con una sola columna ($n = 1$) se llama *matriz columna* o *vector columna*.

- Una matriz se dice *cuadrada de orden* n si tiene el mismo número de filas que de columnas ($m = n$). Simplificaremos la notación $\mathcal{M}_n(\mathbb{K}) := \mathcal{M}_{n\times n}(\mathbb{K})$.

- La *diagonal principal* de $A = (a_{ij})_{i,j} \in \mathcal{M}_n(\mathbb{K})$ es la formada por los elementos a_{ii} con $i = 1, \ldots, n$. La *traza* de $A = (a_{ij})_{i,j} \in \mathcal{M}_n(\mathbb{K})$ es

$$\text{Traza}(A) = \sum_{i=1}^{n} a_{ii} \in \mathbb{K}. \tag{1.1}$$

- Una *matriz diagonal* es una matriz cuadrada tal que todos los elementos que no están en la diagonal principal son cero. Ejemplos de este tipo de matrices son $0 = 0_n$ y la *matriz identidad de orden n*, $I_n = (\delta_{ij})_{i,j} \in \mathcal{M}_n(\mathbb{K})$, donde δ_{ij} es el *delta de Kronecker*:

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

- Dadas $A = (a_{ij})_{i,j}, B = (b_{ij})_{i,j} \in \mathcal{M}_{m\times n}(\mathbb{K})$, se define su suma por

$$A + B = (a_{ij} + b_{ij})_{i,j} \in \mathcal{M}_{m\times n}(\mathbb{K}), \tag{1.2}$$

y el producto de A por $\lambda \in \mathbb{K}$ mediante

$$\lambda A = (\lambda a_{ij})_{i,j} \in \mathcal{M}_{m\times n}(\mathbb{K}). \tag{1.3}$$

- Dadas $A = (a_{ij})_{i,j} \in \mathcal{M}_{m\times n}(\mathbb{K})$ y $B = (b_{ij})_{i,j} \in \mathcal{M}_{n\times p}(\mathbb{K})$, se define su *producto* $A \cdot B = \left((A \cdot B)_{ij}\right)_{i,j} \in \mathcal{M}_{m\times p}(\mathbb{K})$ mediante

$$(A \cdot B)_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}, \qquad \forall i = 1, \ldots, m, \quad \forall l = 1, \ldots, p.$$

Proposición 1.1.1 *1. $(\mathcal{M}_{m\times n}(\mathbb{K}), +)$ es un grupo conmutativo.*

2. El producto de matrices es asociativo $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ y distributivo con respecto a la suma $A \cdot (B + B') = A \cdot B + A \cdot B'$, $(A + A') \cdot B = A \cdot B + A' \cdot B$.

3. $A \cdot I_n = I_m \cdot A = A$, $\forall A \in \mathcal{M}_{m\times n}(\mathbb{K})$.

4. $A \cdot 0 = 0$, $0 \cdot A = 0$.

5. $(\lambda \cdot A) \cdot B = A \cdot (\lambda \cdot B) = \lambda \cdot (A \cdot B)$, $\forall \lambda \in \mathbb{K}$, pero el producto de matrices no es conmutativo.

6. $(\mathcal{M}_n(\mathbb{K}), +, \cdot)$ es un anillo unitario (no conmutativo si $n \geq 2$).

7. $(A + A')^t = A^t + (A')^t$, $(\lambda \cdot A)^t = \lambda \cdot A^t$.

8. $(A^t)^t = A$.
9. $(A \cdot B)^t = B^t \cdot A^t$.
10. $\mathrm{Traza}(A \cdot B) = \mathrm{Traza}(B \cdot A)$

Demostración. Ejercicio 1. $\square$

Nota 1.1.1 En la proposición anterior, puede que tenga sentido multiplicar $A \cdot B$ pero no lo tenga $B \cdot A$. Comparar $A \cdot B$ con $B \cdot A$ sólo tiene sentido si A, B son cuadradas y del mismo orden. Pero incluso en este caso ambos productos pueden ser diferentes:

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \Longrightarrow \qquad A \cdot B = 0_2, \quad B \cdot A = A.$$

Este ejemplo también muestra que si $n \geq 2$, $(\mathcal{M}_n(\mathbb{K}), +, \cdot)$ no es un cuerpo.

Definición 1.1.2 Una matriz $A \in \mathcal{M}_n(\mathbb{K})$ se dice *regular* (o *invertible*) si admite inversa para el producto. Al conjunto de todas las matrices regulares de orden n lo llamaremos *grupo lineal general de orden n sobre* $\mathbb{K}$, $GL(n, \mathbb{K})$.

Notemos que $GL(n, \mathbb{K}) = \mathrm{Inv}\,(\mathcal{M}_n(\mathbb{K}))$. Por la Proposición 0.2.2, $(GL(n, \mathbb{K}), \cdot)$ es un grupo.

1.2. Sistemas de Ecuaciones Lineales (SEL)

Definición 1.2.1 Sea $\mathbb{K}$ un cuerpo conmutativo. Una *ecuación lineal con coeficientes en* $\mathbb{K}$ es una expresión del tipo

$$a_1\, x_1 + \ldots + a_n\, x_n = b, \tag{1.4}$$

en la que $n \in \mathbb{N}$ y $a_1, \ldots, a_n, b \in \mathbb{K}$. Los elementos a_i se llaman *coeficientes*, a b se le llama *término independiente* y las x_i son las *incógnitas*. Una *solución* de (1.4) es una n-upla $(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n$ tal que al sustituir cada incógnita x_i por α_i se cumple la ecuación.

Un *sistema de m ecuaciones lineales con n incógnitas y coeficientes en* $\mathbb{K}$ (SEL) es una expresión del tipo

$$\left\{ \begin{array}{ccccccccc} a_{11}\, x_1 & + & a_{12}\, x_2 & + & \ldots & + & a_{1n}\, x_n & = & b_1 \\ a_{21}\, x_1 & + & a_{22}\, x_2 & + & \ldots & + & a_{2n}\, x_n & = & b_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{m1}\, x_1 & + & a_{m2}\, x_2 & + & \ldots & + & a_{mn}\, x_n & = & b_m \end{array} \right. \tag{1.5}$$

Es cómodo escribir el SEL anterior en su *forma matricial,*

$$Ax = b, \tag{1.6}$$

donde $A = (a_{ij})_{i,j} \in \mathcal{M}_{m\times n}(\mathbb{K})$, $b = (b_i)_i \in \mathcal{M}_{m\times 1}(\mathbb{K})$, $x = (x_j)_j \in \mathcal{M}_{1\times n}(\mathbb{K})$.

Una *solución* de (1.5) o de (1.6) es una n-upla $(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n$ que soluciona todas las ecuaciones de ese SEL.

Dos SEL se dicen *equivalentes* si tienen las mismas soluciones. El problema principal que abordaremos a continuación consiste en saber si un SEL tiene soluciones y, en caso afirmativo, calcular todas las soluciones. A menudo, este se hace pasando a sistemas equivalentes más sencillos.

Un SEL se dice *incompatible* (SI) si no tiene ninguna solución, y *compatible* (SC) en caso contrario. Un SC puede ser:

1. *Sistema Compatible Determinado* (SCD) si tiene una única solución.

2. *Sistema Compatible Indeterminado* (SCI) si tiene más de una solución.

Discutir un SEL consiste en decidir de qué tipo es según la clasificación anterior. *Resolver* un SEL consiste en calcular todas sus soluciones si las hay.

Un SEL se dice *homogéneo* si todos sus términos independientes son cero. Claramente, todo SEL homogéneo es SC, ya que al menos tiene a la solución trivial $x_1 = \cdots = x_n = 0$.

Un SEL se dice *de Cramer* si escrito en forma matricial $Ax = b$, se tiene que $A \in GL(n, \mathbb{K})$. En particular, tiene el mismo número de ecuaciones que de incógnitas.

Proposición 1.2.1 *Todo sistema de Cramer es un SCD.*

Demostración. Sea $Ax = b$ un sistema de Cramer. Como $A \in Gl(n, \mathbb{K})$, existe $A^{-1} \in Gl(n, K)$ y se tiene $x = I_n x = (A^{-1}A)x = A^{-1}(Ax) = A^{-1}b$. □

1.2.1. Sistemas escalonados

Para resolver cualquier SEL aprenderemos primero a resolver sistemas especialmente sencillos.

Definición 1.2.2 Un SEL se dice *escalonado* si la primera incógnita de cada ecuación no aparece en ninguna de las siguientes ecuaciones. Notemos que este concepto depende del orden que elijamos para escribir las incógnitas (siempre escribiremos un SEL de forma que sus incógnitas aparezcan en el mismo orden en todas las ecuaciones).

Observemos que si un SEL escalonado tiene un número m de ecuaciones mayor que el número n de incógnitas, entonces las últimas $m - n$ ecuaciones deben ser del tipo:

$$0x_1 + \cdots + 0x_n = b_j \qquad \forall j \in \{n+1, \ldots, m\},$$

en particular el SEL será SI si alguno de los términos independientes $b_{n+1}, \dots, b_m$ es distinto de cero, y si todos son cero podremos eliminar del SEL las últimas $m-n$ ecuaciones. Esta observación ya forma parte del siguiente procedimiento de discusión del SEL escalonado:

(D1) Si el SEL contiene una ecuación del tipo $0x_1 + \cdots + 0x_n = b$ con $b \neq 0$, entonces es un SI. De lo contrario el SEL será compatible y pasamos al paso (D2).

(D2) Identificamos las *incógnitas principales* y las *incógnitas secundarias* del SEL: las principales son las que aparecen como primera incógnita en alguna de las ecuaciones, y las secundarias son las restantes. Si todas las incógnitas son principales entonces el SEL es SCD. De lo contrario, estamos ante un SCI.

Si el SEL escalonado es compatible, su resolución se hace de forma escalonada, comenzando por abajo:

(R1) Si no hay incógnitas secundarias entonces la única solución del SCD se calculará despejando directamente las incógnitas principales de abajo hacia arriba.

(R2) En caso de que haya incógnitas secundarias, entonces se asigna a cada una de ellas un parámetro distinto (suelen llamarse *grados de libertad*), y se despejan las incógnitas principales en función de estos parámetros de abajo hacia arriba.

Del procedimiento anterior que todo SEL escalonado compatible con coeficientes en un cuerpo infinito tiene una única solución (SCD) o infinitas (SCI).

Como ejemplo, vamos a resolver el SEL escalonado con coeficientes reales siguiente:

$$\left\{ \begin{array}{ccccccc} x & +3y & +2z & +w & = & -5 \\ & y & +\ z & +w & = & -2 \\ & & & -w & = & 1 \end{array} \right. . \tag{1.7}$$

La variable z es secundaria mientras que x, y, w son principales. Por tanto, ponemos $z = \lambda$ donde λ es un parámetro real, y la pasamos al miembro derecho, como parte de la columna de términos independientes:

$$\left\{ \begin{array}{cccccc} x & + & 3y & +w & = & -5-2\lambda \\ & & y & +w & = & -2-\lambda \\ & & & -w & = & 1 \end{array} \right. \tag{1.8}$$

El sistema (1.8) es equivalente a (1.7). (1.8) se puede resolver directamente, sin más que despejar de abajo hacia arriba (primero w en función de λ, luego y en función de λ, w

y por tanto en función de λ, y finalmente x en función de λ). En este caso, se obtiene directamente $w = -1$ en la tercera ecuación, y sustituyendo en la segunda:

$$y = -1 - \lambda$$

Sustituyendo ahora los valores obtenidos de w, y en la primera:

$$x = -3y - w - 5 - 2\lambda = 3 + 3\lambda + 1 - 5 - 2\lambda = -1 + \lambda.$$

Deducimos que estamos ante un SCI con 1 grado de libertad y soluciones $x = -1 + \lambda, y = -1-\lambda, z = \lambda, \quad w = -1$, para todo $\lambda \in \mathbb{R}$, esto es, $\{(-1+\lambda, -1-\lambda, \lambda, -1) : \lambda \in \mathbb{R}\}$.

1.2.2. Método de Gauss

Este método es un algoritmo que transforma cualquier SEL en un SEL escalonado equivalente. Así, la discusión y resolución del sistema original se reduce a aplicar el procedimiento descrito en la sección anterior. La conversión de un SEL en otro escalonado se lleva a cabo mediante las siguientes *transformaciones elementales*:

(I) Intercambiar el orden de dos ecuaciones del SEL.

(II) Multiplicar una ecuación del SEL por un elemento de $\mathbb{K}$ distinto de cero.

(III) Sustituir una ecuación del SEL por el resultado de sumarle a dicha ecuación otra ecuación del SEL multiplicada por un elemento de $\mathbb{K}$.

Proposición 1.2.2 *Las transformaciones elementales (I), (II), (III) transforman un SEL en otro equivalente.*

Demostración. Evidente. $\square$

Como ejemplo, aplicaremos el método de Gauss para resolver el siguiente SEL no escalonado con coeficientes en $\mathbb{R}$:

$$\left\{ \begin{array}{rrrcr} x & +3y & +2z & = & -5 \\ 3x & +y & -2z & = & 1 \\ 2x & +y & -z & = & 0 \end{array} \right.$$

Para comenzar a escalonar el SEL eliminaremos la incógnita x de las ecuaciones segunda y tercera. Para ello, utilizamos transformaciones elementales (concretamente, la transformación (III)): sustituimos la segunda ecuación por el resultado de sumarle la primera multiplicada por -3. También sustituimos la tercera ecuación por el resultado de sumarle la primera multiplicada por -2. Notemos que estos coeficientes se han determinado usando que el coeficiente de x en la primera ecuación (que se llama *elemento pívot*) es 1. Este elemento pívot podría haber sido otro número real no nulo, lo cual habría complicado los cálculos, por lo cual a veces es conveniente aplicar previamente la transformación elemental (II) a la primera ecuación para conseguir que el elemento pívot se transforme en 1. Esto hubiera fallado si la primera ecuación no contiene a la incógnita x (es decir, su coeficiente en esa ecuación es 0), en cuyo caso aplicaremos previamente la transformación elemental (I) intercambiando la primera ecuación por otra que sí tenga coeficiente de x distinto de cero. De este modo, llegamos al SEL equivalente (aún no escalonado):

$$\left\{\begin{array}{cccccc} x & +3y & +2z & = & -5 \\ & -8y & -8z & = & 16 \\ & -5y & -5z & = & 10 \end{array}\right.$$

En el siguiente paso aplicaremos transformaciones elementales para hacer cero por debajo del término $-8y$ de la segunda ecuación. El elemento pívot en este momento es -8, por lo que conviene dividir por -8 la segunda ecuación, es decir, aplicar la transformación elemental (II). Aunque no es estrictamente necesario, también aplicaremos la transformación elemental (II) dividiendo la tercera ecuación por 5, con lo que obtenemos otro SEL equivalente al original:

$$\left\{\begin{array}{ccccc} x & +3y & +2z & = & -5 \\ & y & +z & = & -2 \\ & -y & -z & = & 2 \end{array}\right. ,$$

que sigue sin estar escalonado pero donde el elemento pívot (coeficiente de y en la segunda ecuación) es 1. Aplicamos una transformación de tipo (III): sustituimos la tercera ecuación por el resultado de sumarla con la segunda ecuación, con lo que llegamos al siguiente SEL equivalente al original:

$$\left\{\begin{array}{ccccc} x & +3y & +2z & = & -5 \\ & y & +z & = & -2 \end{array}\right. ,$$

que ya está escalonado (notemos que hemos perdido una ecuación). Razonando como se explicó en la sección anterior para SEL escalonados, se tratan x, y como incógnitas principales y z como secundaria: escribimos $z = \lambda$, y a pasamos a la columna de términos independientes:

$$\left\{\begin{array}{cccc} x & +3y & = & -5-2\lambda \\ & y & = & -2-\lambda \end{array}\right.$$

Así que estamos ante un SEL compatible indeterminado con 1 grado de libertad (infinitas soluciones). Para resolverlo, sustituimos en la primera ecuación el valor de y obtenido en la segunda, o bien simplificamos aún más multiplicando la segunda fila por -3 y sumándosela a la primera (transformación elemental (III)):

$$\left\{\begin{array}{cccc} x & & = & 1+\lambda \\ & y & = & -2-\lambda \end{array}\right.$$

Luego las soluciones del SEL original son

$$x = 1 + \lambda, \quad y = -2 - \lambda, \quad z = \lambda, \qquad \text{con} \;\; \lambda \in \mathbb{R}.$$

1.2.3. Expresión matricial del método de Gauss

Si analizamos lo anterior, nos daremos cuenta de que al aplicar el método de Gauss se están escribiendo superfluamente las incógnitas: lo que de verdad importa en todo el proceso son los coeficientes del SEL y sus términos independientes. Para abreviar la escritura se suele desarrollar el método de Gauss con matrices, que hemos estudiado en la Sección 1.

Consideremos un SEL general con coeficientes es un cuerpo $\mathbb{K}$ dado por:

$$\left\{ \begin{array}{ccccccccc} a_{11}\,x_1 & + & a_{12}\,x_2 & + & \dots & + & a_{1n}\,x_n & = & b_1 \\ a_{21}\,x_1 & + & a_{22}\,x_2 & + & \dots & + & a_{2n}\,x_n & = & b_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{m1}\,x_1 & + & a_{m2}\,x_2 & + & \dots & + & a_{mn}\,x_n & = & b_m \end{array} \right. .$$

Se llama *matriz de coeficientes* del SEL a la matriz

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in \mathcal{M}_{m\times n}(\mathbb{K}),$$

y *matriz ampliada* del SEL a la matriz

$$(A|b) = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array} \right) \in \mathcal{M}_{m\times (n+1)}(\mathbb{K}),$$

Notemos que cada fila de $(A|b)$ codifica una de las ecuaciones del SEL: los elementos de la columna j-ésima de $(A|b)$ con $j = 1, \dots, n$ son los coeficientes del SEL que acompañan a la incógnita x_j, y la última columna de $(A|b)$ contiene los términos independientes del SEL. La barra vertical en $(A|b)$ indica dónde aparece el signo igual en cada ecuación del SEL. Es claro que el SEL queda determinado de forma única por su matriz ampliada.

Las transformaciones elementales (I), (II), (III) que se aplicaban a un SEL para convertirlo en escalonado tienen sus análogos en el lenguaje matricial, que se llaman *transformaciones elementales por filas:*

(I) Intercambiar la posición de dos filas de $(A|b)$.

(II) Multiplicar una fila de $(A|b)$ por un elemento de $\mathbb{K}$ distinto de cero.

(III) Sustituir una fila de $(A|b)$ por el resultado de sumarle a dicha fila otra fila multiplicada por un elemento de $\mathbb{K}$.

La implementación matricial del método de Gauss tiene tres pasos:

1. Escribir la matriz ampliada $(A|b)$ del SEL.
2. Efectuar transformaciones elementales por filas de $(A|b)$ hasta obtener la matriz ampliada asociada a un SEL escalonado.
3. Escribir el SEL escalonado equivalente al original al que se ha llegado en el punto 2, discutirlo y resolverlo.

Veamos un ejemplo: queremos resolver el SEL (es el mismo del último ejemplo)

$$\left\{\begin{array}{rrrcr} x & +3y & +2z & = & -5 \\ 3x & +y & -2z & = & 1 \\ 2x & +y & -z & = & 0 \end{array}\right. .$$

Realizamos los siguientes pasos:

1. Escribimos la matriz ampliada del SEL:
$$(A|b) = \left(\begin{array}{rrr|r} 1 & 3 & 2 & -5 \\ 3 & 1 & -2 & 1 \\ 2 & 1 & -1 & 0 \end{array}\right).$$
2. Realizamos sobre $(A|b)$ tantas transformaciones elementales por filas como sea necesario hasta obtener la matriz ampliada de un SEL escalonado:
$$\left(\begin{array}{rrr|r} 1 & 3 & 2 & -5 \\ 3 & 1 & -2 & 1 \\ 2 & 1 & -1 & 0 \end{array}\right) \underset{\substack{(-3)F_1+F_2 \\ (-2)F_1+F_3}}{\sim} \left(\begin{array}{rrr|r} 1 & 3 & 2 & -5 \\ 0 & -8 & -8 & 16 \\ 0 & -5 & -5 & 10 \end{array}\right) \underset{\substack{-\frac{1}{8}F_2 \\ \frac{1}{5}F_3}}{\sim}$$
$$\left(\begin{array}{rrr|r} 1 & 3 & 2 & -5 \\ 0 & 1 & 1 & -2 \\ 0 & -1 & -1 & 2 \end{array}\right) \underset{F_2+F_3}{\sim} \left(\begin{array}{rrr|r} 1 & 3 & 2 & -5 \\ 0 & 1 & 1 & -2 \\ 0 & 0 & 0 & 0 \end{array}\right).$$
3. En este punto se puede escribir el SEL obtenido y resolver. En nuestro ejemplo el SEL al que llegaríamos es:
$$\left\{\begin{array}{rrrcr} x & +3y & +2z & = & -5 \\ & y & +z & = & -2 \end{array}\right. ,$$
ya solucionado en la sección anterior.

Nota 1.2.1 No es posible realizar transformaciones elementales *por columnas* para resolver un SEL, ya que este tipo de transformaciones no convierten un SEL en otro equivalente. Por ejemplo, consideremos el SEL con coeficientes reales

$$\left\{ \begin{array}{ccccc} x & + & y & = & 2 \\ x & - & y & = & 0 \end{array} \right. ,$$

que es un SCD con solución $x = y = 1$. Si multiplicamos por 2 la segunda columna (esto es una transformación elemental de tipo (II) por columnas) obtenemos el SEL

$$\left\{ \begin{array}{ccccc} x & + & 2y & = & 2 \\ x & - & 2y & = & 0 \end{array} \right. ,$$

que es un SCD con solución $x = 1$, $y = 1/2$, distinta a la anterior.

1.2.4. Cálculo de la matriz inversa por el método de Gauss-Jordan

Aunque más adelante veremos otro método de cálculo de la matriz inversa de una matriz regular, aprovecharemos el método de Gauss para estudiar una variante, llamada método de Gauss-Jordan, que nos permite calcular dicha matriz inversa.

Sea $A \in GL(n, \mathbb{K})$ una matriz regular. Calcular su inversa equivale a solucionar la siguiente ecuación matricial con incógnita X:

$$A \cdot X = I_n, \qquad \text{donde} \qquad X = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \cdots & \cdots & \cdots \\ x_{n1} & \cdots & x_{nn} \end{pmatrix}.$$

La ecuación anterior puede verse como un SEL de n^2 ecuaciones y n^2 incógnitas x_{ij}, ya que al multiplicar A por cada columna de X se obtiene cada una de las columnas de I_n:

$$\left(\begin{array}{c|c|c} A & \cdots & 0 \\ \hline \cdots & \cdots & \cdots \\ \hline 0 & \cdots & A \end{array} \right) \left(\begin{array}{c} x_{11} \\ \cdots \\ x_{n1} \\ \hline \cdots \\ \hline x_{1n} \\ \cdots \\ x_{nn} \end{array} \right) = \left(\begin{array}{c} 1 \\ \cdots \\ 0 \\ \hline \cdots \\ \hline 0 \\ \cdots \\ 1 \end{array} \right). \tag{1.9}$$

Escribamos el SEL anterior en forma matricial como $Bx = b$, siendo $B \in \mathcal{M}_{n^2}(\mathbb{K})$ la matriz de coeficientes (la matriz de la izquierda, que está escrita *por bloques*), $b \in \mathcal{M}_{n^2 \times 1}(\mathbb{K})$ la columna de términos independientes (matriz de la derecha) y $x \in \mathcal{M}_{n^2 \times 1}(\mathbb{K})$ la columna de incógnitas.

Por ser $A \in Gl(n, \mathbb{K})$, la matriz B es regular (su inversa tiene la misma estructura que B cambiando A por A^{-1}). Esto nos dice que el SEL (1.9) es de Cramer. Por la Proposición 1.2.1, (1.9) es un SCD. Por tanto, puede resolverse por el método de Gauss realizando transformaciones elementales por filas a $(B|b)$.

Las mismas transformaciones elementales que se usen para las primeras n filas de B (en el primer bloque) se pueden usar para cada uno de los siguientes bloques de n filas. Esto nos dice que aplicar trasformaciones elementales por filas a $(B|b)$ es equivalente a aplicarlas a la siguiente matriz:

$$(A|I_n) = \left(\begin{array}{ccc|ccc} a_{11} & \cdots & a_{1n} & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} & 0 & \cdots & 1 \end{array} \right)$$

Bastará entonces con realizar transformaciones elementales por filas a $(A|I_n)$ hasta obtener la matriz identidad I_n en la parte izquierda de la matriz, es decir, transformándola en otra del tipo (I_n, C) con $C \in \mathcal{M}_n(\mathbb{K})$. Notemos que cada una de las columnas de C será la solución del SEL de n^2 ecuaciones para la correspondiente columna de incógnitas de X, esto es, $C = A^{-1}$.

El razonamiento anterior es reversible, si podemos aplicar transformaciones elementales por filas a $(A|I_n)$ llegando a una matriz del tipo $(I_n|C)$, entonces A es regular y $C = A^{-1}$.

Veamos un ejemplo: consideremos la matriz $A \in \mathcal{M}_n(\mathbb{K})$ dada por

$$A = \begin{pmatrix} 1 & 2 \\ -1 & 2 \end{pmatrix}.$$

Entonces,

$$(A|I_2) = \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ -1 & 2 & 0 & 1 \end{array} \right) \sim \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & 4 & 1 & 1 \end{array} \right),$$

de donde concluimos que A es regular. Seguimos aplicando transformaciones elementales (la segunda de abajo hacia arriba):

$$(A|I_2) \sim \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & 1 & 1/4 & 1/4 \end{array} \right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 1/2 & -1/2 \\ 0 & 1 & 1/4 & 1/4 \end{array} \right),$$

luego la matriz inversa de A es

$$A^{-1} = \begin{pmatrix} 1/2 & -1/2 \\ 1/4 & 1/4 \end{pmatrix}.$$

1.3. Permutaciones

Definición 1.3.1 Sea $S(n) = \{1, 2, \ldots, n\} \subset \mathbb{N}$. Llamaremos *permutación* de $S(n)$ (o de n elementos cualesquiera) a toda aplicación biyectiva $\sigma : S(n) \to S(n)$. Al conjunto de todas las permutaciones de $S(n)$ lo denotaremos por S_n, que tiene cardinal $n!$.

Como se vio en la Sección 0.2.1, S_n con la composición tiene estructura de grupo (no abeliano a menos que $n \geq 2$). A veces a la composición en S_n se la llama *producto*.

La notación estándar para permutaciones es

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Por ejemplo,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

son permutaciones en S_4 y S_3, respectivamente.

Definición 1.3.2 (A) Un *ciclo* es una permutación $\sigma \in S_n$ que verifica que la reordenación de los elementos que no son fijos es circular. Por ejemplo,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}.$$

son ciclos, pero

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

no lo es.

Existe una notación simplificada para ciclos. En ella, σ y τ se escriben

$$\sigma = (1\ 2\ 3\ 4\ 5) \in S_5, \qquad \tau = (1\ 2\ 3\ 4) \in S_5.$$

(B) Se llama *longitud de un ciclo* al número de símbolos no fijos de un ciclo. Por ejemplo, $\sigma = (1\ 2\ 3\ 4\ 5) \in S_5$ tiene longitud 5, y $\tau = (1\ 2\ 3\ 4) \in S_5$ tiene longitud 4.

Lema 1.3.1 *Toda permutación $\sigma \in S_n$, $\sigma \neq 1$, se descompone como producto de ciclos disjuntos.*

Demostración. Tomemos una permutación

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Supongamos primero que 1 no es fijo por σ. Consideremos el ciclo

$$\tau_1 = (1\ \sigma(1)\ \sigma^2(1)\ \dots\ \sigma^s(1)),$$

donde s es el menor número natural que verifica $\sigma^{s+1} = 1$ (s existe porque $\{1, 2, \ldots, n\}$ es un conjunto finito). Llamemos $\sigma^t(1) = i_t, \quad \forall t = 1, \ldots s$.

Si $s = n$, hemos terminado: σ es un ciclo.

Si $s > n$, en τ_1 hay más de n cifras, luego al menos dos cifras se repiten. Así, existen índices $i, j \in \{1, \ldots, s\}$ tales que $\sigma^i(1) = \sigma^j(1)$, luego $\sigma^{-i+j}(1) = 1$. Por lo tanto, $-i+j \geq s+1$, y de aquí se tiene que $j \geq s+i+1$. Como $j \leq s$, obtenemos que $i+1 \leq 0$, contradicción.

Supongamos entonces que $s < n$. Y por tanto, quedan $j_1, \ldots, j_{n-s}$ cifras que no han salido en τ_1. Ordenemos estas cifras de menor a mayor:

$$j_1 < \ldots < j_{n-s},$$

y la restricción de σ a $\{j_1, \ldots, j_{n-s}\}$ vuelve a ser una permutación, a la aplicaremos el razonamiento anterior. En un número finito de pasos se termina, y por tanto,

$$\sigma = (1\ i_1\ \ldots i_s)(j_1\ \ldots j_t) \cdot \ldots \cdot (k_1\ \ldots k_h),$$

que es un producto de ciclos. Esto termina la demostración en el caso de que 1 no sea fijo por σ. Si $\sigma(1) = 1$, basta aplicar el razonamiento anterior al primer dígito de $\{2, \ldots, n\}$ que no sea fijo por σ. $\square$

Definición 1.3.3 Una *trasposición* es un ciclo de longitud dos. Por ejemplo, las siguientes permutaciones son trasposiciones:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix} = (2\ 3), \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix} = (1\ 5).$$

Lema 1.3.2 *Todo ciclo se descompone como producto de trasposiciones.*

Demostración. $(i_1, \ldots, i_r) = (i_1, i_2) \cdot \ldots \cdot (i_{r-1}, i_r)$. $\square$

Como consecuencia de los Lemas 1.3.1 y 1.3.2 tenemos:

Lema 1.3.3 *Toda permutación se descompone como producto de trasposiciones.*

En general, la descomposición de una permutación en producto de trasposiciones no es única. Por ejemplo,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix} = \begin{cases} = (1\ 2\ 3\ 4) = (1\ 2)(2\ 3)(3\ 4) \\ = (2\ 3\ 4\ 1) = (2\ 3)(3\ 4)(4\ 1) \end{cases}$$

Teorema 1.3.1 *Dada $\sigma \in S_n$, la paridad ó imparidad del número de trasposiciones en que se descompone σ no depende de la descomposición, sino sólo de σ.*

Demostración. Tomemos dos descomposiciones de σ en producto de trasposiciones:

$$\sigma = (i_1\ i_2)\dots(i_{r-1}\ i_r) = (j_1\ j_2)\dots(j_{s-1}\ j_s).$$

Así,

$$(i_{r-1}\ i_r)\dots(i_1\ i_2)(j_1\ j_2)\dots(j_{s-1}\ j_s) = 1,$$

luego hemos reducido el enunciado a probar que la identidad sólo puede descomponerse en un número par de trasposiciones. Para ver esto, consideremos ahora el polinomio simétrico de n variables,

$$\begin{array}{rccl} P: & \mathbb{R}^n & \to & \mathbb{R} \\ & (x_1,\dots,x_n) & \mapsto & \prod_{i<j}(x_i - x_j). \end{array}$$

Dados $i, j \in \{1,\dots,n\}$, $i < j$, podemos escribir P como

$$P(x_1,\dots,x_n) = (x_i - x_j)\cdot \prod_{\substack{k=1 \\ k\neq i \\ k\neq j}}^{n} (x_i - x_k)(x_j - x_k)\cdot Q,$$

donde $Q = Q(x_1,\dots,\widehat{x_i},\dots,\widehat{x_j},\dots x_n)$ es un polinomio en $n-2$ variables. Llamemos σ a la trasposición $\sigma = (i\ j)$, con $i < j$. Entonces, de la última ecuación se tiene que

$$P(x_{\sigma(1)},\dots,x_{\sigma(n)}) = -P(x_1,\dots,x_n).$$

Y por tanto, si σ_1, σ_2 son dos trasposiciones,

$$P(x_{(\sigma_1\circ\sigma_2)(1)},\dots,x_{(\sigma_1\circ\sigma_2)(n)}) = -P(x_{\sigma_2(1)},\dots,x_{\sigma_2(n)}) = P(x_1,\dots,x_n),$$

y en general, si $\sigma_1,\dots,\sigma_s$ son trasposiciones,

$$P(x_{(\sigma_1\circ\dots\circ\sigma_s)(1)},\dots,x_{(\sigma_1\circ\dots\circ\sigma_s)(n)}) = (-1)^s\cdot P(x_1,\dots,x_n).$$

Luego si descomponemos la identidad de S_n como producto de s trasposiciones, $1 = \sigma_1\circ\dots\circ\sigma_s$, entonces de la última fórmula obtenemos que

$$P(x_1,\dots,x_n) = (-1)^s\cdot P(x_1,\dots,x_n),$$

$\forall (x_1,\dots x_n) \in \mathbb{R}^n$. Luego s debe ser par (P no es idénticamente cero). □

Definición 1.3.4

(A) Una permutación $\sigma \in S_n$ se dice *par* (resp. *impar*) cuando se descompone en un número par (resp. impar) de trasposiciones.

Por ejemplo,

$$\sigma = (1\ 2\ 3\ 4) \quad \text{es impar},$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (1\ 2\ 3)(4\ 5) = (1\ 2)(2\ 3)(4\ 5) \quad \text{es impar},$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = (1\ 2\ 3) = (1\ 2)(2\ 3) \quad \text{es par}.$$

(B) Se define la *signatura* de una permutación $\sigma \in S_n$ como

$$\operatorname{sig}(\sigma) := (-1)^{[\sigma]} = \begin{cases} 1 & \text{si } \sigma \text{ es par}, \\ -1 & \text{si } \sigma \text{ es impar}. \end{cases}$$

La notación $[\sigma]$ corresponde al *número de inversiones* de σ: diremos que dos elementos $i < j$ de $\{1, \ldots, n\}$ presentan una *inversión* de σ si $\sigma(i) > \sigma(j)$.

Lema 1.3.4 sig: $S_n \to (\{-1, 1\}, \cdot)$ *es un homomorfismo de grupos. En particular, se verifican:*

$$\operatorname{sig}(\sigma \circ \tau) = \operatorname{sig}(\sigma) \cdot \operatorname{sig}(\tau), \quad \operatorname{sig}(\sigma) = \operatorname{sig}(\sigma^{-1}), \quad \operatorname{sig}(1) = 1.$$

Demostración. Sean $\sigma, \tau \in S_n$. Veamos que $\operatorname{sig}(\sigma \circ \tau) = \operatorname{sig}(\sigma) \cdot \operatorname{sig}(\tau)$, y habremos terminado. Notemos que si tenemos σ y τ descompuestas en producto de trasposiciones, al yuxtaponer estas descomposiciones tendremos una descomposición de $\sigma \circ \tau$ en producto de trasposiciones, y el número de trasposiciones que aparece en dicha descomposición para $\sigma \circ \tau$ es la suma de los números de trasposiciones de las descomposiciones de σ y de τ. Así pues, si ambas son pares ó ambas impares, la composición es par, y si una es par y la otra impar, la composición es impar. □

1.4. Determinante de una matriz cuadrada

En toda esta sección, $\mathbb{K}$ será un cuerpo conmutativo de característica distinta de 2, a cuyos elementos llamaremos *escalares*.

Definición 1.4.1 Sea $A = (a_{ij})_{i,j} \in \mathcal{M}_n(\mathbb{K})$. Se define el *determinante de A* como

$$\det A = |A| = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} := \sum_{\sigma \in S_n} \operatorname{sig}(\sigma)\, a_{\sigma(1)\,1} \ldots a_{\sigma(n)\,n} \tag{1.10}$$

Por ejemplo, en el caso $n = 2$ tenemos

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21},$$

y si $n = 3$ tenemos la *regla de Sarrus:*

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}.$$

Volviendo al caso general, notemos que en cada sumando de la sumatoria de (1.10) aparece un único elemento de cada fila y de cada columna. El siguiente resultado muestra que el papel de filas y columnas es intercambiable en la definición de determinante.

Proposición 1.4.1 $\det A = \det A^t$, *para toda* $A \in \mathcal{M}_n(\mathbb{K})$.

Demostración. Sea $A = (a_{ij})$ y $A^t = (b_{ij})$ (esto es, $b_{ij} = a_{ji}$).

$$\begin{aligned}
\det A &= \sum_{\sigma\in S_n} \mathrm{sig}(\sigma)\; a_{\sigma(1)1} \dots a_{\sigma(n)n} \\
&\overset{(a)}{=} \sum_{\sigma\in S_n} \mathrm{sig}(\sigma)\; a_{1\,\sigma^{-1}(1)} \dots a_{n\,\sigma^{-1}(n)} \overset{(b)}{=} \sum_{\sigma\in S_n} \mathrm{sig}(\sigma^{-1})\; a_{1\,\sigma^{-1}(1)} \dots a_{n\,\sigma^{-1}(n)} \\
&\overset{(c)}{=} \sum_{\tau\in S_n} \mathrm{sig}(\tau)\; a_{1\,\tau(1)} \dots a_{n\,\tau(n)} \overset{(d)}{=} \sum_{\tau\in S_n} \mathrm{sig}(\tau)\; b_{\tau(1)\,1} \dots b_{\tau(n)\,n} \\
&= \det A^t,
\end{aligned}$$

donde en (a) se reordenan (usando la conmutatividad de $\mathbb{K}$) los factores de cada sumando por orden creciente del primer subíndice; en (b) se usa que $\mathrm{sig}(\sigma) = \mathrm{sig}(\sigma^{-1})$ (Lema 1.3.4); en (c) se ha sustituido $\tau = \sigma^{-1}$ y se ha usado en el indice de la sumatoria que es equivalente sumar en $\sigma \in S_n$ que en $\tau = \sigma^{-1} \in S$, ya que la aplicación $\sigma \mapsto \sigma^{-1}$ es una biyección de S_n en sí mismo; por último, en (d) se ha sustituido cada a_{ij} por b_{ji}. □

Nota 1.4.1 Como consecuencia de la Proposición 1.4.1, todas las propiedades de los determinantes que se obtengan “por columnas” serán también válidas “por filas” y viceversa.

1.4.1. Propiedades elementales de los determinantes

Proposición 1.4.2 *Sea* $A \in \mathcal{M}_n(\mathbb{K})$. *Entonces:*

1. *Si una fila o columna de* A *se multiplica por un escalar* $a \in \mathbb{K}$, *entonces el determinante de la matriz resultante también queda multiplicado por* a. *En particular,* $|aA| = a^n|A|$.

2. *Si cada elementos a_k de una fila o columna se expresa como la suma de dos escalares $a_k = b_k + c_k$, entonces $|A|$ es igual a la suma de dos determinantes, uno de ellos con cada escalar a_k reemplazado por el primer escalar de la suma b_k, y el otro con el segundo c_k.*

3. *Si se intercambian dos filas entre sí (o columnas), el determinante de la matriz resultante cambia de signo.*

4. *Dada una permutación $\sigma_0 \in S_n$, sea A^{σ_0} la matriz que se obtiene cambiando cada fila (o columna) i-ésima de A por la $\sigma_0(i)$-ésima. Entonces, $|A^{\sigma_0}| = \operatorname{sig}(\sigma_0)\,|A|$.*

5. *Si dos filas o columnas de $|A|$ son iguales, entonces $|A| = 0$.*

6. *Si dos filas o columnas de $|A|$ son proporcionales (en particular, si una es nula), entonces $|A| = 0$.*

7. *Si una fila o columna de A se puede expresar como combinación lineal del resto de filas o columnas, entonces $|A| = 0$.*

8. *Si a una fila o columna de A se le suma una combinación lineal del resto de filas o columnas, entonces el valor del determinante no varía.*

9. $\det I_n = 1$.

10. *Si $C \in \mathcal{M}_n(\mathbb{K})$, entonces $|A \cdot C| = |A| \cdot |C|$. En particular $|A \cdot C| = |C \cdot A|$.*

Demostración. Probamos cada apartado anterior por filas (por columnas se tendrá probado gracias a la Nota 1.4.1)

Para el apartado 1, como en cada sumando de (1.10) aparece un único elemento de cada fila y de cada columna, necesariamente en cada sumando aparecerá un único elemento de la fila multiplicada por a. Usando la conmutatividad de $\mathbb{K}$ podemos sacar factor común a aplicando la propiedad distributiva en $\mathbb{K}$.

Para el apartado 2, al reemplazar cada a_k por $b_k + c_k$ en (1.10), se obtiene que en cada sumando un único factor se reemplaza por $(b_k + c_k)$. Aplicando la propiedad distributiva en $\mathbb{K}$ se tiene lo que se busca.

Para el apartado 3, supongamos que se intercambian las filas i-ésima y j-ésima de A, $1 \leq i < j \leq n$. Consideremos la trasposición $\tau = (ij) \in S_n$. Sea A^{τ} la correspondiente matriz obtenida permutando las filas i, j. Entonces,

$$\begin{aligned}
\det A^{\tau} &= \sum_{\sigma \in S_n} \mathrm{sig}(\sigma)\; a_{\sigma(\tau(1)),1} \dots a_{\sigma(\tau(n)),n} \\
&\overset{(a)}{=} - \sum_{\sigma \in S_n} \mathrm{sig}(\sigma \circ \tau)\; a_{(\sigma\circ\tau)(1),1} \dots a_{(\sigma\circ\tau)(n),n} \\
&\overset{(b)}{=} - \sum_{\sigma' \in S_n} \mathrm{sig}(\sigma')\; a_{\sigma'(1)\,1} \dots a_{\sigma'(n)\,n} = -\det A.
\end{aligned}$$

donde en (a) se ha usado que $\mathrm{sig}(\sigma \circ \tau) = -\mathrm{sig}(\sigma)$ (porque τ es una trasposición) y en (b) se ha llamado σ' a $\sigma \circ \tau$ y se ha usado que, fijada $\tau \in S_n$, la aplicación $\sigma \mapsto \sigma'$ es una biyección en S_n.

El apartado 4 sobre A^{σ_0} se deduce del apartado 3, usando que toda permutación se escribe como producto de un número par o impar de trasposiciones.

El apartado 5 es consecuencia directa del 3 (ya que la característica de $\mathbb{K}$ es distinta de 2), y el apartado 6 se deduce directamente de 1 y 5. El apartado 7 se deduce de 2 y 6. El 8 se deduce de 2 y 7.

Para el apartado 9, recordemos que $(I_n)_{ij} = \delta_{ij}$ por lo que

$$\det I_n = \sum_{\sigma \in S_n} \mathrm{sig}(\sigma)\; \delta_{\sigma(1)\,1} \dots \delta_{\sigma(n)\,n} = \delta_{11} \dots \delta_{nn} = 1.$$

Por último, la demostración de la propiedad no es inmediata a partir de la definición (1.10), sino que se prueba a partir del enfoque de determinante de una matriz a partir del determinante de un endomorfismo (se prueba que el determinante de la composición de dos endomorfismos es el producto de los determinantes de ambos endomorfismos). Posponemos esta demostración hasta estudiar este enfoque[1]. $\square$

Nota 1.4.2 De los dos últimos apartados se deduce que si $A \in \mathcal{M}_n(\mathbb{K})$ es regular, entonces

$$1 = \det(A \cdot A^{-1}) = \det\, A \cdot \det(A^{-1})$$

En particular, $\det\, A \neq 0$ y $\det(A^{-1}) = (\det A)^{-1}$. El recíproco es cierto (Proposición 1.4.4)

1.4.2. Desarrollo del determinante por adjuntos

Definición 1.4.2 Dada una matriz $A = (a_{ij})_{i,j} \in \mathcal{M}_n(\mathbb{K})$, llamaremos

- *Menor complementario* del elemento (i, j) al determinante $\alpha_{ij} \in \mathbb{K}$ de la matriz de orden $n - 1$ que se obtiene suprimiendo la fila i-ésima y la columna j-ésima de A.

[1] Una demostración distinta puede consultarse en el libro de L. Merino y E. Santos.

- *Adjunto* del elemento (i,j) a $\Delta_{ij} := (-1)^{i+j}\alpha_{ij} \in \mathbb{K}$, y *matriz adjunta*, $\mathrm{Adj}(A) = (\Delta_{ij})_{i,j} \in \mathcal{M}_n(\mathbb{K})$ a la la matriz cuyo elemento (i,j) es el adjunto del elemento (i,j) de A, $\forall i,j \in \{1,\ldots,n\}$.

Proposición 1.4.3 *Sea* $A = (a_{ij})_{i,j} \in \mathcal{M}_n(\mathbb{K})$.

1. *Dados* $i_0, j_0 \in \{i, \ldots n\}$*, se tiene*

$$\begin{aligned} |A| &= \sum_{j=1}^{n} a_{i_0 j}\Delta_{i_0 j} \quad \textit{(desarrollo por la fila } i_0\textit{)}, \\ &= \sum_{i=1}^{n} a_{i j_0}\Delta_{i j_0} \quad \textit{(desarrollo por la columna } j_0\textit{)}. \end{aligned}$$

2. $\displaystyle\sum_{k=1}^{n} a_{ik}\Delta_{jk} = \sum_{k=1}^{n} a_{ki}\Delta_{kj} = \delta_{ij}|A|, \qquad i,j \in \{1,\ldots,n\}.$

3. $A \cdot [\mathrm{Adj}(A)]^t = [\mathrm{Adj}(A)]^t \cdot A = |A| I_n$.

Demostración. Para el apartado 1, consideremos primero el caso $i_0 = 1$. Dado $j \in \{1,\ldots,n\}$, llamemos $S[j] := \{\sigma \in S_n : \sigma(1) = j\}$, conjunto de $(n-1)!$ elementos. Entonces,

$$\begin{aligned} |A| &\overset{(a)}{=} \sum_{\sigma\in S_n} (-1)^{[\sigma]}\, a_{1\sigma(1)} \ldots a_{n\sigma(n)} \\ &\overset{(b)}{=} \sum_{j=1}^{n} a_{1j} \left(\sum_{\sigma\in S[j]} (-1)^{[\sigma]}\, a_{2\sigma(2)} \ldots a_{n\sigma(n)} \right) \\ &\overset{(c)}{=} \sum_{j=1}^{n} (-1)^{j-1} a_{1j} \left(\sum_{\sigma\in S[j]} (-1)^{[\sigma]-(j-1)}\, a_{2\sigma(2)} \ldots a_{n\sigma(n)} \right) \\ &\overset{(d)}{=} \sum_{j=1}^{n} (-1)^{j-1} a_{1j}\alpha_{1j} = \sum_{j=1}^{n} a_{1j}(-1)^{j+1}\alpha_{1j} = \sum_{j=1}^{n} a_{1j}\Delta_{1j}, \end{aligned}$$

donde en (a) se ha usado la definición de $|A|$ $(= |A^t|)$; en (b) se han agrupado los sumandos según el valor de $j = \sigma(1)$; en (c) se multiplica y divide por $(-1)^{j-1}$; en (d) se ha usa la siguiente expresión del menor complementario:

$$\alpha_{1j} = \sum_{\sigma\in S[j]} (-1)^{[\sigma]-(j-1)}\, a_{2\sigma(2)} \ldots a_{n\sigma(n)},$$

que se deduce de que en cada sumando los valores $\sigma(2), \ldots, \sigma(n)$ pueden verse como una permutación del conjunto $A = \{1, \ldots, j-1, j+1, \ldots, n\}$ cuyo número de inversiones se calcula descontando a $[\sigma]$ las $j-1$ inversiones correspondientes a $\sigma(1)=j$. Esto prueba la fórmula del desarrollo del determinante por la primera fila.

Para el caso $i_0>1$, haciendo i_0-1 trasposiciones de índices contiguos de filas llevaremos la i_0-ésima de A hasta la primera posición, con lo que llegaremos una nueva matriz A_0 cuyo determinante es $|A_0|=(-1)^{i_0-1}|A|$. Los menores complementarios de la primera fila de A_0 son iguales a los menores complementarios de la fila i_0 de A; y los adjuntos de A_0 difieren de los de A en el factor $(-1)^{i_0-1}$. Esto nos dice que aplicando el desarrollo del determinante de A_0 por la primera fila y multiplicando la expresión por $(-1)^{i_0-1}$, se obtiene el desarrollo del determinante de A por los adjuntos de su fila i_0-ésima.

Finalmente, el desarrollo del determinante por la columna j_0-ésima se reduce al del desarrollo por filas sin más que trasponer la matriz y usar que los menores complementarios del elemento (i,j) de la matriz A y (j,i) de la matriz A^t coinciden. Esto termina de probar el apartado 1.

Veamos el apartado 2: en el caso $i=j$ la fórmula se tiene porque

$$\sum_{k=1}^{n} a_{ik}\Delta_{jk} \tag{1.11}$$

es el desarrollo de $|A|$ por los adjuntos de su fila i-ésima, y

$$\sum_{k=1}^{n} a_{ki}\Delta_{kj} \tag{1.12}$$

es el desarrollo de $|A|$ por los adjuntos de su columna j-ésima. En el caso $i\neq j$, (1.11) se anula porque es el desarrollo por adjuntos de una matriz con dos filas repetidas; concretamente, la matriz que se obtiene reemplazando en A su fila j-ésima por su fila i-ésima (ya que el adjunto del elemento (j,k) es el mismo para esas dos matrices). Un argumento similar prueba que (1.12) se anula si $i\neq j$.

El apartado 3 no es más que escribir el 2 en forma matricial. □

Usando la Proposición 1.4.3, el cálculo de un determinante de orden n se reduce al de n determinantes de orden $n-1$. En principio, esto permite reducir formalmente el cálculo de un determinante de cualquier orden $n>3$ al caso $n=3$, para el cual podemos usar la regla de Sarrus. Sin embargo, este procedimiento no es eficiente: se necesitaran calcular $n!/3! = n!/6$ determinantes de orden 3, pero $n!$ crece demasiado rápido para que este algoritmo sea computacionalmente eficiente. Esto se resuelve usando las otras propiedades de los determinantes (Proposición 1.4.2) para simplificar los cálculos.

1.4.3. Cálculo de un determinante "haciendo ceros" (Regla de Chio)

Esencialmente, esta regla consiste en conseguir que todos los elementos de una fila o columna del determinante de una matriz $A\in\mathcal{M}_n(\mathbb{K})$ sean nulos excepto uno de ellos, al cual llamaremos *elemento base* o *pívot*, que además se podrá tomar como 1. Aplicando el desarrollo por los adjuntos de esa fila o columna tendremos que $|A|$ coincide con el adjunto del elemento base. Lo vemos más en detalle:

1. Escogemos una fila o columna de A que contenga un 1 o un -1 y el mayor número posible ceros. En el caso de que ningún elemento de A sea 1 ó -1, escogeremos uno de los elementos no nulos[2], a, de la fila o columna elegida de entre las de más ceros, y dividiremos todos los elementos de esa fila o columna por a; esto hará que el determinante quede dividido por a. Con esto tendremos elegido el elemento base.

2. Una vez escogido el elemento base, haremos que el resto de los elementos de su fila o columna sean nulos multiplicando sucesivamente la columna o fila del elemento base por un escalar apropiado y restándolo o sumándolo a las otras columnas o filas.

Por ejemplo, si el elemento base es $a_{11} = 1$ y escogemos hacer ceros en la primera fila, multiplicaremos sucesivamente su columna por $a_{12}, \ldots, a_{1n}$ restaremos el resultado a las siguientes columnas:

$$|A| = \begin{vmatrix} 1 & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} 1 & 0 & \cdots & 0 \\ a_{21} & a_{22} - a_{12}a_{21} & \cdots & a_{2n} - a_{1n}a_{21} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} - a_{12}a_{n1} & \cdots & a_{nn} - a_{1n}a_{n1} \end{vmatrix}.$$

Según lo anterior, $|A|$ es el adjunto Δ_{11} de la matriz de la derecha. En general, el determinante a calcular será $1/a$ (recordemos el paso 1 anterior) multiplicado por el adjunto del elemento base o su opuesto, según que el elemento base fuera 1 ó -1. En el ejemplo anterior,

$$|A| = 1 \cdot \Delta_{11} + 0 \cdot \Delta_{12} + \cdots + 0 \cdot \Delta_{1n} = \Delta_{11}.$$

Ejemplo 1.4.1 Calculemos el siguiente determinante usando la regla de Chio:

$$\begin{vmatrix} 5 & 3 & 2 & 3 \\ 4 & 3 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 0 & 2 & 2 & 3 \end{vmatrix}$$

Los pasos son entonces: (1) tomamos como elemento base el $(3,1)$ y desarrollaremos por la primera columna (pues $a_{31} = 1$ y la primera columna tiene el mayor número de ceros); (2) para conseguir que en la primera columna los elementos distintos de la posición $(3,1)$ sean 0, multiplicamos la tercera fila por 5 y 4 y se la restamos a la primera y la segunda filas;

[2] Si todos los elementos de una fila o columna de A son 0, entonces $\det A = 0$ y no hay nada que calcular.

(3) el determinante se reduce entonces al adjunto del elemento $(3,1)$ de la nueva matriz. Esto es:

$$\begin{vmatrix} 5 & 3 & 2 & 3 \\ 4 & 3 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 0 & 2 & 2 & 3 \end{vmatrix} = \begin{vmatrix} 0 & -2 & -8 & -2 \\ 0 & -1 & -7 & -3 \\ 1 & 1 & 2 & 1 \\ 0 & 2 & 2 & 3 \end{vmatrix} = (-1)^{1+3} \begin{vmatrix} -2 & -8 & -2 \\ -1 & -7 & -3 \\ 2 & 2 & 3 \end{vmatrix} = \begin{vmatrix} -2 & -8 & -2 \\ -1 & -7 & -3 \\ 2 & 2 & 3 \end{vmatrix}$$

Este último determinante ya se puede calcular usando la regla de Sarrus. No obstante, puede ser más sencillo seguir aplicando la regla de Chio, tomando ahora como base el elemento $(2,1)$ y desarrollando por los adjuntos de su columna:

$$\begin{vmatrix} -2 & -8 & -2 \\ -1 & -7 & -3 \\ 2 & 2 & 3 \end{vmatrix} = \begin{vmatrix} 0 & 6 & 4 \\ -1 & -7 & -3 \\ 0 & -12 & -3 \end{vmatrix} = (-1)(-1)^{2+1} \begin{vmatrix} 6 & 4 \\ -12 & -3 \end{vmatrix} = 30.$$

1.4.4. Cálculo de la inversa de una matriz regular

Veamos el recíproco de la Nota 1.4.2.

Proposición 1.4.4 *Sea $A = (a_{ij})_{i,j} \in \mathcal{M}_n(\mathbb{K})$. Si $|A| \neq 0$, entonces A es regular y su inversa viene dada por:*

$$A^{-1} = \frac{\mathrm{Adj}(A)^t}{|A|}.$$

Demostración. Como $|A| \neq 0$, podemos dividir por $|A|$ en el apartado 3 de la Proposición 1.4.3, y aplicar la definición de matriz inversa. □

Nota 1.4.3 Es muy fácil comprobar aplicando la definición que la matriz traspuesta de $\mathrm{Adj}(A)$ es la matriz adjunta de A^t, es decir $\mathrm{Adj}(A)^t = \mathrm{Adj}(A^t)$.

Corolario 1.4.1 *Sea $A \in \mathcal{M}_n(\mathbb{K})$. Entonces, $A \in GL(n,\mathbb{K})$ si y sólo si Si* $\det A \neq 0$.

Ejemplo 1.4.2 Calculemos la inversa de la matriz

$$A = \begin{pmatrix} 1 & 2 & -1 \\ 3 & 4 & -3 \\ 2 & 2 & 2 \end{pmatrix}.$$

Calculamos en primer lugar su determinante:

$$\begin{vmatrix} 1 & 2 & -1 \\ 3 & 4 & -3 \\ 2 & 2 & 2 \end{vmatrix} = \begin{vmatrix} 1 & 2 & -1 \\ 0 & -2 & 0 \\ 0 & -2 & 4 \end{vmatrix} = -8.$$

Como $\det A \neq 0$, sabemos que A es regular luego admite inversa. Para calcularla, primero calculamos la matriz adjunta:

$$\mathrm{Adj}(A) = \begin{pmatrix} 14 & -12 & -2 \\ -6 & 4 & 2 \\ -2 & 0 & -2 \end{pmatrix}.$$

Ahora aplicamos la fórmula de la Proposición 1.4.4:

$$A^{-1} = \frac{1}{|A|} \cdot \mathrm{Adj}(A)^t = \frac{1}{(-8)} \cdot \begin{pmatrix} 14 & -6 & -2 \\ -12 & 4 & 0 \\ -2 & 2 & -2 \end{pmatrix} = \begin{pmatrix} -7/4 & 3/4 & 1/4 \\ 3/2 & -1/2 & 0 \\ 1/4 & -1/4 & 1/4 \end{pmatrix}.$$

1.5. Aplicaciones de los determinantes a los SEL

1.5.1. Rango por filas y por columnas

Definición 1.5.1 Sea $A \in \mathcal{M}_{m\times n}(\mathbb{K})$.

1. Una *submatriz* de A es una matriz B que se obtenga suprimiendo k filas y l columnas de A, donde $k \in \{0, 1, \dots m\}$, $l \in \{0, 1, \dots, n\}$.

2. Las filas de submatriz B de A se dicen *linealmente independientes* cuando no existe una fila f de B que se pueda expresar como combinación lineal de las filas de $B \setminus \{f\}$. Por ejemplo, si B está formado por una sola fila, entonces es B es linealmente independiente si y sólo si $B \neq 0$; y si B está formado por dos filas, entonces es B es linealmente independiente si y sólo si sus filas no son proporcionales. Todo esto se puede expresar análogamente para columnas de A.

3. Llamaremos *rango por filas* (resp. *por columnas*) de A al número máximo de filas (resp. columnas) de A linealmente independientes.

   Por ejemplo, el rango de una matriz escalonada coincide con el número de filas no nulas que contiene. Esto quiere decir que el método de Gauss permite también calcular el rango de una matriz.

4. Un *menor de orden* h de A es una submatriz cuadrada de orden $h \in \{1, \dots, \text{mín}\{m, n\}\})$.

Nota 1.5.1 Aunque aún no podemos probarlo, los rangos por filas y por comunas de una matriz coinciden (Teorema del Rango).

Recordemos las transformaciones elementales (por filas) introducidas para el estudio de los SEL en la Sección 1.2.3. Es fácil comprobar que estas transformaciones no alteran el rango por filas de la matriz a la que se aplican, y por el Teorema del Rango, tampoco alteran el rango si se realizan por columnas.

Para probar la siguiente proposición usaremos resultados que aún no se han demostrado, pero es útil enunciarla ahora por razones prácticas.

Proposición 1.5.1 *El rango de una matriz* $A \in \mathcal{M}_{m\times n}(\mathbb{K})$ *es el mayor orden* h *de los menores de* A *con determinante distinto de* 0.

Demostración. Llemamos $r = \text{rango}(A)$, y sea h el orden de un menor B de A con determinante distinto de cero.
$\boxed{r \geq h}$: Las h columnas (o filas) de B son linealmente independientes. Por tanto, las correspondientes h columnas (o filas) de A también son linealmente independientes.
$\boxed{r \leq h}$: Por definición de rango por columnas, A contiene r columnas independientes. Éstas forman una submatriz $B \in M_{m\times r}$, y el rango de B por columnas coincide con su rango por filas. Por tanto, B contiene r filas linealmente independientes. Estas r filas de B forman una submatriz cuadrada C de B de orden r. Es claro que C es una submatriz cuadrada de A. Además, $|C| \neq 0$ al ser independientes sus filas y columnas. □

En la demostración anterior se han usado los siguientes resultados que se probarán más adelante:

1. El Teorema del Rango (el rango por filas de cualquier matriz es igual a su rango por columnas), para poder hablar sólo del rango de la matriz A. Este resultado se verá en la Sección 4.6 como consecuencia de los anuladores en el espacio dual y la aplicación traspuesta.

2. Si una matriz cuadrada es regular (equivalentemente, si su determinante es no nulo), entonces sus columnas son linealmente independientes. Y recíprocamente: si una matriz cuadrada tiene todas sus columnas independientes, entonces es regular. Esto se verá en la Sección 3.2.

Calcular el rango de una matriz $A \in \mathcal{M}_{m\times n}(\mathbb{K})$ se reduce entonces a encontrar un menor con determinante distinto de cero del orden mayor posible. A menudo, esto se pueda hacer con una simple inspección de los elementos de A, pero es útil disponer de un método sistemático. Supongamos que se ha obtenido un menor B de A con orden $h < \text{mín}\{m, n\}$ y determinante distinto de 0. No hace falta calcular todos los determinantes de menores de orden $h + 1$, sino sólo los de aquellos que contienen a la submatriz B.

Lo explicamos con un ejemplo: Consideremos la matriz

$$A = A_0 = \begin{pmatrix} -5 & -3 & 1 & -1 & 0 \\ -1 & 0 & 2 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 2 & 0 & -4 & -2 & 0 \\ -3 & -3 & -3 & 2 & 0 \end{pmatrix}.$$

1. Primero suprimimos las filas o columnas que sean nulas o proporcionales a otras.

   En nuestro ejemplo se puede suprimir la última columna (por ser nula) y la cuarta fila (por ser proporcional a la segunda). El problema se reduce entonces a calcular el rango de[3] la submatriz

$$A_1 = \begin{pmatrix} -5 & -3 & 1 & -1 \\ -1 & 0 & 2 & 1 \\ 1 & 1 & 1 & 1 \\ -3 & -3 & -3 & 2 \end{pmatrix}.$$

2. Escogemos un elemento de la matriz A_1 que sea distinto de 0, con lo que podemos asegurar que el rango es al menos 1. A continuación, *orlamos* ese menor, esto es, formamos un menor de orden 2, añadiéndole elementos de una nueva fila y columna de A_1. Si alguno de esos menores tiene determinante no nulo podremos asegurar que el rango de A es al menos 2, y repetir sucesivamente este paso.

   En el ejemplo, escogemos el elemento -5 (elemento $(1,1)$) que es distinto de 0, y lo orlamos con los elementos de las segundas fila y columna para obtener el menor B de A_1 de orden 2 cuyo determinante es $\begin{vmatrix} -5 & -3 \\ -1 & 0 \end{vmatrix} = -3$, también distinto de 0. Esto implica que rango$(A) \geq 2$. Seguimos orlando de la manera más sencilla (usando la tercera fila y columna de A_1), pero encontramos

$$\begin{vmatrix} -5 & -3 & 1 \\ -1 & 0 & 2 \\ 1 & 1 & 1 \end{vmatrix} = 0.$$

   Así que no concluimos nada al orlar B de esta forma. En este caso, debemos orlar B de otra manera y seguir comprobando. Por ejemplo, en vez de añadir la tercera columna añadimos la cuarta, y seguimos orlando con la tercera fila:

$$B_1 = \begin{pmatrix} -5 & -3 & -1 \\ -1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \qquad |B_1| = 0 - 3 + 1 - 0 - 3 + 5 = 0.$$

   Así que no nos quedan opciones con la tercera fila de A_1 para orlar B. Seguimos orlando B pero con la cuarta fila de A_1. Empezamos con la tercera columna de A_1:

$$B_2 = \begin{pmatrix} -5 & -3 & 1 \\ -1 & 0 & 2 \\ -3 & -3 & -3 \end{pmatrix}, \qquad |B_2| = 0 + 18 + 3 - 0 + 9 - 30 = 0.$$

[3] El procedimiento sigue siendo válido sin suprimir la cuarta fila, aunque resulta más largo.

Como tampoco nos vale, seguimos orlando B con la cuarta fila de A_1 y ahora con la cuarta columna de A_1:

$$B_3 = \begin{pmatrix} -5 & -3 & -1 \\ -1 & 0 & 1 \\ -3 & -3 & 2 \end{pmatrix}, \qquad |B_3| = 0 + 9 - 3 - 0 - 6 - 15 \neq 0,$$

luego B_3 es un menor de orden 3 con determinante no nulo. Por tanto, rango$(A) \geq 3$. Ahora tenemos que orlar B_3, y sólo hay una manera posible, que es con toda la matriz A_1. Pero $|A_1| = 0$, luego el rango de A_1 no puede ser 4. Así que rango$(A) = 3$.

1.5.2. Regla de Cramer y Teorema de Rouché-Frobenius

Recordemos que en la Proposición 1.2.1 se vio que todo sistema de Cramer $Ax = b$ es un SCD, y que su solución está dada por $x = A^{-1}b$.

Proposición 1.5.2 (Regla de Cramer) *Sea $Ax = b$ un sistema de Cramer, es decir, $A \in Gl(n, \mathbb{K})$. Entonces, su única solución viene dada por*

$$x_1 = \frac{\begin{vmatrix} b_1 & a_{12} & \cdots & a_{1n} \\ b_2 & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_n & a_{n2} & \cdots & a_{nn} \end{vmatrix}}{|A|}, \ldots, x_n = \frac{\begin{vmatrix} a_{11} & a_{12} & \cdots & b_1 \\ a_{21} & a_{22} & \cdots & b_2 \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & b_n \end{vmatrix}}{|A|} \tag{1.13}$$

(el numerador de x_j se obtiene calculando el determinante de la matriz obtenida tras reemplazar la columna j-ésima de A por la columna de términos independientes b).

Demostración. Usando la forma explícita de la matriz inversa tenemos

$$x = A^{-1} \cdot b = \frac{1}{|A|} \mathrm{Adj}(A)^t \cdot b = \frac{1}{|A|} \begin{pmatrix} \Delta_{11} & \Delta_{21} & \cdots & \Delta_{n1} \\ \Delta_{12} & \Delta_{22} & \cdots & \Delta_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ \Delta_{1n} & \Delta_{2n} & \cdots & \Delta_{nn} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \frac{1}{|A|} \begin{pmatrix} \sum_{i=1}^n \Delta_{i1} b_i \\ \vdots \\ \sum_{i=1}^n \Delta_{in} b_i \end{pmatrix},$$

y (1.13) se deduce de que cada componente $\sum_{i=1}^n \Delta_{ij} b_i = \sum_{i=1}^n b_i \Delta_{ij}$ es el desarrollo por los adjuntos de la columna j-ésima en el numerador de (1.13) . $\square$

Ejemplo 1.5.1 Discutiremos y resolveremos el SEL

$$\left.\begin{array}{rl} 2x_1 - x_2 + x_3 & = 3 \\ 2x_2 - x_3 & = 1 \\ -x_1 + x_2 \quad & = 1 \end{array}\right\}$$

El determinante de la matriz A de coeficientes es:

$$\begin{vmatrix} 2 & -1 & 1 \\ 0 & 2 & -1 \\ -1 & 1 & 0 \end{vmatrix} = \begin{vmatrix} 2 & 1 & 0 \\ 0 & 2 & -1 \\ -1 & 1 & 0 \end{vmatrix} = \begin{vmatrix} 2 & 1 \\ -1 & 1 \end{vmatrix} = 3,$$

luego $A \in Gl(3, \mathbb{R})$ y el sistema es de Cramer. Calculamos su solución por la regla de Cramer:

$$x_1 = \frac{1}{3}\begin{vmatrix} 3 & -1 & 1 \\ 1 & 2 & -1 \\ 1 & 1 & 0 \end{vmatrix} = \frac{1}{3}\begin{vmatrix} 4 & 1 & 0 \\ 1 & 2 & -1 \\ 1 & 1 & 0 \end{vmatrix} = 1$$

$$x_2 = \frac{1}{3}\begin{vmatrix} 2 & 3 & 1 \\ 0 & 1 & -1 \\ -1 & 1 & 0 \end{vmatrix} = \frac{1}{3}\begin{vmatrix} 2 & 4 & 0 \\ 0 & 1 & -1 \\ -1 & 1 & 0 \end{vmatrix} = 2$$

$$x_3 = \frac{1}{3}\begin{vmatrix} 2 & -1 & 3 \\ 0 & 2 & 1 \\ -1 & 1 & 1 \end{vmatrix} = \frac{1}{3}\begin{vmatrix} 0 & 1 & 5 \\ 0 & 2 & 1 \\ -1 & 1 & 1 \end{vmatrix} = 3.$$

Consideremos ahora un SEL arbitrario,

$$Ax = b, \qquad A \in \mathcal{M}_{m\times n}(\mathbb{K}). \tag{1.14}$$

Como la matriz de coeficientes A es una submatriz de la matriz ampliada $(A|b)$, se tiene que $\text{rango}(A) \leq \text{rango}(A|b)$. Además, como $(A|b)$ sólo tiene una columna más que A, tenemos dos opciones: $\text{rango}(A) = \text{rango}(A|b)$ o bien $\text{rango}(A) + 1 = \text{rango}(A|b)$.

Teorema 1.5.1 (Rouché-Frobenius) *El SEL* (1.14) *es compatible si y sólo si* $\text{rango}(A) = \text{rango}(A|b)$.

Demostración. Supongamos que (1.14) compatible, y sea $(x_1, \ldots, x_n) \in \mathbb{K}^n$ una solución. Reescribiendo (1.14) como

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \cdots \\ a_{m1} \end{pmatrix} x_1 + \begin{pmatrix} a_{12} \\ a_{22} \\ \cdots \\ a_{m2} \end{pmatrix} x_2 + \begin{pmatrix} a_{1n} \\ a_{2n} \\ \cdots \\ a_{mn} \end{pmatrix} x_n = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}, \tag{1.15}$$

es evidente que la columna b de términos independientes es combinación lineal de las columnas de A, luego b no aporta nada al rango de $(A|b)$ por columnas, es decir, $\text{rango}(A) = \text{rango}(A|b)$.

Recíprocamente, supongamos que rango(A) = rango$(A|b)$. Viendo este rango por columnas, concluimos que b ha de ser combinación lineal de las columnas de A, y por tanto existen $x_1, \ldots, x_n \in \mathbb{K}$ tales que (1.15) se cumple, es decir $(x_1, \ldots, x_n) \in \mathbb{K}^n$ es solución de (1.14). □

Supongamos que (1.14) es compatible, y por tanto, rango(A) = rango$(A|b) := r$. Tomemos un menor B de A con determinante distinto de cero y orden r (B es también un menor de $(A|b)$ que representa su rango). Suprimimos las filas de $(A|b)$ que no contengan las filas de B. Las columnas de B determinan r incógnitas que tomaremos como principales del sistema. Las otras $n-r$ incógnitas se consideran secundarias, y se las puede tomar como parámetros $\lambda_1, \ldots, \lambda_{n-r}$ y aplicarles la regla de Cramer. (en particular, (1.14) será determinado si y sólo si $n = r$). Suponiendo que esas incógnitas principales son las r primeras, el SEL original resulta equivalente a:

$$\left.\begin{array}{c} a_{11}x_1 + \ldots + a_{1r}x_r = b_1 - a_{1(r+1)}\lambda_1 \ldots - a_{1n}\lambda_{n-r} \\ \cdots \\ a_{r1}x_1 + \ldots + a_{rr}x_r = b_r - a_{r(r+1)}\lambda_1 \ldots - a_{rn}\lambda_{n-r} \end{array}\right\}$$

Para cada valor de los parámetros, este sistema es de Cramer, por lo que podemos usar la regla de Cramer para solucionarlo:

$$x_1 = \frac{\begin{vmatrix} b_1 - a_{1(r+1)}\lambda_1 \ldots - a_{1n}\lambda_{n-r} & a_{12} & \cdots & a_{1r} \\ \cdots & \cdots & \cdots & \cdots \\ b_r - a_{r(r+1)}\lambda_1 \ldots - a_{rn}\lambda_{n-r} & a_{r2} & \cdots & a_{rr} \end{vmatrix}}{\begin{vmatrix} a_{11} & \cdots & a_{1r} \\ \cdots & \cdots & \cdots \\ a_{r1} & \cdots & a_{rr} \end{vmatrix}}, \ldots$$

$$\ldots,\ x_r = \frac{\begin{vmatrix} a_{11} & \cdots & a_{1(r-1)} & b_1 - a_{1(r+1)}\lambda_1 \ldots - a_{1n}\lambda_{n-r} \\ \cdots & \cdots & \cdots & \cdots \\ a_{r1} & \cdots & a_{r(r-1)} & b_r - a_{r(r+1)}\lambda_1 \ldots - a_{rn}\lambda_{n-r} \end{vmatrix}}{\begin{vmatrix} a_{11} & \cdots & a_{1r} \\ \cdots & \cdots & \cdots \\ a_{r1} & \cdots & a_{rr} \end{vmatrix}}.$$

Ejemplo 1.5.2 Discutiremos y resolveremos el SEL

$$\left.\begin{array}{rl} x_1 + x_2 + x_3 + x_4 & = 1 \\ -x_1 + x_2 - x_3 + x_4 & = 0 \\ -x_1 + 5x_2 - x_3 + 5x_4 & = 2 \end{array}\right\}.$$

Primero escribimos la matriz ampliada,

$$(A|b) = \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & 0 \\ -1 & 5 & -1 & 5 & 2 \end{array} \right).$$

Para calcular el rango de A consideramos el menor $\begin{vmatrix} 1 & 1 \\ -1 & 1 \end{vmatrix} = 2(\neq 0)$. El rango de A es, por tanto, al menos 2. Orlando este menor se ontiene

$$\begin{vmatrix} 1 & 1 & 1 \\ -1 & 1 & -1 \\ -1 & 5 & -1 \end{vmatrix} = 0, \qquad \begin{vmatrix} 1 & 1 & 1 \\ -1 & 1 & 1 \\ -1 & 5 & 5 \end{vmatrix} = 0.$$

Por tanto, el rango de A es 2 y el menor $B = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ tiene orden máximo dentro de A con determinante no nulo.

Para $(A|b)$ tenemos una posibilidad más a la hora de orlar, que es haciéndolo con la columna de términos independientes. Como

$$\begin{vmatrix} 1 & 1 & 1 \\ -1 & 1 & 0 \\ -1 & 5 & 2 \end{vmatrix} = 0,$$

deducimos que rango$(A|b) = 2$, luego sistema es compatible e indeterminado. Para resolverlo, teniendo en cuenta el menor B, suprimimos la tercera ecuación y escogemos x_1, x_2 como incógnitas principales. Así, x_3, x_4 se toman como parámetros,

$$x_3 = \lambda_1 \qquad x_4 = \lambda_2,$$

y el sistema se reescribe

$$\left. \begin{array}{rl} x_1 + x_2 & = 1 - \lambda_1 - \lambda_2 \\ -x_1 + x_2 & = \lambda_1 - \lambda_2 \end{array} \right\}.$$

Su solución usando la regla de Cramer es

$$x_1 = \frac{1}{2} \cdot \begin{vmatrix} 1 - \lambda_1 - \lambda_2 & 1 \\ \lambda_1 - \lambda_2 & 1 \end{vmatrix} = \frac{1}{2} - \lambda_1,$$

$$x_2 = \frac{1}{2} \cdot \begin{vmatrix} 1 & 1 - \lambda_1 - \lambda_2 \\ -1 & \lambda_1 - \lambda_2 \end{vmatrix} = \frac{1}{2} - \lambda_2.$$

1.6. Ejercicios.

1. Probar la Proposición 1.1.1.

2. Discutir y resolver el siguiente SEL:

$$\left\{\begin{array}{rcrcrcrcrcl} x & + & 2y & & & + & s & & & = & 7 \\ & & y & + & z & - & 2s & + & t & = & 2 \\ 2x & - & y & + & z & + & 4s & + & t & = & 0 \end{array}\right. .$$

3. Discutir y resolver el siguiente SEL con coeficientes complejos:

$$\left\{\begin{array}{rcrcrcl} i\,x & + & 2i\,y & + & z & = & 0 \\ x & - & 3y & + & 2z & = & 0 \\ 2i\,x & & & + & (i+1)\,z & = & i \end{array}\right. .$$

4. Discutir y resolver el siguiente SEL con coeficientes reales:

$$\left\{\begin{array}{rcrcrcr} & - & 4y & - & z & = & -7 \\ x & + & y & + & z & = & 2 \\ x & - & 2y & + & z & = & -2 \\ -x & + & 2y & & & = & 3 \end{array}\right. .$$

5. Probar que si tenemos una matriz por cajas $\left(\begin{array}{c|c} A & 0_{n\times m} \\ \hline C & D \end{array}\right)$ donde $A \in M_n(\mathbb{K}), D \in M_m(\mathbb{K})$ y $C \in \mathcal{M}_{m\times n}(\mathbb{K})$, entonces

$$\det\left(\begin{array}{c|c} A & 0 \\ \hline C & D \end{array}\right) = |A| \cdot |D|.$$

6. Demuéstrese que si $A \in GL(n, \mathbb{K})$ entonces $A^t \in GL(n, \mathbb{K})$ siendo $(A^t)^{-1} = (A^{-1})^t$.

7. Constrúyanse explícitamente todos los elementos de S_1, S_2 y S_3.

8. Demuéstrese por inducción que el cardinal (número de elementos) de S_n es $n! := 1 \cdot 2 \cdot \cdots \cdot (n-1) \cdot n$.

9. Probar que el grupo de permutaciones S_n es abeliano si y sólo si $n \leq 2$. Dado un conjunto $X \neq \varnothing$ (posiblemente infinito), demostrar que $(S(X), \circ)$ no es abeliano salvo que el número de elementos de X sea 1 ó 2.

10. Demuéstrese que en cada grupo S_n con $n \geq 2$ el número de permutaciones pares es igual al de las impares.

11. Calcular el valor de los siguientes determinantes:

a) $\begin{vmatrix} 3 & a & a & a & a \\ a & 3 & a & a & a \\ a & a & 3 & a & a \\ a & a & a & 3 & a \\ a & a & a & a & 3 \end{vmatrix}$

b) $\begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ 1 & a_3 & a_3^2 & \cdots & a_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{vmatrix}$ (Vandermonde)

12. *a*) Una matriz $A \in \mathcal{M}_n(\mathbb{K})$ se dice *antisimétrica* si $A^t = -A$. Probar que si A es antisimétrica, entonces $\det(A) = (-1)^n \det(A)$.

    b) Una matriz $A \in Gl(n, \mathbb{K})$ se dice *ortogonal* si $A^t = A^{-1}$. Probar que si A es ortogonal, entonces $\det(A) = \pm 1$.

    c) Una matriz $A \in \mathcal{M}_n(\mathbb{C})$ se dice *hermítica* si $A^t = \overline{A}$ (conjugada de la matriz A). Probar que si A es hermítica, entonces:

    1) $\det(A) \in \mathbb{R}$ y los elementos de la diagonal principal son números reales.
    2) A se puede escribir $A = B + iC$ donde $B, C \in \mathcal{M}_n(\mathbb{R})$ con B simétrica y C antisimétrica.
    3) La inversa de una matriz hermítica invertible es también hermítica.
    4) Si $\lambda \in \mathbb{C}$ y $x \in \mathbb{C}^n \setminus \{0\}$ cumplen $Ax = \lambda x$, entonces $\lambda \in \mathbb{R}$.

Capítulo 2

Espacios vectoriales

La estructura de espacio vectorial abstrae propiedades básicas y a menudo elementales de $\mathbb{R}^n$. Está en la base de muchas teorías matemáticas: aparecen en Geometría, Álgebra, Cálculo, etc. A pesar de su sencillez, los espacios vectoriales desempeñan un papel clave en el estudio de objetos complicados, como curvas, superficies o variedades: a cada uno se estos objetos se les asocia en cada punto el espacio vectorial que "mejor las aproxime" en cierto sentido (la recta, el plano o el espacio tangente en ese punto), y a partir de ahí nos centramos en analizar la variación de este espacio vectorial al mover el punto. Los espacios vectoriales también son muy importantes en Física, donde sirven para modelar velocidades y fuerzas, entre otros conceptos.

2.1. Noción de espacio vectorial sobre un cuerpo

Cuando hablamos de vectores es natural pensar en segmentos de recta orientados (flechas), con propiedades tales como la "dirección", el "sentido" o el "módulo". Sabemos desde la enseñanza secundaria que en el plano o en el espacio dos vectores se pueden sumar obteniéndose otro vector. También se puede multiplicar un número real por un vector y el resultado es un nuevo vector. Estas operaciones presentan propiedades con ciertas similitudes a las que se vieron en la definición de estructuras algebraicas. Los espacios vectoriales suponen la abstracción matemática de los conjuntos que admiten una ley de composición interna y un producto por elementos de un cuerpo, de modo que se cumplen las mismas propiedades formales que cuando operamos vectores en un plano o en el espacio.

Definición 2.1.1 Un *espacio vectorial* sobre un cuerpo conmutativo $\mathbb{K}$ (en casi todos los casos nos restringiremos a $\mathbb{K} = \mathbb{R}$ ó $\mathbb{C}$, pero en alguna ocasión tomaremos $\mathbb{K} = \mathbb{Q}$) es una terna $(V, +, \cdot)$ formada por un conjunto V, una ley de composición interna $+ : V \times V \to V$

y una aplicación $\cdot : \mathbb{K} \times V \to V$ (llamada *ley de composición externa*) tales que se cumplen las siguientes propiedades:

1. $(V, +)$ es un grupo abeliano:
   (i) Asociativa: $(u+v)+w = u+(v+w)$, $\forall u, v, w \in V$.
   (ii) Elemento neutro: $\exists 0 \in V$ (este 0 es sólo notación y no debe confundirse con el 0 de $\mathbb{K}$) tal que $v+0 = 0+v = v$, $\forall v \in V$.
   (iii) Elemento simétrico: $\forall v \in V$, $\exists w \in V$ tal que $v+w = w+v = 0$. Al simétrico de v se le denotará por $-v$ y se le llamará *opuesto de* v.
   (iv) Conmutativa: $u+v = v+u$, $\forall u, v \in V$.

2. La ley de composición externa verifica las propiedades:
   (i) *Pseudoasociativa:* $(a \cdot b) \cdot v = a \cdot (b \cdot v)$, $\forall a, b \in \mathbb{K}, \forall v \in V$.
   (ii) *Unimodular:* $1 \cdot v = v$, $\forall v \in V$, siendo $1 \in \mathbb{K} \setminus \{0\}$ es el elemento neutro del producto de $\mathbb{K}$.
   (iii) *Distributiva respecto de la suma en* $\mathbb{K}$*:* $(a+b) \cdot v = a \cdot v + b \cdot v$, $\forall a, b \in \mathbb{K}$, $\forall v \in V$.
   (iv) *Distributiva respecto de la suma en* V*:* $a \cdot (u+v) = a \cdot u + a \cdot v$, $\forall a \in \mathbb{K}$, $\forall u, v \in V$.

Simplificaremos la notación escribiendo $V(\mathbb{K})$ cuando queramos denotar un espacio vectorial sobre $\mathbb{K}$. A los elementos de V se les llama *vectores*[1], y a los de $\mathbb{K}$, escalares. Cuando $\mathbb{K} = \mathbb{R}$ (resp. $\mathbb{K} = \mathbb{C}$) diremos que $V(\mathbb{R})$ es un *espacio vectorial real* (resp. *espacio vectorial complejo*).

Notemos que si $V(\mathbb{K})$ es un espacio vectorial, entonces $V \neq \varnothing$ ya que $V(, +)$ debe tener un elemento neutro.

Sea $V(\mathbb{K})$ un espacio vectorial. Como $(V, +)$ es un grupo abeliano, todas las propiedades que conocemos de grupos se mantienen para la suma de vectores. En particular:

1. El elemento neutro $0 \in V$ de la suma de vectores es único.
2. Si $v+w = v+w'$ o bien $w+v = w'+v$, entonces $w = w'$.
3. $\forall v \in V$, su elemento opuesto $-v \in V$ es único. En particular, $-(-v) = v$. Dados $u, v \in V$, escribiremos $u - v := u + (-v)$.

Proposición 2.1.1 *Sea* $V(\mathbb{K})$ *un espacio vectorial. Entonces,*

1. $a \cdot 0 = 0$*,* $\forall a \in \mathbb{K}$*.*

[1]Pero no han de ser flechas en el sentido habitual de $\mathbb{R}^2$ o $\mathbb{R}^3$.

2. $0 \cdot v = 0$, $\forall v \in V$.

3. *Dados* $a \in \mathbb{K}$ *y* $v \in V$, *si* $a \cdot v = 0$, *entonces* $a = 0$ *ó* $v = 0$.

4. $-(a \cdot v) = (-a) \cdot v = a \cdot (-v)$, $\forall a \in \mathbb{K}$, $\forall v \in V$.

5. $-v = (-1) \cdot v$, $\forall v \in V$.

6. $-(u + v) = -u - v$, $\forall u, v \in V$.

7. $(-a) \cdot (-v) = a \cdot v$, $\forall a \in \mathbb{K}$, $\forall v \in V$.

8. *Si* $a \cdot u = a \cdot v$ *con* $a \in \mathbb{K}$, $a \neq 0$ *y* $u, v \in V$, *entonces* $u = v$.

9. *Si* $a \cdot v = b \cdot v$ *con* $a, b \in \mathbb{K}$ *y* $v \in V$ *con* $v \neq 0$, *entonces* $a = b$.

Demostración. 1) Usando la propiedad de neutro para 0 en $(V, +)$ y la distributiva, $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, y ahora simplificamos en $(V, +)$.
2) Usando que 0 es el neutro en $(\mathbb{K}, +)$, $0 \cdot v = (0+0) \cdot v = 0 \cdot v + 0 \cdot v$, y ahora simplificamos en $(V, +)$.
3) Sean $a \in \mathbb{K}$ y $v \in V$ con $a \cdot v = 0$. Basta demostrar que si $a \neq 0$ entonces $v = 0$, vemos esto último: como $a \neq 0$ y $\mathbb{K}$ es un cuerpo, existe $a^{-1} \in \mathbb{K}$. Multiplicando por a^{-1} a ambos lados de $a \cdot v = 0$ y usando la propiedad 1), tenemos $0 = a^{-1} \cdot (a \cdot v) = (a^{-1} \cdot a) \cdot v = 1 \cdot v = v$, donde hemos usado la propiedad pseudoasociativa en la segunda igualdad y la unimodular en la última.
4) Tenemos que demostrar dos igualdades. Para la primera igualdad basta observar que $(a \cdot v) + ((-a) \cdot v) = (a + (-a)) \cdot v = 0 \cdot v = 0$. Para la segunda, $(a \cdot v) + a \cdot (-v) = a \cdot (v - v) = a \cdot 0 = 0$.
5) Tomar $a = 1$ en la primera igualdad de 4) y usar la propiedad unimodular.
6) Por 4) y una de las distributivas, $-(u + v) = (-1) \cdot (u + v) = (-1) \cdot u + (-1) \cdot v = -u + (-v) = -u - v$.
7) Por la propiedad 5) y la pseudoasociativa, $(-a) \cdot (-v) = (-a) \cdot ((-1) \cdot v) = ((-a) \cdot (-1)) \cdot v = a \cdot v$.
8) Multiplicar por a^{-1} ambos lados de $a \cdot u = a \cdot v$, y usar la pseudoasociativa y la unimodular.
9) La igualdad $a \cdot v = b \cdot v$ equivale a $a \cdot v - (b \cdot v) = 0$. Partiendo de esta igualdad, usando 4) y una de las distributivas, $0 = a \cdot v - (b \cdot v) = a \cdot v + (-b) \cdot v = (a + (-b)) \cdot v = (a - b) \cdot v$. Como por hipótesis $v \neq 0$, de la propiedad 3) tenemos que $a - b = 0$, es decir, $a = b$. □

Nota 2.1.1 Una consecuencia inmediata de la propiedad 9) es la siguiente:

> Si $V(\mathbb{K})$ es un espacio vectorial sobre un cuerpo infinito $\mathbb{K}$, entonces o bien $V = \{0\}$ o V contiene infinitos vectores.

Para comprobarlo, supongamos que existe $v \in V$ con $v \neq 0$. Sea $L(v) := \{a \cdot v \mid a \in \mathbb{K}\} \subset V$. Basta ver que $L(v)$ es infinito. Si $a \cdot v = b \cdot v$, entonces por la propiedad 9) tendremos $a = b$. Por tanto, para diferentes valores de $a \in \mathbb{K}$ los vectores $a \cdot v$ son distintos. Como $\mathbb{K}$ es infinito, entonces $L(v)$ también lo es.

En lo que sigue, simplificaremos $a\,v := a\,v$ para $a \in \mathbb{K}$ y $v \in V$.

2.1.1. Ejemplos de espacios vectoriales

1. Sea $\mathbb{K}$ un cuerpo conmutativo y $n \in \mathbb{N}$. $\mathbb{K}^n = \{(x_1, \dots, x_n) \mid x_i \in \mathbb{K}, \forall i = 1, \dots, n\}$. Sobre $\mathbb{K}^n$ se definen la suma "coordenada a coordenada" y el producto por escalares de $\mathbb{K}$:

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) := (x_1 + y_1, \dots, x_n + y_n), \quad a(x_1, \dots, x_n) := (ax_1, \dots, ax_n).$$

   Es fácil verificar que con las operaciones anteriores, $\mathbb{K}^n$ es un espacio vectorial sobre $\mathbb{K}$, al que llamaremos $\mathbb{K}^n(\mathbb{K})$ o simplemente $\mathbb{K}^n$. El vector nulo es $(0, \dots, 0)$, y el opuesto de $(x_1, \dots, x_n)$ es $(-x_1, \dots, -x_n)$. $\mathbb{K}^n$ será muy importante pues veremos que, en cierto sentido, es el modelo de cualquier espacio vectorial de *dimensión finita*.

2. **(Espacios de matrices)** Dados $m, n \in \mathbb{N}$, $\mathcal{M}_{m\times n}(\mathbb{K})$ tiene estructura de espacio vectorial sobre $\mathbb{K}$ con la suma dada por (1.2) y el producto por escalares en $\mathbb{K}$ dado por (1.3). Por el apartado 1 de la Proposición 1.1.1, $(\mathcal{M}_{m\times n}(\mathbb{K}), +)$ es un grupo abeliano. En cuanto a la propiedad pseudoasociativa, dados $a, b \in \mathbb{K}$ y $A = (a_{ij})_{i,j} \in \mathcal{M}_{m\times n}(\mathbb{K})$, se tiene

$$(a\,b)\,A = ((a\,b)\,a_{ij})_{i,j} = (a\,(b\,a_{ij}))_{i,j} = a\,(b\,a_{ij})_{i,j} = a\,(b\,A),$$

   donde hemos usado la propiedad asociativa del producto de $\mathbb{K}$. Comprobemos la propiedad unimodular: dada $A = (a_{ij})_{i,j} \in \mathcal{M}_{m\times n}(\mathbb{K})$, $1\,A = (1\,a_{ij})_{i,j} = (a_{ij})_{i,j} = A$, donde hemos usado que 1 es el neutro para el producto en $\mathbb{K}$. Finalmente, veamos las dos propiedades distributivas: Sean $a, b \in \mathbb{K}$ y $A = (a_{ij})_{i,j}, B = (b_{ij})_{i,j} \in \mathcal{M}_{m\times n}(\mathbb{K})$.

$$\begin{aligned} (a+b)\,A &= ((a+b)\,a_{ij})_{i,j} = (a\,a_{ij} + b\,a_{ij})_{i,j} = (a\,a_{ij})_{i,j} + (b\,a_{ij})_{i,j} \\ &= a\,A + b\,A, \\ a\,(A+B) &= a\,(a_{ij} + b_{ij})_{i,j} = (a\,(a_{ij} + b_{ij}))_{i,j} = (a\,a_{ij} + a\,b_{ij})_{i,j} \\ &= (a\,a_{ij})_{i,j} + (a\,b_{ij})_{i,j} = a\,A + a\,B. \end{aligned}$$

   Por tanto, $\mathcal{M}_{m\times n}(\mathbb{K})$ es un espacio vectorial sobre $\mathbb{K}$. El vector nulo es la matriz nula $0_{m\times n}$.

3. **(Vectores libres)** En el plano o en el espacio se consideran los vectores fijos $\overrightarrow{AB}$ donde A, B son puntos llamados *extremos inicial y final.* No todo par de vectores fijos $\overrightarrow{AB}, \overrightarrow{CD}$ se pueden sumar: hace falta que $B = C$ para trazar el vector fijo $\overrightarrow{AD}$ y verlo como la suma $\overrightarrow{AB} + \overrightarrow{CD}$. Además, esto tiene problemas de tipo lógico si queremos dotar de sentido a una igualdad tan natural como

$$\overrightarrow{AB} + \overrightarrow{CD} = \overrightarrow{CD} + \overrightarrow{AB},$$

ya que para escribir el miembro de la izquierda se necesita que $B = C$, mientras que para escribir el de la derecha se necesita que $D = A$. Para solucionar estos problemas se introduce el concepto de vectores *equipolentes.* A cada vector fijo $\overrightarrow{AB}$ le asociamos su *módulo* $|\overrightarrow{AB}| := d(A, B)$, donde $d(A, B)$ es la distancia entre sus extremos, su *dirección* (entendida como la de la recta que pasa por el origen y es paralela a la que pasa por A y B si $A \neq B$ y su *sentido*, que asocia a A (resp. B) el papel de extremo inicial (resp. final) del vector fijo $\overrightarrow{AB}$. En el caso particular de $A = B$, el módulo es cero, y la dirección degenera en $\{0\}$ visto dentro de $\mathbb{R}^2$ o $\mathbb{R}^3$. En el conjunto X de vectores fijos del plano definimos la llamada *relación de equipolencia:* dados $\overrightarrow{AB}, \overrightarrow{CD} \in X$, diremos que $\overrightarrow{AB} \sim \overrightarrow{CD}$ si ambos vectores fijos tienen igual módulo, dirección y sentido[2]. Es fácil probar que $\sim$ es una relación de equivalencia. Cada clase de equivalencia $[\overrightarrow{AB}]$ se denomina un *vector libre.* El conjunto cociente $V := X/_\sim$ de los vectores libres tiene estructura de espacio vectorial, definiendo la suma de vectores libres como

$$\begin{array}{cccc} +: & V \times V & \to & V \\ & ([\overrightarrow{AB}], [\overrightarrow{CD}]) & \mapsto & [\overrightarrow{AB}] + [\overrightarrow{CD}] := [\overrightarrow{AB} + \overrightarrow{BD'}] \end{array} \tag{2.1}$$

donde D' es el único punto determinado por la condición $\overrightarrow{BD'} \sim \overrightarrow{CD}$ y el producto por escalares reales como

$$\begin{array}{ccc} \mathbb{R} \times V & \to & V \\ (a, [\overrightarrow{AB}]) & \mapsto & a\,[\overrightarrow{AB}] := [\overrightarrow{AB'}] \end{array} \tag{2.2}$$

siendo B' el único punto de forma que $d(A, B') = |a| d(A, B)$, la dirección de $\overrightarrow{AB'}$ es la misma de la de $\overrightarrow{AB'}$ y el sentido de $\overrightarrow{AB'}$ es el mismo del de $\overrightarrow{AB}$ cuando $a > 0$ (para los casos $a < 0, a = 0$ esta definición se extiende de la forma obvia). Es un ejercicio fácil comprobar que las operaciones anteriores están bien definidas (Ejercicio 4) y que cumplen las propiedades de un espacio vectorial.

[2] Estrictamente hablando, el sentido no se ha definido para un vector fijo del tipo $\overrightarrow{AA}$, pero este vector tiene módulo 0 y recíprocamente, cualquier vector fijo con módulo 0 es de esta forma; así que la definición de equipolencia de vectores fijos se extiende a estos vectores especiales diciendo que $\overrightarrow{AA} \sim \overrightarrow{BB}$ para cualquier par de puntos A, B.

4. **(Espacios de funciones)** El siguiente ejemplo es relevante en Análisis Matemático. Sea X un conjunto no vacío y $\mathbb{K}$ un cuerpo conmutativo. Una *función* de X en $\mathbb{K}$ es cualquier aplicación $f\colon X \to \mathbb{K}$. Representaremos por $\mathcal{F}(X,\mathbb{K})$ al conjunto de todas las funciones de X en $\mathbb{K}$. Veamos que $\mathcal{F}(X,\mathbb{K})$ admite una estructura natural de espacio vectorial sobre $\mathbb{K}$.

   Dadas $f,g \in \mathcal{F}(X,\mathbb{K})$, definimos su suma como la función $f+g\colon X \to \mathbb{K}$, $(f+g)(x) := f(x)+g(x)$, $\forall x \in X$. Dado $a \in \mathbb{K}$ y $f \in \mathcal{F}(X,\mathbb{K})$, definimos $a\,f\colon X \to \mathbb{K}$, $(a\,f)(x) := a\,f(x)$, $\forall x \in X$. Usando las propiedades de anillo unitario de $\mathbb{K}$ es fácil ver que estas operaciones hacen de $\mathcal{F}(X,\mathbb{K})$ un espacio vectorial sobre $\mathbb{K}$. El vector nulo de $\mathcal{F}(X,\mathbb{K})$ es la *función nula* $0\colon X \to \mathbb{K}$ que asocia a cada $x \in X$ el elemento $0 \in \mathbb{K}$. El vector opuesto de una función $f \in \mathcal{F}(X,\mathbb{K})$ es la función de X en $\mathbb{K}$ que asocia a cada $x \in X$ el opuesto $-f(x)$ de $f(x)$ en $\mathbb{K}$.

   En el caso particular, $\mathbb{K}=\mathbb{R}$ y $X \subset \mathbb{R}$, $\mathcal{F}(X,\mathbb{K})$ es el espacio vectorial real de todas las funciones reales de una variable real definidas en X; cuando $X=\mathbb{N}$ obtenemos el espacio vectorial real de las *sucesiones de números reales*.

5. **(Espacios de polinomios)** Un caso particular de la construcción anterior es el espacio vectorial $\mathcal{F}(\mathbb{K},\mathbb{K})$. Dentro de éste podemos considerar el subconjunto $\mathbb{K}[x]$ de polinomios

   $$p(x) = a_0 + a_1\,x + \ldots + a_n\,x^n, \qquad \forall x \in \mathbb{K}, \tag{2.3}$$

   siendo $n \in \mathbb{N} \cup \{0\}$, $a_i \in \mathbb{K}$ para cada $i=0,\ldots,n$. Es fácil comprobar que las operaciones suma y producto por escalares de $\mathcal{F}(\mathbb{K},\mathbb{K})$, se inducen de manera natural en $\mathbb{K}[x]$.

Nota 2.1.2 Un mismo grupo abeliano $(V,+)$ puede ser un espacio vectorial sobre diferentes cuerpos. Por ejemplo, $\mathbb{C}(\mathbb{C})$ es un espacio vectorial complejo, caso particular del ejemplo 1 de la sección anterior. El grupo abeliano $(\mathbb{C},+)$ también admite una estructura de espacio vectorial real $\mathbb{C}(\mathbb{R})$, de la siguiente manera. La suma de números complejos sigue siendo la misma, y el producto por escalares reales es $\colon \mathbb{R}\times\mathbb{C} \to \mathbb{C}$, que a cada $a \in \mathbb{R}$ y $z = x + y\,i \in \mathbb{C}$ le asocia $a\,z := (a\,x) + (a\,y)\,i$ (es decir, la restricción a $\mathbb{R}\times\mathbb{C}$ del producto por escalares en $\mathbb{C}(\mathbb{C})$). Con estas operaciones, $\mathbb{C}(\mathbb{R})$ es un espacio vectorial real. Sin embargo, veremos que $\mathbb{C}(\mathbb{C})$ y $\mathbb{C}(\mathbb{R})$ tienen propiedades muy distintas.

La construcción del párrafo anterior se generaliza diciendo que si $(V,+)$ es un grupo abeliano que admite una estructura de espacio vectorial complejo, entonces la restricción del producto por escalares a $\mathbb{R}$ dota a $(V,+)$ es estructura de espacio vectorial real. Análogamente, si $(V,+)$ es un grupo abeliano que admite una estructura de espacio vectorial real, entonces la restricción del producto por escalares a $\mathbb{Q}$ dota a $(V,+)$ es estructura de espacio vectorial sobre $\mathbb{Q}$.

2.2. Subespacios vectoriales

Consideraremos en adelante un espacio vectorial V.

Definición 2.2.1 Un subconjunto $U \subset V$ se dice *subespacio vectorial* de $V(\mathbb{K})$ (denotado por $U \leq V$) si con las operaciones restringidas de $(V, +, \mathbb{K})$, $(U, +, \mathbb{K})$ es un espacio vectorial. Es decir, se cumplen:

(i) $\forall u, v \in U$, $u + v \in U$, lo que produce una ley de composición interna $+ \colon U \times U \to U$.

(ii) $\forall a \in \mathbb{K}$, $\forall u \in U$, $a\, u \in U$. Así, tenemos un producto por escalares $\colon \mathbb{K} \times V \to V$.

Nota 2.2.1

1. En la definición anterior, las 4 propiedades de grupo abeliano de $(U, +)$ y las 4 propiedades del producto por escalares $\colon \mathbb{K} \times U \to U$ son automáticas al verificarse en V.

2. Si $U \leq V$, entonces el neutro de $(U, +)$ coincide con el neutro 0 de $(V, +)$, y el simétrico de un elemento de $(U, +)$ coincide con el simétrico de ese mismo elemento en $(V, +)$: Para probar que $0 \in U$, tomamos un $u \in U$ y observamos que $0 = 0\, u$ en $V(\mathbb{K})$. Usando (ii) de la Definición 2.2.1 tendremos $0 \in U$. Y si $u \in U$, el opuesto $-u$ de u en V está en U ya que $-u = (-1)\, u$.

Podemos simplificar las propiedades (i), (ii) de la definición anterior en una sola condición.

Proposición 2.2.1 *Sea $V(\mathbb{K})$ un espacio vectorial y $U \subset V$, $U \neq \varnothing$. Entonces, $U \leq V$ si y sólo si*

$$\forall a, b \in \mathbb{K}, \forall u, v \in U, \quad a\, u + b\, v \in U. \tag{2.4}$$

Demostración. Supongamos que $U \leq V$, y sean $a, b \in \mathbb{K}$, $u, v \in U$. Por la propiedad (ii) de la Definición 2.2.1, $a\, u, b\, v \in U$. Por la propiedad (i), $a\, u + b\, v \in U$.

Recíprocamente, supongamos que $\varnothing \neq U \subset V$ cumple (2.4) y probemos las propiedades (i), (ii) de la Definición 2.2.1: Para (i), sean $u, v \in U$. $u + v = 1\, u + 1\, v$ pertenece a U aplicando (2.4). Para (ii), sean $a \in \mathbb{K}$ y $u \in U$. $a\, u = a\, u + 0 = a\, u + 0\, u$ de nuevo pertenece a U aplicando (2.4). □

Nota 2.2.2 Un subespacio vectorial siempre contiene al neutro 0; en particular, en $\mathbb{R}^2(\mathbb{R})$ ninguna recta que no pase por el origen, o la la circunferencia de ecuación $x^2 + y^2 = 1$, puedes ser subespacios vectoriales.

2.2.1. Ejemplos de subespacios vectoriales

1. **(Subespacios vectoriales propios/impropios)** Todo espacio vectorial $V(\mathbb{K})$ tiene dos subespacios vectoriales especiales, $U = \{0\}$ y $U = V$. Estos subespacios se llaman *impropios*. Todo subespacio vectorial de V que no sea uno de los anteriores se dice *propio*.

2. Si $V, W \leq V$, entonces $V \cap W \leq V$ (lo mismo es cierto si cambiamos dos por cualquier número de subespacios). Esto es consecuencia inmediata de la Proposición 2.2.1.

3. **(Rectas y planos)** Usando la Proposición 2.2.1 es fácil comprobar que las rectas en $\mathbb{R}^2(\mathbb{R})$ que pasan por el origen son subespacios vectoriales. Análogamente, las rectas y planos en $\mathbb{R}^3$ que pasan por el origen son subespacios vectoriales de $\mathbb{R}^3$.

4. **(Polinomios de grado menor o igual que k)** Sea $k \in \mathbb{N} \cup \{0\}$. Dentro del espacio $\mathbb{K}[x]$ de polinomios en la variable x con coeficientes en un cuerpo $\mathbb{K}$, tenemos

$$\begin{aligned}\mathbb{K}_k[x] &:= \{p(x) \in \mathbb{K}[x] \ : \ \text{grado}(p(x)) \leq k\} \\ &= \{a_0 + a_1\, x + \ldots + a_n\, x_k \mid a_i \in \mathbb{K}, \forall\, i = 0, \ldots, k\}.\end{aligned}$$

   La Proposición 2.2.1 implica que $\mathbb{K}_k[x] \subset \mathbb{K}[x]$. Notemos que si cambiamos $\leq$ por $=$ en la definición de $\mathbb{K}_k[x]$, éste ya no es un subespacio vectorial (la suma de dos polinomios de grado k puede tener grado menor que k).

5. **(Sucesiones convergentes)** Sea $\mathcal{F}(\mathbb{N}, \mathbb{R})$ el espacio vectorial real de las sucesiones de números reales. Sea $U \subset \mathcal{F}(\mathbb{N}, \mathbb{R})$ el subconjunto formado por las sucesiones convergentes. Propiedades elementales de Analisis Matemático implican que la Proposición 2.2.1 es aplicable a U, luego $U \leq \mathcal{F}(\mathbb{N}, \mathbb{R})$.

6. **(Funciones continuas/derivables/integrables)** Sea $I \subset \mathbb{R}$ un intervalo, y $\mathcal{F}(I, \mathbb{R})$ el espacio vectorial real de las funciones $f : I \to \mathbb{R}$. Dentro de $\mathcal{F}(I, \mathbb{R})$ consideramos los subconjuntos

$$\begin{array}{ll}\mathcal{C}(I, \mathbb{R}) & := \{f \in \mathcal{F}(I, \mathbb{R}) \mid f \text{ es continua}\}, \\ \mathcal{D}(I, \mathbb{R}) & := \{f \in \mathcal{F}(I, \mathbb{R}) \mid f \text{ es derivable}\}, \\ \mathcal{I}(I, \mathbb{R}) & := \{f \in \mathcal{F}(I, \mathbb{R}) \mid f \text{ es integrable}\},\end{array}$$

   donde en el segundo ejemplo $I = (a, b)$ y en el tercero $I = [a, b]$. De nuevo propiedades elementales de Analisis Matemático implican Proposición 2.2.1 es aplicable a $\mathcal{C}(I, \mathbb{R}), \mathcal{D}(I, \mathbb{R}), \mathcal{I}(I, \mathbb{R})$ por lo que éstos son subespacios vectoriales de $\mathcal{F}(I, \mathbb{R})$. De hecho, si $I = (a, b)$ entonces $\mathcal{D}(I, \mathbb{R}) \leq \mathcal{C}(I, \mathbb{R})$ y si $I = [a, b]$ entonces $\mathcal{C}(I, \mathbb{R}) \leq \mathcal{I}(I, \mathbb{R})$.

7. **(Matrices simétricas/antisimétricas)** Por la Definición 1.1.1, la trasposición de matrices puede verse como una aplicación
$$^t\colon \mathcal{M}_{m\times n}(\mathbb{K}) \to \mathcal{M}_{n\times m}(\mathbb{K}), \qquad A \mapsto A^t.$$
que cumple las siguientes propiedades (Proposición 1.1.1):
   1) $(A+B)^t = A^t + B^t$, $\forall A, B \in \mathcal{M}_{m\times n}(\mathbb{K})$,
   2) $(a\,A)^t = a\,A^t$, $\forall a \in \mathbb{K}$, $\forall A \in \mathcal{M}_{m\times n}(\mathbb{K})$,
   3) $(A^t)^t = A$, $\forall A \in \mathcal{M}_{m\times n}(\mathbb{K})$.

   Si nos restringimos al caso $n = m$ de matrices cuadradas de orden n, la trasposición va de $\mathcal{M}_n(\mathbb{K})$ en sí mismo y tiene cuadrado identidad[3].

   Una matriz $A = (a_{ij})_{i,j} \in \mathcal{M}_n(\mathbb{K})$ se dice *simétrica* (resp. *antisimétrica*) si $A^t = A$ (resp. $A^t = -A$). Al conjunto de matrices simétricas (resp. antisimétricas) se le denota por $\mathcal{S}_n(\mathbb{K})$ (resp. $\mathcal{A}_n(\mathbb{K})$). Por ejemplo, $0_n \in \mathcal{S}_n(\mathbb{K}) \cap \mathcal{A}_n(\mathbb{K})$. Toda matriz diagonal $A = (a_{ij})_{i,j} \in \mathcal{M}_n(\mathbb{K})$ (esto es, $a_{ij} = 0\ \forall i \neq j$) es simétrica, en particular $I_n \in \mathcal{S}_n(\mathbb{K})$. Si $A \in \mathcal{A}_n(\mathbb{K})$, entonces $a_{ii} = 0\ \forall i = 1, \ldots, n$ (estamos suponiendo que $\mathbb{K}$ tiene característica distinta de 2). Usando la Proposición 2.2.1, es fácil probar que $\mathcal{S}_n(\mathbb{K}), \mathcal{A}_n(\mathbb{K}) \leq \mathcal{M}_n(\mathbb{K})$.

8. **(Soluciones de un SEL homogéneo)** Consideremos un SEL de m ecuaciones y n incógnitas con coeficientes en un cuerpo $\mathbb{K}$:
$$\left\{\begin{array}{ccccccccc} a_{11}\,x_1 & + & a_{12}\,x_2 & + & \ldots & + & a_{1n}\,x_n & = & b_1 \\ a_{21}\,x_1 & + & a_{22}\,x_2 & + & \ldots & + & a_{2n}\,x_n & = & b_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{m1}\,x_1 & + & a_{m2}\,x_2 & + & \ldots & + & a_{mn}\,x_n & = & b_m \end{array}\right.$$
Sea U el subconjunto de $\mathbb{K}^n$ formado por todas las soluciones del SEL. Una condición necesaria para que U sea un subespacio vectorial de $\mathbb{K}^n$ es que $(0, \ldots, 0) \in U$. Si esto último ocurre, entonces el SEL es homogéneo. Recíprocamente, la Proposición 2.2.1 implica que el conjunto de soluciones de un SEL homogéneo es un subespacio vectorial de $\mathbb{K}^n$. Volveremos a esto cuando hablemos de las ecuaciones cartesianas de un subespacio vectorial de $\mathbb{K}^n$.

Nota 2.2.3 El cuerpo base influye en qué subconjuntos son subespacios vectoriales: recordemos que $(\mathbb{C}, +)$ admite dos estructuras de espacio vectorial, $\mathbb{C}(\mathbb{C})$ y $\mathbb{C}(\mathbb{R})$. Sea $U = \{b\,i \mid b \in \mathbb{R}\}$ el subconjunto de números complejos imaginarios puros. Usando la Proposición 2.2.1 se prueba fácilmente que $U \leq \mathbb{C}(\mathbb{R})$. Pero U no es subespacio vectorial de $\mathbb{C}(\mathbb{C})$: si lo fuera, se debería cumplir $a\,u \in U\ \forall u \in U$ y $\forall a \in \mathbb{C}$. Esto falla tomando $a = i \in \mathbb{C}$, $u = i \in U$.

[3] A una aplicación que al componerla consigo misma produzca la identidad se la llama *involución*.

2.2.2. Subespacio generado por una familia de vectores

Todo subespacio vectorial se pueden escribir a partir de unos pocos de sus vectores (cuantos menos mejor). Por ejemplo, en $\mathbb{R}^3$ consideramos el subconjunto

$$U = \{(x, y, z) \in \mathbb{R}^3 \mid x - 2y + 3z = 0\}.$$

Como U es el conjunto de soluciones de un SEL homogéneo, $U \leq \mathbb{R}^3$ (gráficamente, U un plano en $\mathbb{R}^3$ que pasa por el origen). Todos los elementos de U se pueden escribir en combinación lineal de dos de ellos: si $y = \lambda$ y $z = \mu$, entonces $x = 2\lambda - 3\mu$ luego

$$U = \{(2\lambda - 3\mu, \lambda, \mu) \in \mathbb{R}^3 \mid \lambda, \mu \in \mathbb{R}\} = \{\lambda(2, 1, 0) + \mu(-3, 0, 1) \mid \lambda, \mu \in \mathbb{R}\},$$

luego usando solo los vectores $(2, 1, 0)$ y $(-3, 0, 1)$ podemos generar todos los demás vectores de U. En este sentido decimos que U es el subespacio vectorial generado por $(2, 1, 0)$ y $(-3, 0, 1)$. Generalizamos esto a continuación.

Definición 2.2.2 Sea $V(\mathbb{K})$ un espacio vectorial y $\varnothing \neq H = \{v_1, \ldots, v_m\} \subset V$. Una *combinación lineal* de H es cualquier vector de V de la forma $a_1\, v_1 + \ldots + a_m\, v_m$, donde $a_i \in \mathbb{K}\ \forall i = 1, \ldots, m$. Denotaremos $L(H)$ al subconjunto de V formado por las combinaciones lineales de elementos de H.

Si $H \subset V$ es un subconjunto infinito, denotaremos por $L(H)$ al subconjunto de V formado por todas las *combinaciones lineales finitas* de vectores de H:

$$L(H) = \{a_1\, v_1 + \ldots + a_m\, v_m \mid m \in \mathbb{N}, v_i \in H, a_i \in \mathbb{K}, \forall i = 1, \ldots, m\}.$$

Proposición 2.2.2 *prop:eles Sea $V(\mathbb{K})$ un espacio vectorial. Entonces:*

1. *$\forall H \subset V$ no vacío, $L(H) \leq V$.*
2. *$L(H)$ es el menor subespacio vectorial de V que contiene a H.*
3. *Si $H' \subset H$, $H' \neq \varnothing$, entonces $L(H') \leq L(H)$.*

Demostración. El apartado 1 es consecuencia directa de la Proposición 2.2.1.

Que $H \subset L(H)$ se deduce de que dado $v \in H$, v se escribe como la combinación lineal $a\, v$ con $a = 1$ (si H fuera finito, pondremos coeficiente cero a todos los vectores de $H \setminus \{v\}$). Para ver la propiedad de "menor" del apartado 2, supongamos que $U \leq V$ contiene a H. Dados $v_1, \ldots v_m \in H$ y $a_1, \ldots, a_m \in \mathbb{K}$, se tiene que $v_1, \ldots v_m \in U$ porque $H \subset U$ y como $U \leq V$, la Proposición 2.2.1 implica que $a_1 v_1 + \ldots + a_m v_m \in U$. Así que todo elemento de $L(H)$ está en U, es decir, $L(H) \subset U$.

El apartado 3 es trivial si H es infinito. Y si H es finito, se deduce de que toda combinación lineal de vectores de H' puede verse como combinación lineal de vectores de H poniendo coeficiente cero a todos los vectores de $H \setminus H'$. $\square$

Nota 2.2.4 EL apartado 2 permite redefinir $L(H)$ como el menor subespacio vectorial de V que contiene a H, independientemente de si H es finito o no.

Ejemplo 2.2.1 Para $H = \{v\}$ a $L(\{v\})$ se le denotará también $L(v)$. Cuando $v = 0$ se tiene $L(0) = \{0\}$; y si $v \neq 0$ a $L(v)$ se le llama *recta vectorial de V generada por v.*

2.2.3. Operaciones con subespacios vectoriales

Vimos en el apartado 2 de ejemplos de subespacios vectoriales que la intersección de dos subespacios vectoriales de un espacio vectorial vuelve a ser un subespacio vectorial. Además, es trivial comprobar que $U \cap W$ es el mayor subespacio vectorial de V que está contenido a la vez en U y en W (de nuevo esto es generalizable a cualquier número de subespacios).

Sin embargo, la unión de dos subespacios vectoriales no tiene porqué ser subespacio vectorial. Por ejemplo, cada eje de coordenadas es un subespacio vectorial de $\mathbb{R}^2$ (porque son rectas que pasan por el origen), pero la unión de los dos ejes no es subespacio vectorial de $\mathbb{R}^2$ porque si tomamos $u \neq 0$ en el eje de abscisas y $v \neq 0$ en el eje de ordenadas, la suma $u + v$ no está en la unión de ambos ejes.

El problema anterior dado por la unión de subespacios se solventa sustituyendo la unión por la suma:

Definición 2.2.3 Sea $V(\mathbb{K})$ un espacio vectorial y $U_1, \ldots, U_m \leq V$. Definimos

$$U_1 + \ldots + U_m = \{x_1 + \ldots x_m \mid x_i \in U_i, \ \forall i = 1, \ldots, m\}.$$

Proposición 2.2.3 *Sea $V(\mathbb{K})$ un espacio vectorial y $U_1, \ldots, U_m \leq V$. Entonces, $U_1 + \ldots + U_m$ es el menor subespacio vectorial de V que contiene a todos los U_i, $i = 1, \ldots, m$.*

Demostración. Que $U_1 + \ldots + U_m \leq V$ es consecuencia directa de la Proposición 2.2.1. Para ver la propiedad de "menor", sea $W \leq V$ tal que $U_i \subset W$ para cada $i = 1, \ldots, m$. Dado $x \in U_1 + \ldots + U_m$, existen $x_i \in U_i$ para cada $i = 1, \ldots, m$ tales que $x = x_1 + \ldots + x_m$. Como $x_i \in U_i \subset W$ y W es cerrado para las sumas, concluimos que $x \in W$. □

Nota 2.2.5 La definición y propiedades de la suma de una familia finita de subespacios vectoriales se extiende a cualquier familia (no necesariamente finita) de subespacios sin más que tener en cuenta que las sumas que se hagan de elementos serán siempre finitas.

Ejemplo 2.2.2 En $\mathbb{R}^3$ si tomamos como U_1 y U_2 dos ejes coordenados, entonces $U_1 + U_2$ es el plano vectorial que los contiene.

Lema 2.2.1 *Sea $V(\mathbb{K})$ un espacio vectorial y si $H_1, \ldots, H_m \subset V$. Entonces, $L(H_1 \cup \ldots H_m) = L(H_1) + \ldots + L(H_m)$.*

Demostración. Como $L(H_1 \cup \ldots \cup H_m)$ es el menor subespacio vectorial de V que contiene a $H_1 \cup \ldots \cup H_m$, si vemos que $L(H_1) + \ldots + L(H_m)$ contiene a $H_1 \cup \ldots \cup H_m$ tendremos probado que $L(H_1 \cup \ldots \cup H_m) \subseteq L(H_1) + \ldots + L(H_m)$. Pero $H_i \subset L(H_i) \subset L(H_1) + \ldots + L(H_m)$ para cada i, luego $H_1 \cup \ldots \cup H_m \subset L(H_1) + \ldots + L(H_m)$.

Como $L(H_1) + \ldots + L(H_m)$ es el menor subespacio vectorial de V que contiene a cada $L(H_i)$, si vemos que $L(H_1 \cup \ldots \cup H_m)$ contiene a cada $L(H_i)$ tendremos probado que $L(H_1) + \ldots + L(H_m) \subseteq L(H_1 \cup \ldots \cup H_m)$. Pero $H_i \subset H_1 \cup \ldots \cup H_m$ luego $L(H_i) \subset L(H_1 \cup \ldots \cup H_m)$. $\square$

Sea $V(\mathbb{K})$ un espacio vectorial y $U_1, \ldots, U_m \leq V$. Dado $x \in \sum_{i=1}^m U_i$, sabemos que $x = x_1 + \ldots + x_m$ donde $x_i \in U_i$ $\forall i = 1, \ldots, m$. Esta forma de expresar x como suma de vectores en cada U_i no tiene por qué ser única. Veamos esto con un ejemplo.

Ejemplo 2.2.3 Sean

$$U_1 = \{(x, y, z) \in \mathbb{R}^3 \mid x = 0\}, \qquad U_2 = \{(x, y, z) \in \mathbb{R}^3 \mid z = 0\}.$$

Todo vector $v = (x, y, z)$ de $\mathbb{R}^3$ se puede expresar como $u_1 + u_2$, donde $u_1 = (0, y, z) \in U_1$ y $u_2 = (x, 0, 0) \in U_2$. Por tanto, $U_1 + U_2 = \mathbb{R}^3$. Sin embargo, $(0, 0, 0) = (0, 1, 0) + (0, -1, 0)$ y también $(0, 0, 0) = (0, 2, 0) + (0, -2, 0)$ son descomposiciones distintas de $(0, 0, 0)$ como suma de un primer sumando en U_1 y un segundo en U_2. De hecho, $(0, 0, 0) = (0, a, 0) + (0, -a, 0)$, para cada $a \in \mathbb{R}$.

¿Bajo qué condiciones la expresión de $x \in \sum_{i=1}^m U_i$ como suma de vectores $x_i \in U_i$ es única?

Proposición 2.2.4 *Sea $V(\mathbb{K})$ un espacio vectorial y $U_1, \ldots, U_m \leq V$, $m \geq 2$. Entonces, son equivalentes:*

1. *Para cada $x \in U_1 + \ldots + U_m$, $\exists! x_i \in U_i$, $i = 1, \ldots, m$, tales que $x = x_1 + \ldots + x_m$.*
2. *$\forall j = 1, \ldots, m-1$, $(U_1 + \ldots + U_j) \cap U_{j+1} = \{0\}$.*

Demostración. Primero veremos la demostración en el caso $m = 2$. En este caso, la afirmación 2 se reduce a la igualdad $U_1 \cap U_2 = \{0\}$.

$\boxed{1 \Rightarrow 2}$. Sea $x \in U_1 \cap U_2$. Como $x = x + 0$, $x = 0 + x$ son dos descomposiciones de x en sumandos en U_1 y U_2, la unicidad de 1 implica $x = 0$.

$\boxed{2 \Rightarrow 1}$ Sea $x \in U_1 + U_2$ y supongamos que $x = x_1 + x_2 = x_1' + x_2'$ siendo $x_1, x_1' \in U_1$, $x_2, x_2' \in U_2$. Como $x_1 + x_2 = x_1' + x_2'$, tenemos $v := x_1' - x_1 = x_2 - x_2'$. Como U_1 es un subespacio vectorial y $x_1, x_1' \in U_1$, concluimos que $v \in U_1$. Análogamente, $v \in U_2$ y por tanto $v \in U_1 \cap U_2$. Como $U_1 \cap U_2 = \{0\}$ por la afirmación 2, deducimos que $v = 0$. Esto nos dice que $u_1 = u_1'$ y $u_2 = u_2'$.

Ahora probaremos la proposición en el caso m general.

$\boxed{1 \Rightarrow 2}$. Fijamos $j \in \{1, \ldots, m-1\}$, y sea $x \in (U_1 + \ldots + U_j) \cap U_{j+1} = \{0\}$. Como $x \in U_1 + \ldots + U_j$, existen $u_i \in U_i$, $i = 1, \ldots, j$, tales que $x = x_1 + \ldots + x_j$. Ahora escribimos x de dos formas distintas como suma de vectores de U_i

$$x = x_1 + \ldots + x_j + 0_{j+1} + 0_{j+2} + \ldots + 0_m, \qquad x = 0_1 + \ldots + 0_j + x + 0_{j+2} + \ldots + 0_m.$$

Por la hipótesis 1, todos los vectores de las expresiones anteriores son nulos. En particular, $x = 0$, luego se tiene 2.

$\boxed{2 \Rightarrow 1}$. El argumento es por inducción sobre el número de m de sumandos. El resultado ya ha sido demostrado para $m = 2$ (y es trivial para $m = 1$). Supongamos como hipótesis de inducción que la implicación $\boxed{2 \Rightarrow 1}$ es cierta para $m - 1$ sumandos, y veámosla para m sumandos. Sea $x \in U_1 + \ldots + U_m$; supongamos que para cada $i = 1, \ldots, m$, existen $x_i, x_i' \in U_i$ tales que

$$x = x_1 + \ldots + x_m = x_1' + \ldots + x_m'.$$

Queremos ver que $x_i' = x_i$ para cada $i = 1, \ldots, m$. Tenemos

$$v := (x_1 - x_1') + \ldots + (x_{m-1} - x_{m-1}') = x_m' - x_m.$$

Entonces, $v \in U_1 + \ldots + U_{m-1}$ (por la primera expresión de v) y $v \in U_m$ (por la segunda). Aplicando la hipótesis 2 con $j = m - 1$ se deduce que $v = 0$. Esto implica que $x_m' = x_m$ y $(x_1 - x_1') + \ldots + (x_{m-1} - x_{m-1}') = 0$. Esta última igualdad supone escribir el vector 0 como suma de vectores pertenecientes a U_i con $i = 1, \ldots, m-1$. Por la hipótesis de inducción aplicada a $U_1, \ldots, U_{m-1}$ (que trivialmente satisfacen 2) concluimos que cada paréntesis en $(x_1 - x_1') + \ldots + (x_{m-1} - x_{m-1}')$ es cero, que es lo que faltaba por probar. $\square$

Nota 2.2.6 Una consecuencia inmediata de la Proposición 2.2.4 es que la condición 2 es independiente de la ordenación de los subespacios U_i (porque es equivalente a 1).

Definición 2.2.4 Sea $V(\mathbb{K})$ un espacio vectorial y $U_1, \ldots, U_m \leq V$. Diremos que la suma $U_1 + \ldots + U_m$ es *directa* si se verifican las condiciones equivalentes de la Proposición 2.2.4. En este caso, denotaremos al subespacio suma por $U_1 \oplus \ldots \oplus U_m$.

En el caso $V = U_1 \oplus \ldots \oplus U_m$, diremos que V es *suma directa* de $U_1, \ldots, U_m$.

En el caso $m = 2$, la expresión $U = U_1 \oplus U_2$ significa que $U = U_1 + U_2$ y $U_1 \cap U_2 = \{0\}$. En este caso, diremos que U_2 es un subespacio *suplementario* de U_1 en U, y viceversa.

Ejemplo 2.2.4 En el Ejemplo 2.2.3 teníamos $\mathbb{R}^3 = U_1 + U_2$. Sin embargo, no es cierto que $\mathbb{R}^3 = U_1 \oplus U_2$, porque vimos que el vector nulo se expresa de varias formas distintas como suma de un vector de U_1 y otro de U_2. Por otro lado, se tiene que $U_1 \cap U_2 \neq \{0\}$, porque $(0, 1, 0) \in U_1 \cap U_2$.

Ejemplo 2.2.5 Suma directa de matrices simétricas y antisimétricas. Sea $n \in \mathbb{N}$ y $\mathbb{K}$ un cuerpo conmutativo con característica distinta de 2. Veamos que

$$\mathcal{M}_n(\mathbb{K}) = \mathcal{S}_n(\mathbb{K}) \oplus \mathcal{M}_n(\mathbb{K}).$$

Primero veamos que $\mathcal{M}_n(\mathbb{K}) = \mathcal{S}_n(\mathbb{K}) + \mathcal{A}_n(\mathbb{K})$. La inclusión $\mathcal{S}_n(\mathbb{K}) + \mathcal{A}_n(\mathbb{K}) \subset \mathcal{M}_n(\mathbb{K})$ es trivial. Para ver la inclusión contraria, descomponemos cada $A \in \mathcal{M}_n(\mathbb{K})$ como

$$A = \frac{1}{2}(A + A^t) + \frac{1}{2}(A - A^t).$$

(en la igualdad anterior el símbolo $1/2$ representa el inverso de 2 en $\mathbb{K}$, que existe ya que $2 \neq 0$). Llamamos $B = (1/2)(A + A^t)$ y $C = (1/2)(A - A^t)$, luego $A = B + C$. Veamos que $B \in \mathcal{S}_n(\mathbb{K})$ y $C \in \mathcal{A}_n(\mathbb{K})$:

$$\begin{aligned} B^t &= \frac{1}{2}(A + A^t)^t = \frac{1}{2}\left(A^t + (A^t)^t\right) = \frac{1}{2}(A^t + A) = B \ \Rightarrow\ B \in \mathcal{S}_n(\mathbb{K}), \\ C^t &= \frac{1}{2}(A - A^t)^t = \frac{1}{2}\left(A^t - (A^t)^t\right) = \frac{1}{2}(A^t - A) = -C \ \Rightarrow\ C \in \mathcal{A}_n(\mathbb{K}). \end{aligned}$$

Por último, comprobemos que $\mathcal{S}_n(\mathbb{K}) \cap \mathcal{A}_n(\mathbb{K}) = \{0_n\}$. Sea $A \in \mathcal{S}_n(\mathbb{K}) \cap \mathcal{A}_n(\mathbb{K})$. Como $A \in \mathcal{S}_n(\mathbb{K})$, entonces $A^t = A$. Y como $A \in \mathcal{A}_n(\mathbb{K})$ tenemos $A^t = -A$. Por tanto, $A = -A$ luego $2A = 0_n$ y como $2 \neq 0$, llegamos a $A = 0_n$.

2.3. Espacio vectorial cociente

Sea $V(\mathbb{K})$ un espacio vectorial y $U \leq V$ un subespacio vectorial Definimos una relación binaria $\sim$ en V: dados $u, v \in V$,

$$v \sim w \iff v - w \in U. \tag{2.5}$$

Esta relación es de equivalencia, ya que

- Propiedad reflexiva: como $v - v = 0 \in U$, se tiene $v \sim v$, $\forall v \in V$.
- Propiedad simétrica: si $v \sim w$ entonces $v - w \in U$ y al ser $U \leq V$, tenemos $w - v = -(v - w) \in U$, luego $w \sim v$.
- Propiedad transitiva: si $v \sim v'$ y $v' \sim v''$ entonces $v - v' \in U$ y $v' - v'' \in U$. Por ser $U \leq V$, tenemos $v - v'' = (v - v') + (v' - v'') \in U$ y así, $v \sim v''$.

Para cada $v \in V$, su clase de equivalencia $[v]$ es

$$v + U := [v] = \{v + u \mid u \in U\}.$$

Para demostrar $[v] \subset \{v+u : u \in U\}$, observemos que si $v' \in [v]$ entonces $u := v' - v \in U$ por lo que $v' = v+u$ para un $u \in U$. Para la inclusión contraria, como $(v+u)-v = u \in U$, las clases de $v+u$ y v coinciden, esto es, $v+u \in [v]$.

Al conjunto cociente $V/\sim$ lo denotaremos V/U.

Nos podemos preguntar si V/U hereda una estructura de espacio vectorial de V. Definimos

$$(2.6)\qquad \begin{array}{rccc} +: & V/U \times V/U & \to & V/U \\ & (v+U, w+U) & \mapsto & (v+w)+U \end{array} \qquad \begin{array}{rccc} : & \mathbb{K} \times V/U & \to & V/U \\ & (a, v+U) & \mapsto & (a\,v)+U \end{array}$$

Esta definición depende en principio de la elección de representantes v y w en cada clase. El siguiente lema nos dice que las aplicaciones anteriores están bien definidas.

Lema 2.3.1 *Sean $V(\mathbb{K})$ un espacio vectorial y $U \leq V$. Supongamos que $v, v', w, w' \in V$ cumplen $v+U = v'+U$, $w+U = w'+U$. Entonces,*

$$(v+w)+U = (v'+w')+U \qquad y \qquad (a\,v)+U = (a\,v')+U.$$

Demostración. Por hipótesis, $v-v' \in U, w-w' \in U$. Por ser $U \leq V$, $(v+w)-(v'+w') = (v-v')+(w-w') \in U$, $a\,v - a\,v' = a\,(v-v') \in U$. □

Proposición 2.3.1 *Sean $V(\mathbb{K})$ un espacio vectorial y $U \leq V$. Con las operaciones de* (2.6)*, $(V/U, +, \mathbb{K})$ es un espacio vectorial, llamado* espacio cociente *de V sobre U.*

Demostración. Tenemos que comprobar las 8 propiedades de espacio vectorial; cada una de ellas es un cálculo directo aplicando las definiciones de las operaciones y las propiedades de espacio vectorial de $V(\mathbb{K})$. Lo hacemos sólo para una de ellas y el resto se deja como ejercicio (Ejercicio 31):

$$\begin{aligned} a\ ((v+U)+(w+U)) = &\ a\ ((v+w)+U) = (a\,(v+w))+U = ((a\,v)+(a\,w))+U \\ = &\ ((a\,v)+U)+((a\,w)+U) = a\ (v+U)+a\ (w+U) \end{aligned}$$

donde en las igualdades de la primera línea se usan, por orden, la definición de la suma en V/U, la del producto por escalares en V/U y la propiedad distributiva del producto por escalares en V, mientras que en la segunda se usan la definición de la suma en V/U y la del producto por escalares en V/U. □

2.4. Sistemas de generadores

Definición 2.4.1 Sea $V(\mathbb{K})$ un espacio vectorial. Un subconjunto $\varnothing \neq H \subset V$ se dice *sistema de generadores* de V si $V = L(H)$. Esto equivale a que todo vector de V se escribe como combinación lineal finita de vectores de H.

Como $V = L(V)$, V es un sistema de generadores de V. Y si $H \subset H' \subset V$ y H es sistema de generadores, entonces H' también lo es. Pero queremos generar todos los vectores de V a partir de la *menor* cantidad posible de vectores.

Definición 2.4.2 Un espacio vectorial $V(\mathbb{K})$ se dice *finitamente generado* si admite un sistema de generadores con un número finito de vectores.

Ejemplo 2.4.1 (A) En $\mathbb{R}^2$, el conjunto $H = \{v_1 = (1,0), v_2 = (1,1)\}$ es un sistema de generadores. Para ver esto, sea $v = (x,y) \in \mathbb{R}^2$. Buscamos $a, b \in \mathbb{R}$ tales que $v = a\,v_1 + b\,v_2$. Tomando componentes y operando esta igualdad tenemos $(x,y) = (a+b, b)$. Por tanto, llegamos al SEL dado por $a+b = x$, $b = y$, que es compatible determinado con soluciones $b = y$, $a = x - y$. Por tanto, H es un sistema de generadores de $\mathbb{R}^2$ y $\mathbb{R}^2(\mathbb{R})$ es finitamente generado.

(B) En $\mathbb{R}^2$, el conjunto $H = \{v_1, v_2, v_3\}$ con $v_1 = (1,2)$, $v_2 = (2,4)$ y $v_3 = (3,6)$ no es sistema de generadores. Para verlo, buscamos $v = (x,y) \in \mathbb{R}^2$ que no se escriba como combinación lineal de H, es decir, que no existan $a, b, c \in \mathbb{R}$ tales que $v = a\,v_1 + b\,v_2 + c\,v_3$. Tomando componentes y operando, esto equivale a que $(x,y) = (a + 2b + 3c, 2a + 4b + 6c)$. Llegamos así al SEL $a+2b+3c = x$, $2a+4b+6c = y$. Claramente, este SEL es compatible si y sólo si $2x = y$. Por tanto, tomando $v = (x,y) \in \mathbb{R}^2$ que no cumpla que $2x = y$ (por ejemplo, $v = (0,1)$) concluimos que v no es combinación lineal de H.

(C) Consideremos $\mathbb{K}^n$ como espacio vectorial sobre $\mathbb{K}$, con $n \in \mathbb{N}$. Para cada $i \in \{1, \ldots, n\}$ definimos $e_i = (0, 0, \ldots, 1, \ldots, 0, 0)$, donde el 1 se encuentra en la i-ésima posición. Entonces, $H = \{e_1, \ldots, e_n\}$ es un sistema de generadores de $\mathbb{K}^n$ ya que todo vector $x = (x_1, \ldots, x_i, \ldots, x_n) \in \mathbb{K}^n$ se escribe como $x_1\,e_1 + \ldots + x_i\,e_i + \ldots + x_n\,e_n$, en combinación lineal de H (los coeficientes de la combinación coinciden con las componentes de x). En particular, $\mathbb{K}^n(\mathbb{K})$ es finitamente generado.

(D) Para $\mathbb{K} = \mathbb{R}$ ó $\mathbb{C}$, el espacio de polinomios $\mathbb{K}[x]$ con coeficientes en $\mathbb{K}$ no es finitamente generado: si lo fuera, existiría un sistema de generadores finito $H \subset \mathbb{K}[x]$. Sea k el máximo grado de los polinomios en H (que existe, por ser H finito). Entonces, ningún polinomio de grado $k+1$ está en $L(H)$ luego H no puede ser sistema de generadores de $\mathbb{R}[x]$, contradicción. Un sistema de generadores de $\mathbb{K}[x]$ es

$$H_0 = \{p_i(x) = x^i \mid i \in \mathbb{N} \cup \{0\}\}.$$

Esto es cierto porque todo polinomio $p(x) = a_0 + a_1\,x + \ldots + a_n\,x^n \in \mathbb{K}[x]$ se escribe como combinación lineal finita $a_0\,p_0(x) + a_1\,p_1(x) + \ldots + a_n\,p_n(x)$ de elementos de H_0.

(E) Sean $m, n \in \mathbb{N}$ y $\mathbb{K}$ un cuerpo. Consideremos $\mathcal{M}_{m\times n}(\mathbb{K})$ como espacio vectorial sobre $\mathbb{K}$. Generalizando el ejemplo (C), para cada $i \in \{1, \ldots, m\}$ y $j \in \{1, \ldots, n\}$, definimos la matriz
$$E_{ij} = (e_{kl})_{k,l} = (\delta_{ik}\, \delta_{jl})_{k,l} \in \mathcal{M}_{m\times n}(\mathbb{K}).$$
Entonces, el conjunto $H = \{E_{ij} \mid i = 1, \ldots, m,\ j = 1, \ldots, n\}$ es un sistema de generadores de $\mathcal{M}_{m\times n}(\mathbb{K})$, ya que toda matriz $A = (a_{ij})_{i,j} \in \mathcal{M}_{m\times n}(\mathbb{K})$ se expresa como
$$A = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}\, E_{ij},$$
en combinación lineal de H (los coeficientes de la combinación coinciden son las entradas de A). Así, $\mathcal{M}_{m\times n}(\mathbb{K})$ es finitamente generado.

(F) En el espacio vectorial real $\mathcal{F}(\mathbb{R}, \mathbb{R})$ de las funciones $f\colon \mathbb{R} \to \mathbb{R}$, definimos el subconjunto
$$U = \{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \mid \exists f', f'' \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \text{ y } f''(x) + f(x) = 0\ \forall x \in \mathbb{R}\}$$
Usando la Proposición 2.2.1 es fácil probar que $U \leq \mathcal{F}(\mathbb{R}, \mathbb{R})$. Derivando dos veces las funciones $\operatorname{sen} x$ y $\cos x$ se comprueba que ambas están en U. Veamos que $H = \{\operatorname{sen} x, \cos x\}$ es un sistema de generadores de U (en particular, U es finitamente generado): dada $f \in U$, aplicando resultados de ecuaciones diferenciales se prueba que dado $b > 0$, la restricción de f a $[0, b]$ está determinada unívocamente por los valores $f(0), f'(0)$. Esto nos dice que tanto f como $h(x) = f'(0)\operatorname{sen} x + f(0)\cos x$ son soluciones de la ecuación diferencial que define a U, y $f(0) = h(0)$, $f'(0) = h'(0)$. Por tanto, $f = h$ en $[0, b]$. como $b > 0$ es arbitrario, $f = h$ en $[0, \infty)$. El mismo razonamiento puede aplicarse en intervalos de la forma $[a, 0]$ con $a < 0$, con lo que deducimos que $f = h$ en todo $\mathbb{R}$. Esto es, f es combinación lineal (como elemento de U de H. En particular, U es finitamente generado como espacio vectorial real.

(G) Como en otros conceptos, el cuerpo base juega un papel crucial en los sistemas de generadores y en ser finitamente generado. Para ver esto, pensemos en $\mathbb{C}(\mathbb{C})$, que tiene a $\{1\}$ como sistema de generadores (ejemplo (C) con $\mathbb{K} = \mathbb{C}$ y $n = 1$). Sin embargo, $\{1\}$ no es un sistema de generadores de $\mathbb{C}(\mathbb{R})$ porque ningún número imaginario puro se escribe como $a\,1$ con $a \in \mathbb{R}$ (de hecho, $L(S) = \mathbb{R}$ en $\mathbb{C}(\mathbb{R})$). Por otro lado, $\mathbb{R}(\mathbb{R})$ es finitamente generado (ejemplo (C) con $\mathbb{K} = \mathbb{R}$ y $n = 1$), pero $\mathbb{R}(\mathbb{Q})$ no lo es (Ejercicio 38).

Ya hemos comentado que un objetivo es dado un espacio vectorial $V(\mathbb{K})$, encontrar un sistema de generadores "lo más pequeño posible". Asociado a esto tenemos una cuestión natural:

Si $V(\mathbb{K})$ es un espacio vectorial finitamente generado, ¿cuál es el menor número de vectores que puede tener un sistema de generadores?

De alguna forma, podemos ver el número mínimo de vectores de un sistema de generadores de $V(\mathbb{K})$ como una medida del "tamaño" del espacio vectorial (esto se precisará con el concepto de dimensión).

Para empezar a aclarar la cuestión anterior, nos planteamos cuándo es posible suprimir de un sistema de generadores algún vector de forma que el resultado siga siendo un sistema de generadores.

Proposición 2.4.1 *Sea $V(\mathbb{K})$ un espacio vectorial sobre un cuerpo $\mathbb{K}$, y $H = \{v_1, \ldots, v_m\}$ un sistema de generadores de V.*

1. *Si $H' \subset V$ y $H \subset H'$, entonces H' es un sistema de generadores de V.*
2. *Si $m \geq 2$ y $\exists i \in \{1, \ldots, m\}$ tal que $v_i \in L(H \setminus \{v_i\})$, entonces $H \setminus \{v_i\}$ es un sistema de generadores de V.*

Demostración. Para el apartado 1, como H es sistema de generadores de V tenemos $V = L(H)$. De $H \subset H'$ deducimos que $L(H) \subset L(H')$ y por tanto $V \subset L(H')$, luego $V = L(H')$ y H' es un sistema de generadores.

Para el apartado 2, sea $v \in V$. Queremos ver que v se expresa como combinación lineal de $H \setminus \{v_i\}$. Por un lado, como H es un sistema de generadores de V, existen $a_1, \ldots, a_m \in \mathbb{K}$ tales que $v = a_1 v_1 + \ldots + a_{i-1} v_{i-1} + a_i v_i + a_{i+1} v_{i+1} + \ldots + a_m v_m$. Como $v_i \in L(H \setminus \{v_i\})$, entonces existen $b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_m \in \mathbb{K}$ tales que $v_i = b_1 v_1 + \ldots + b_{i-1} v_{i-1} + b_{i+1} v_{i+1} + \ldots + b_m v_m$. Sustituyendo la última igualdad en la primera y reordenando llegamos a

$$\begin{aligned}
v &= a_1 v_1 + \ldots + a_{i-1} v_{i-1} \\
&\quad + a_i (b_1 v_1 + \ldots + b_{i-1} v_{i-1} + b_{i+1} v_{i+1} + \ldots + b_m v_m) \\
&\quad + a_{i+1} v_{i+1} + \ldots + a_m v_m \\
&= (a_1 + a_i b_1) v_1 + \ldots + (a_{i-1} + a_i b_{i-1}) v_{i-1} \\
&\quad + (a_{i+1} + a_i b_{i+1}) v_{i+1} + \ldots + (a_m + a_i b_m) v_m,
\end{aligned}$$

luego $v \in L(H \setminus \{v_i\})$. □

El apartado 2 de la Proposición 2.4.1 nos dice que si un sistema de generadores tiene vectores que se escriben como combinación lineal de los demás, entonces estos vectores se pueden eliminar para obtener un sistema de generadores más pequeño. ¿Hasta dónde podemos llegar con esta reducción?

2.5. Dependencia e independencia lineal

Lema 2.5.1 *Sea* $H = \{v_1, \ldots, v_m\}$ *(*$m \in \mathbb{N}$*) un subconjunto de un espacio vectorial* $V(\mathbb{K})$*. Entonces, son equivalentes:*

1. *No existe* $v_i \in H$ *tal que* $v_i \in L(H \setminus \{v_i\})$*.*
2. *La única combinación lineal de elementos de* H *igual a 0 es la que tiene todos sus coeficientes nulos, esto es:*

$$\text{(2.7)} \qquad \textit{Si } a_1, \ldots a_m \in \mathbb{K} \textit{ cumplen } a_1 v_1 + \ldots + a_m v_m = 0 \;\Rightarrow\; a_1 = \cdots = a_m = 0.$$

Demostración. $\boxed{1 \Rightarrow 2}$. Razonando por reducción al absurdo, supogamos que $\exists a_1, \ldots, a_m \in \mathbb{K}$ no todos nulos tales que $a_1\, v_1 + \ldots + a_m\, v_m = 0$. Tomemos un $i \in \{1, \ldots, m\}$ tal que $a_i \neq 0$. Despejando v_i (se puede porque $\exists a_i^{-1} \in \mathbb{K}$) tenemos

$$v_i = -a_i^{-1}\, a_1\, v_1 - \ldots - a_i^{-1}\, a_{i-1}\, v_{i-1} - a_i^{-1}\, a_{i+1}\, v_{i+1} + \ldots - a_i^{-1}\, a_m\, v_m,$$

luego $v_i \in L(H \setminus \{v_i\})$, contradicción.

$\boxed{2 \Rightarrow 1}$. De nuevo por reducción al absurdo, supongamos que $\exists v_i \in H$ tal que $v_i \in L(H \setminus \{v_i\})$. Por tanto, $v_i = a_1\, v_1 + \ldots + a_{i-1}\, v_{i-1} + a_{i+1}\, v_{i+1} + \ldots + a_m\, v_m$ para ciertos $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_m \in \mathbb{K}$. Así que

$$a_1\, v_1 + \ldots + a_{i-1}\, v_{i-1} + (-1)\, v_i + a_{i+1}\, v_{i+1} + \ldots + a_m\, v_m = 0$$

es una combinación lineal de elementos de H igual a 0 y no todos sus coeficientes son nulos, contradicción. □

Nota 2.5.1 En la situación anterior, si H cumple la propiedad 2, entonces cualquier subconjunto $H' \subset H$ también la cumple.

Definición 2.5.1 Sea $V(\mathbb{K})$ un espacio vectorial. Diremos que un subconjunto finito $H \subset V$ es *linealmente independiente* si cumple cualquiera de las condiciones equivalentes 1 y 2 del Lema 2.5.1. Si H es infinito, diremos que es linealmente independiente si todos sus subconjuntos finitos son linealmente independientes.

Diremos que H es *linealmente dependiente* cuando no sea linealmente independiente.

Algunos comentarios:

1. En el caso de que $H = \{v\}$ tenga un único vector, H es linealmente independiente si y sólo si $v \neq 0$. Esto se sigue de que $a\, v = 0$ ocurre si y sólo si $a = 0$ ó $v = 0$.

2. Si $0 \in H$ contiene al vector nulo, entonces H es linealmente dependiente. Esto es así porque $1\,0 = 0$ es una combinación lineal de elementos de H con no todos sus coeficientes nulos.

3. Si $H = \{v_1, \dots, v_i, \dots, v_j, \dots, v_m\}$ cumple $v_i = v_j$ con $i < j$, entonces H es linealmente dependiente ya que $1\,v_i + (-1)\,v_j = 0$ es una combinación lineal de elementos de H con no todos sus coeficientes nulos.

4. Si $H = \{u, v\}$, entonces H es linealmente dependiente si y sólo si o bien u es proporcional a v o al revés. Esto se tiene porque si $u = av$ con $a \in \mathbb{K}$, entonces $u - av = 0$ es una combinación lineal de elementos de H con no todos sus coeficientes nulos. Y recíprocamente, si $a_1u + a_2v = 0$ con $a_1 \neq 0$, entonces $u = av$ siendo $a = -a_1^{-1}a_2$. Notemos que la relación de proporcionalidad entre vectores no es simétrica en general; por ejemplo, 0 es proporcional a todos vectores pero el único vector proporcional a 0 es el propio 0.

5. En el caso $H = \{u, v\}$ linealmente independiente, llamaremos a $L(\{u, v\})$ el *plano vectorial* generado por u y v. En el caso de los vectores libres (ejemplo 3 de la Sección 2.1.1), esto se suele resumir diciendo que $\{\vec{u}, \vec{v}\}$ es linealmente independiente si y sólo $\vec{u}, \vec{v}$ no son *colineales*. Para una cantidad mayor de vectores libres, el concepto de dependencia lineal generaliza al de colinealidad. Así, para los vectores libres del espacio, el conjunto $H = \{\vec{u}, \vec{v}, \vec{w}\}$ en es linealmente dependiente si y sólo si los vectores libres de H son *coplanares*, es decir, existe un plano vectorial que los contiene a todos.

Proposición 2.5.1 *Sea $V(\mathbb{K})$ un espacio vectorial y $H \subset V$ un subconjunto. Entonces, H es linealmente independiente si y sólo si todo elemento de $L(H)$ se escribe de forma única como combinación lineal de los elementos de H.*

Demostración. Para la condición necesaria, supongamos que $v \in L(H)$ se escribe

$$v = a_1\,v_1 + \cdots + a_m\,v_m = a_1'\,v_1 + \cdots + a_m'\,v_m. \tag{2.8}$$

Entonces, $(a_1 - a_1')\,v_1 + \cdots + (a_m - a_m')\,v_m = 0$, que es una combinación lineal de elementos de H igual a 0. Como H es linealmente independiente, $a_1 - a_1' = s = a_m - a_m' = 0$ luego $a_1 = a_1', \dots, a_m = a_m'$.

Recíprocamente, supongamos que todo elemento de $L(H)$ se escribe de forma única como combinación lineal de los elementos de H. Como $0 \in L(H)$, por definición de independencia lineal deducimos que H es linealmente independiente. □

De forma parecida a lo que ocurría con los sistemas de generadores, podríamos pensar que cuantos más vectores linealmente independientes tengamos en un espacio vectorial, mayor "tamaño" tendrá éste (direcciones en las que podemos movernos libremente dentro del espacio). Esto nos lleva a un problema similar al que planteamos para sistema de generadores:

> Si $V(\mathbb{K})$ es un espacio vectorial finitamente generado, ¿cuál es el mayor número de vectores que puede tener un subconjunto linealmente independiente?

Proposición 2.5.2 (Ampliación de subconjuntos linealmente independientes) *Sea $V(\mathbb{K})$ un espacio vectorial y $H \subset V$ un subconjunto linealmente independiente. Si $v \in V \setminus L(H)$, entonces $H \cup \{v\}$ es linealmente independiente.*

Demostración. consideremos una combinación lineal finita de elementos de $H \cup \{v\}$. Si el coeficiente de v es cero, entonces todos los coeficientes serán nulos por ser H linealmente independiente. Así que, razonando por reducción al absurdo, podemos suponer que el coeficiente de v es distinto de cero:

$$a_1\, v_1 + \ldots + a_m\, v_m + a\, v = 0,$$

con $a_1, \ldots, a_m, a \in \mathbb{K}$, $v_1, \ldots, v_m \in H$, $a \neq 0$. Esto nos dice que $\exists a^{-1} \in \mathbb{K}$, luego $v = -a^{-1}a_1\, v_1 - \ldots - a^{-1}a_m\, v_m$, lo que contradice la hipótesis $v \in V \setminus L(H)$. $\square$

Veamos algunos ejemplos.

1. En $\mathbb{R}^2$ el subconjunto $H = \{v_1, v_2, v_3\}$ con $v_1 = (1, 0)$, $v_2 = (1, 1)$ y $v_3 = (0, 1)$ es linealmente dependiente ya que $v_2 = v_1 + v_3$. En particular, existe una combinación lineal del tipo $a\, v_1 + b\, v_2 + c\, v_3 = 0$ con no todos sus coeficientes nulos. Podemos calcularlas explícitamente tomando componentes y operando, con lo que la igualdad anterior se transforma en $(a + b, b + c) = (0, 0)$. El SEL homogéneo

$$\left.\begin{array}{ccccc} a & +b & & = & 0 \\ & b & +c & = & 0 \end{array}\right\}$$

es compatible indeterminado, por lo que tiene infinitas soluciones. Por ejemplo $a = 1$, $b = -1$ y $c = 1$ es solución y produce la combinación lineal $v_1 - v_2 + v_3 = 0$. Veremos que en $\mathbb{R}^2$ no puede haber conjuntos linealmente independiente con más de dos vectores.

2. En $\mathbb{R}[x]$, el subconjunto $H = \{p_1(x), p_2(x), p_3(x)\}$ donde $p_1(x) = x^2 + x + 1$, $p_2(x) = 2x + 1$ y $p_3(x) = x^2 + 1$, es linealmente independiente. Para verlo, consideremos una combinación lineal del tipo $a\, p_1(x) + b\, p_2(x) + c\, p_3(x) = 0$. Operando, tenemos $(a + c)\, x^2 + (a + 2b)\, x + (a + b + c) = 0$. Esto nos lleva al SEL homogéneo

$$\left.\begin{array}{ccccc} a & & +c & = & 0 \\ a & +2b & & = & 0 \\ a & +b & +c & = & 0 \end{array}\right\}$$

Este SEL es compatible determinado y, por tanto, su única solución es $a = b = c = 0$. Por tanto, H es linealmente independiente.

3. En $\mathbb{K}^n$, el subconjunto $H = \{e_1, \ldots, e_n\}$ del Ejemplo (C) de la Sección 2.4 es linealmente independiente. Para verlo, tomamos una combinación lineal del tipo $a_1\, e_1 + \ldots + a_n\, e_n = 0$. Al tomar componentes y operar, obtenemos $(a_1, \ldots, a_n) = (0, \ldots, 0)$, por lo que $a_1 = \ldots = a_n = 0$.

4. En $\mathcal{M}_{m\times n}(\mathbb{K})$, el subconjunto $H = \{E_{ij} \,|\, i = 1, \ldots, m,\ j = 1, \ldots, n\}$ definido en el Ejemplo (E) de la Sección 2.4 es linealmente. Para verlo, tomamos una combinación lineal del tipo

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}\, E_{ij} = a_{11}\, E_{11} + \ldots + a_{1n}\, E_{1n} + \ldots + a_{m1}\, E_{m1} + \ldots + a_{mn}\, E_{mn} = 0_{m\times n}.$$

Teniendo en cuenta cómo se definen las matrices E_{ij}, la igualdad anterior equivale a la igualdad $A = (a_{ij})_{i,j} = 0_{m\times n}$.

5. En $\mathbb{K}[x]$, el subconjunto $H = \{p_i(x) \,|\, i \in \mathbb{N} \cup \{0\}\}$ definido en el Ejemplo (D) de la Sección 2.4 es linealmente independiente. Para verlo, hay que comprobar que cada subconjunto finito de H es linealmente independiente; tomemos cualquier $H' = \{p_{i_1}(x), \ldots, p_{i_m}(x)\} \subset H$ y una combinación lineal del tipo $a_1\, p_{i_1}(x) + \ldots + a_m\, p_{i_m}(x) = 0$, con $a_1, \ldots, a_m \in \mathbb{K}$. Como $p_{i_k}(x) = x^{i_k}$, tenemos $a_1 x^{i_1} + \ldots + a_m x^{i_m} = 0$. Como los grados de cada monomio de la izquiera son distintos, deducimos que $a_i = 0$ para cada $i = 1, \ldots, m$.

6. En $(\mathbb{C}, +)$ consideramos el subconjunto $H = \{v_1, v_2\}$ con $v_1 = 1$ y $v_2 = i$. H es linealmente dependiente en $\mathbb{C}(\mathbb{C})$, ya que $v_2 = i\, v_1$. Pero H es linealmente independiente en $\mathbb{C}(\mathbb{R})$, ya que si $a_1 + a_2\, i = 0$ con $a_1, a_2 \in \mathbb{R}$ entonces $a_1 = a_2 = 0$.

2.6. Bases y dimensión

Ya hemos comentado que nos interesa encontrar, dado un espacio vectorial $V(\mathbb{K})$ finitamente generado, un sistema de generadores de V con la menor cantidad posible de vectores, y un subconjunto linealmente independiente con la mayor cantidad posible de vectores.

Teorema 2.6.1 (Teorema de Steinitz) *Sea $V(\mathbb{K})$ un espacio vectorial. Supongamos que $H = \{u_1, u_2, \ldots, u_m\} \subset V$ es un sistema de generadores de V y $H' = \{v_1, v_2, \ldots, v_k\} \subset V$ es linealmente independiente. Entonces, $m \geq k$.*

Demostración. Razonando por reducción al absurdo, supongamos que $m < k$.

Paso 1. Veamos que, salvo una reordenación de H, se puede sustituir u_1 por v_1 en H de modo que $H_1 := \{v_1, u_2, \ldots, u_m\}$ sigue siendo sistema de generadores de V:

Como $L(H) = V$, el apartado 1 de la Proposición 2.4.1 asegura que $\{v_1, u_1, u_2, \ldots, u_m\}$ es un sistema de generadores de V. Además, el vector v_1 se expresa como combinación lineal de H, es decir, $\exists a_1, a_2, \ldots, a_m \in \mathbb{K}$ tales que

$$v_1 = a_1\, u_1 + a_2\, u_2 + \ldots + a_m\, u_m. \tag{2.9}$$

Además $v_1 \neq 0$ ya que H' es linealmente independiente. Esto nos dice que en (2.9) no todos los coeficientes del miembro de la derecha son nulos. Reordenando y renombrando si fuese necesario los vectores de H, podemos suponer $a_1 \neq 0$. Despejamos ahora el vector u_1 en (2.9), obteniendo

$$u_1 = a_1^{-1}\, v_1 + (-a_1^{-1}\, a_2)\, u_2 + \ldots + (-a_1^{-1}\, a_m)\, u_m,$$

por lo que $u_1 \in L(\{v_1, u_2, \ldots, u_m\})$. Por el apartado 2 de la Proposición 2.4.1, tenemos que $\{v_1, u_2, \ldots, u_m\}$ es un sistema de generadores de V.

Paso 2. Veamos que, salvo una reordenación de H_1, se puede sustituir su segundo elemento u_2 por v_2 de modo que $H_2 := \{v_1, v_2, u_3 \ldots, u_m\}$ sigue siendo un sistema de generadores de V:

Como H_1 es un sistema de generadores de V, el apartado 1 de la Proposición 2.4.1 asegura que $\{v_1, v_2, u_2, \ldots, u_m\}$ es un sistema de generadores de V. Además, el vector v_2 de H_1, es decir, $\exists b_1, \ldots, b_m \in \mathbb{K}$ tales que

$$v_2 = b_1\, v_1 + b_2\, u_2 + b_3\, u_3 \ldots + b_m\, u_m. \tag{2.10}$$

Alguno de los escalares b_i con $i \geq 2$ tiene que ser distinto de 0 (en caso contrario el subconjunto $\{v_1, v_2\}$ sería linealmente independiente, luego h' también lo sería). Reordenando y renombrando los vectores $u_2, \ldots, u_m$ de H_1 podemos suponer que $b_2 \neq 0$. Despejamos el vector u_2 en (2.10), obteniendo

$$u_2 = b_2^{-1}\, v_2 + (-b_2^{-1}\, b_1)\, v_1 + (-b_2^{-1}\, b_3)\, u_3 + \ldots + (-b_2^{-1}\, b_m)\, u_m,$$

por lo que $u_2 \in L(\{v_1, v_2, \ldots, u_m\})$. Por el apartado 2 de la Proposición 2.4.1, $\{v_1, v_2, u_3, \ldots, u_m\}$ es un sistema de generadores de V.

Ahora reiteramos el proceso anterior de ir sustituyendo vectores de H por otros de H'. Como estamos suponiendo $m < k$, se nos acaban antes los de H que los de H', es decir, llegamos a $H_m = \{v_1, v_2, \ldots, v_m\}$ sistema de generadores de V, y aún tenemos al menos $v_{m+1} \in H'$ que no ha participado en el proceso de sustitución. Como $L(H_m) = V$, deducimos que $v_{m+1} \in L(H_m)$, y por tanto $\{v_1, \ldots, v_m, v_{m+1}\}$ es linealmente dependiente. Esto contradice que H' es linealmente independiente. $\square$

Definición 2.6.1 Una *base* de un espacio vectorial $V(\mathbb{K})$ es un subconjunto $\mathcal{B} \subset V$ que sea a la vez sistema de generadores de V y linealmente independiente.

Veamos algunos ejemplos.

1. En $\mathbb{K}^n$, el subconjunto $\mathcal{B}_u = \{e_1, \ldots, e_n\}$ definido en el Ejemplo (C) de la Sección 2.4 es una base, que llamaremos *base usual o canónica de* $\mathbb{K}^n$*.*

2. En $\mathcal{M}_{m\times n}(\mathbb{K})$, el subconjunto $\mathcal{B}_u = \{E_{ij} \,|\, i = 1, \ldots, m,\ j = 1, \ldots, n\}$ definido en el Ejemplo (E) de la Sección 2.4 es una base, que llamaremos *base usual o canónica de* $\mathcal{M}_{m\times n}(\mathbb{K})$*.*

3. En $\mathbb{K}[x]$, el subconjunto $\mathcal{B}_u = \{p_i(x) = x^i \,|\, i \in \mathbb{N} \cup \{0\}\}$ es una base de $\mathbb{K}[x]$, que llamaremos *base usual o canónica* de $\mathbb{K}[x]$.

4. Dos vectores libres no colineales en el plano, o tres no coplanares en el espacio son bases.

Teorema 2.6.2 (Existencia de bases) *Sea $V(\mathbb{K}) \neq \{0\}$ un espacio vectorial finitamente generado. Entonces, de cualquier sistema de generadores finito de V se puede extraer una base.*

Demostración. Sea $H = \{v_1, \ldots, v_m\}$ un sistema de generadores de V. Si H es linealmente independiente, H será base de V y hemos terminado. Supongamos estonces que H es linealmente dependiente. Por el Lema 2.5.1, $\exists v_i \in H$ tal que $v_i \in (H \setminus \{v_i\})$. Salvo reordenar y renombrar los elementos de H, podemos suponer $i = m$. Por el apartado 2 de la Proposición 2.4.1, $H' := \{v_1, \ldots, v_m\}$ sigue siendo sistema de generadores de V. Si H' es linealmente independiente, H' será base de V y hemos terminado. Si H' es linealmente dependiente, volvemos a repetir del proceso de eliminar un vector de H' que dependa linealmente del resto, que podemos suponer es v_{m-1} tras reordenar. Este proceso se terminará en una cantidad finita de pasos (no podemos eliminar todos los vectores de H ya que cuando tengamos un sólo vector v_1, decir que $\{v_1\}$ es linealmente dependiente equivale a que $v_1 = 0$, pero como $L(\{v_1\}) = V$ eso nos lleva a que $V = \{0\}$, contradicción), y al terminar llegamos a un subconjunto de H linealmente independiente y sistema de generadores, es decir, una base de V. $\square$

Nota 2.6.1 El Teorema 2.6.2 también es cierto sin la hipótesis de ser finitamente generado, pero para demostrarlo se necesita el llamado *axioma de elección*, que se puede enunciar de distintas formas; nosotros usaremos el *Lema de Zorn*:

> Sea $X \neq \varnothing$ un conjunto con una relación de orden parcial $\leq$, en el que toda *cadena*[4] $C \subset X$ posee una *cota superior*[5]. Entonces, X admite un elemento *maximal*[6].

Para demostrar la existencia de bases en $V(\mathbb{K})$, tomamos como X el conjunto de todos los subconjuntos de V linealmente independientes, X no es vacío, puesto que $\{v\}$ es linealmente independiente siempre que $v \in V$, $v \neq 0$. La relación de orden parcial en X se toma como la inclusión. Un cadena C en X es una colección totalmente ordenada por $\subset$ de subconjuntos linealmente independientes de X, y la unión de todos ellos sirve como cota superior (notemos que dicha unión es un subconjunto linealmente independiente de V porque cualquier subconjunto finito suyo estará incluido en algún elemento de la cadena, el cual es linealmente independiente por la definición de X).

Aplicando el lema de Zorn a X, existe un elemento maximal $\mathcal{B} \in X$. Queda comprobar que $\mathcal{B}$ es una base de V: $\mathcal{B}$ es linealmente independiente por pertenecer a X, y $\mathcal{B}$ es sistema de generadores de V por la Proposición 2.5.2, ya que si $\exists v \in V \setminus L(\mathcal{B})$ entonces $\mathcal{B} \cup \{v\} \in X$, lo que contradice la maximalidad de $\mathcal{B}$.

Teorema 2.6.3 (de la base) *Todas las bases de un espacio vectorial finitamente generado son finitas y tienen el mismo número de vectores.*

Demostración. Sea $V(\mathbb{K})$ un espacio vectorial finitamente generado. Sabemos que V tiene bases y que alguna de ellas tiene cardinal finito, por el Teorema 2.6.2. Tomemos una base $\mathcal{B}_1$ con cardinal finito $n_1 \in \mathbb{N}$ y sea $\mathcal{B}_2$ otra base de V, con cardinal $n_2 \in \mathbb{N} \cup \{\infty\}$ respectivamente. Si $n_2 \geq n_1+1$ (incluimos el caso $n_2 = \infty$), tomamos en $\mathcal{B}_2$ un subconjunto H' con n_1+1 vectores. Como $H' \subset \mathcal{B}_2$ y $\mathcal{B}_2$ es linealmente independiente, H' es linealmente independiente. Usando el Teorema de Steinitz con el sistema de geeradores $H = \mathcal{B}_1$ y el conjunto linealmente independiente H', deducimos que $m \geq m+1$, contradicción. Así que $n_2 \leq n_1$. En particular, toda base de V tiene un número finito de vectores. Ahora intercambiamos los papeles de $\mathcal{B}_1$ y $\mathcal{B}_2$ para deducir que $n_1 \leq n_2$. $\square$

Definición 2.6.2 Sea $V(\mathbb{K})$ un espacio vectorial. Se define la *dimensión* $\dim_{\mathbb{K}}(V)$ de $V(\mathbb{K})$, de la siguiente forma:

(i) Si $V = \{0\}$, $\dim_{\mathbb{K}} V = 0$.

(ii) Si $V \neq \{0\}$ es finitamente generado, $\dim_{\mathbb{K}}(V)$ es el cardinal de cualquier base de V.

(iii) Si V no es finitamente generado, $\dim_{\mathbb{K}} V = \infty$.

---

[4] Un subconjunto $C \subset X$ es una cadena si $(C, \leq)$ está totalmente ordenado.
[5] Es decir, un elemento $s \in X$ tal que $a \leq s$ para todo $a \in C$.
[6] Un elemento $x \in X$ se dice maximal si no existe $a \in X \setminus \{x\}$ tal que $x \leq a$.

En el caso particular $\dim_{\mathbb{K}}(V) = 1$, diremos que V es una *recta vectorial*. Y si $\dim_K(V) = 2$, que V es un *plano vectorial*.

Veamos algunos ejemplos.

1. $\dim_{\mathbb{K}} \mathbb{K}^n = n$.
2. $\dim_{\mathbb{K}} \mathcal{M}_{m\times n}(\mathbb{K}) = m\,n$, $\dim_{\mathbb{K}} \mathcal{M}_n(\mathbb{K}) = n^2$.
3. $\dim_{\mathbb{K}} \mathbb{K}[x] = \infty$.
4. La dimensión del espacio vectorial de los vectores libres del plano es 2, y la de los vectores libres del espacio es 3.
5. $\dim_{\mathbb{C}} \mathbb{C} = 1$, y $\dim_{\mathbb{R}} \mathbb{C} = 2$. En general, si V es un espacio vectorial complejo con $\dim_{\mathbb{C}} V = n$, entonces V es un espacio vectorial real con $\dim_{\mathbb{R}} V = 2n$.

Corolario 2.6.1 *Sea $V(\mathbb{K})$ un espacio vectorial finitamente generado. Dados $H = \{v_1, \ldots, v_k\} \subset V$ un subconjunto linealmente independiente y $H' = \{u_1, \ldots, u_m\}$ un sistema de generadores de V, se tiene $k \leq \dim_{\mathbb{K}} V \leq m$.*

Demostración. Sea $\mathcal{B}$ una base de V. Por definición, el cardinal de $\mathcal{B}$ es $n := \dim_{\mathbb{K}} V$. Usando el Teorema de Steinitz con H como subconjunto linealmente independiente y $\mathcal{B}$ como sistema de generadores, se deduce que $k \leq n$. Usando el mismo teorema con $\mathcal{B}$ como subconjunto linealmente independiente y H' como sistema de generadores se deduce que $n \leq m$. □

Corolario 2.6.2 *Si $V(\mathbb{K})$ es un espacio vectorial finitamente generado, entonces todo subespacio vectorial de V es finitamente generado y $\dim_{\mathbb{K}} U \leq \dim_{\mathbb{K}} V$.*

Demostración. Sea $n = \dim_{\mathbb{K}} V \in \mathbb{N}$. Supongamos que $U \leq V$ es un subespacio vectorial. Claramente, todo subconjunto linealmente independiente de U es linealmente independiente en V. Por tanto, el Corolario 2.6.1 asegura que llamando A al conjunto de los cardinales de subconjuntos de U linealmente independientes, se tiene $\sup A \leq n$. En particular, $\sup A$ es un número natural $k \leq n$ y existe un subconjunto $H \subset U$ linealmente independiente con cardinal k. Si $L(H) \neq U$, entonces la Proposición 2.5.2 aplicada a $V = U$ asegura que podemos ampliar H a un subconjunto $H \cup \{v\} \subset U$ linealmente independiente, lo que contradice que el supremo de A es k. Así que $L(H) = U$, y por tanto H es base de U y $\dim_{\mathbb{K}} U = k$. □

Corolario 2.6.3 *Sea $V(\mathbb{K})$ un espacio vectorial con $\dim_{\mathbb{K}} V = n \in \mathbb{N}$ y $H = \{v_1, \ldots, v_n\} \subset V$ un subconjunto linealmente independiente. Entonces, H es una base de V.*

Demostración. Si H no es sistema de generadores de V, entonces $\exists v \in V \setminus L(H)$. Como H es linealmente independiente, la Proposición 2.5.2 garantiza que $H \cup \{v\}$ es linealmente independiente, lo que contradice el Corolario 2.6.1. □

Corolario 2.6.4 *Sea $V(\mathbb{K})$ es un espacio vectorial finitamente generado, y $U \leq V$ un subespacio vectorial. Entonces, $\dim_{\mathbb{K}} U = \dim_{\mathbb{K}} V$ si y sólo si $U = V$.*

Demostración. Si $U = V$ entonces no hay nada que probar. Supongamos que $\dim_{\mathbb{K}} U = \dim_{\mathbb{K}} V$. Por el Corolario 2.6.2, U es finitamente generado luego admite una base $\mathcal{B}_U$. Visto como subconjunto de V, $\mathcal{B}_U$ es linealmente independiente. Como su cardinal es $\dim_{\mathbb{K}} U = \dim_{\mathbb{K}} V$, el Corolario 2.6.3 implica que $\mathcal{B}_U$ es base de V, y por tanto $U = L(\mathcal{B}_U) = V$. □

Corolario 2.6.5 *Sea $V(\mathbb{K})$ un espacio vectorial con $\dim_{\mathbb{K}} V = n \in \mathbb{N}$ y $H = \{v_1, \ldots, v_n\} \subset V$ un sistema de generadores de V. Entonces, H es una base de V.*

Demostración. Si H es linealmente dependiente, entonces el Lema 2.5.1 implica que $\exists v_i \in H$ tal que $v_i \in L(H \setminus \{v_i\})$. En particular, $n \geq 2$. Aplicando el apartado 2 de la Proposición 2.4.1 deducimos que $H \setminus \{v_i\}$ es un sistema de generadores de V con $n-1$ vectores, lo que contradice el Corolario 2.6.1. □

Uniendo la definición de base con los Corolarios 2.6.3 y 2.6.5 tenemos la siguiente equivalencia (que no es generalizable al caso de dimensión infinita):

Corolario 2.6.6 *Sea $V(\mathbb{K})$ un espacio vectorial con $\dim_{\mathbb{K}} V = n \geq 1$. Dada un subconjunto $\mathcal{B} = \{v_1, \ldots, v_n\}$ con n vectores de V, son equivalentes:*

1. *$\mathcal{B}$ es una base de V.*
2. *$\mathcal{B}$ es un sistema de generadores de V.*
3. *$\mathcal{B}$ es linealmente independiente.*

En el Teorema 2.6.2 vimos que de cualquier sistema de generadores se puede extraer una base. Ahora veremos que también se puede conseguir una base añadiendo vectores a un subconjunto linealmente independiente.

Teorema 2.6.4 (Ampliación de la base) *Sea $V(\mathbb{K})$ un espacio vectorial con $\dim_{\mathbb{K}} V = n \in \mathbb{N}$. Si $H = \{v_1, \ldots, v_k\}$ es un conjunto linealmente independiente y $k < n$, entonces $\exists v_{k+1}, \ldots, v_n \in V$ tales que $\mathcal{B} := \{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$ es una base de V.*

Demostración. Como $k < n$, H no puede ser sistema de generadores de V (si lo fuera H sería una base, lo que contradice el Teorema 2.6.3). Así que $\exists v_{k+1} \in V \setminus L(H)$. Por la Proposición 2.5.2, el subconjunto $H \cup \{v_{k+1}\} = \{v_1, \ldots, v_k, v_{k+1}\}$ es linealmente independiente. Si $k+1 = n$, entonces $H \cup \{v_{k+1}\}$ es una base de V por el Corolario 2.6.3 y hemos terminado. Si $k+1 < n$, repetimos el argumento cambiando H por $H \cup \{v_{k+1}\}$. Este proceso de ir añadiendo vectores obteniendo subconjuntos linealmente independientes cada vez mayores tiene que pararse en una cantidad finita de pasos por la primera desigualdad del Corolario 2.6.1. Y se se para es porque habremos obtenido una base de V, que tendrá exactamente n elementos por el Teorema de la base. Así que al final habremos ampliado H con $n-k$ vectores. $\square$

Nota 2.6.2

1. La ampliación $\{v_{k+1}, \ldots, v_n\}$ del conjunto H a una base no es única: por ejemplo, podemos cambiar v_{k+1} por av_{k+1} siendo a cualquier escalar no nulo.

2. Como caso particular, a partir de cualquier vector $v \in V \setminus \{0\}$ se puede construir una base $\mathcal{B}$ de V con $v \in \mathcal{B}$.

3. El Teorema 2.6.4 se puede extender a dimensión infinita, esto es, cualquier conjunto linealmente independiente S se puede ampliar a una base. Su demostración puede llevarse a cabo razonando con argumentos similares a los de la Nota 2.6.1.

4. La razón por la que el Teorema 2.6.4 se llama "de ampliación de la base" es la siguiente: supongamos que $V(\mathbb{K})$ un espacio vectorial con $\dim_{\mathbb{K}} V = n \in \mathbb{N}$. Sea $U \leq V$ con $\dim_{\mathbb{K}} U = m \leq n$ y sea $\mathcal{B}_U = \{v_1, \ldots, v_m\}$ una base de U. Entonces, $\exists v_{k+1}, \ldots, v_n \in V$ tales que $\mathcal{B} := \{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$ es una base de V (esto es consecuencia directa del Teorema 2.6.4.)

Proposición 2.6.1 *Sea $V(\mathbb{K})$ un espacio vectorial, $H = \{v_1, \ldots, v_m\} \subset V$ y $v = \sum_{i=1}^m a_i v_i \in L(H)$, siendo $a_1, \ldots, a_m \in \mathbb{K}$. Entonces:*

1. *Si H es sistema de generadores y $a_i \neq 0$, entonces $[H \setminus \{v_i\}] \cup \{v\}$ es sistema de generadores.*

2. *Supongamos que H es linealmente independiente. Entonces, $[H \setminus \{v_i\}] \cup \{v\}$ es linealmente independiente si y sólo si $a_i \neq 0$.*

3. *Supongamos que H es base de V. Entonces, $[H \setminus \{v_i\}] \cup \{v\}$ es base de V si y sólo si $a_i \neq 0$.*

Demostración. Para el apartado 1, notemos que $H \cup \{v\}$ es sistema de generadores de V (porque H lo es). Como $a_i \neq 0$, concluimos que $v_i \in L([H \setminus \{v_i\}] \cup \{v\})$. Aplicando el apartado 2 de la Proposición 2.4.1, $[H \setminus \{v_i\}] \cup \{v\}$ es sistema de generadores.

Para el apartado 2, primero supongamos que $a_i = 0$. Entonces,

$$a_1 v_1 + \ldots + a_{i-1} v_{i-1} + (-1)v + a_{i+1} v_{i+1} + \ldots + a_m v_m = 0$$

es una combinación lineal de vectores de $[H \setminus \{v_i\}] \cup \{v\}$ igual a cero y con no todos sus coeficientes nulos, luego $[H \setminus \{v_i\}] \cup \{v\}$ es linealmente dependiente. Esto prueba que si $[H \setminus \{v_i\}] \cup \{v\}$ es linealmente independiente, entonces $a_i \neq 0$.

Recíprocamente, supongamos que $a_i \neq 0$ y veamos que $[H \setminus \{v_i\}] \cup \{v\}$ es linealmente independiente. Sean $\lambda_1, \ldots, \lambda_m \in \mathbb{K}$ tales que

$$\lambda_1 v_1 + \ldots + \lambda_{i-1} v_{i-1} + \lambda_i v + \lambda_{i+1} v_{i+1} + \ldots + \lambda_m v_m = 0. \tag{2.11}$$

Sustituyendo $v = \sum_{i=1}^{m} a_i v_i$ en (2.11) y agrupando, obtenemos

$$(\lambda_1 + \lambda_i a_1) v_1 + \ldots + (\lambda_{i-1} + \lambda_i a_{i-1}) v_{i-1} + \lambda_i a_i v_i + (\lambda_{i+1} + \lambda_i a_{i+1}) v_{i+1} + \ldots + (\lambda_m + \lambda_i a_m) v_m = 0.$$

Como H es linealmente independiente, tenemos $\lambda_j + \lambda_i a_j = 0 \ \forall j \in \{1, \ldots, m\} \setminus \{i\}$ y $\lambda_i a_i = 0$. Como $a_i \neq 0$, de la última ecuación obtenemos $\lambda_i = 0$. Sustituyendo esto en las otras $m-1$ ecuaciones obtenemos $\lambda_j = 0 \ \forall j \in \{1, \ldots, m\} \setminus \{i\}$, luego $[H \setminus \{v_i\}] \cup \{v\}$ es linealmente independiente.

Finalmente, supongamos que H es base de V y veamos el apartado 3. Si $[H \setminus \{v_i\}] \cup \{v\}$ es base, entonces es linealmente independiente luego aplicando el apartado 2, $a_i \neq 0$. Recíprocamente, si $a_i \neq 0$ entonces por el apartado 2, $[H \setminus \{v_i\}] \cup \{v\}$ es linealmente independiente. Como $\dim_{\mathbb{K}} V = m$ (porque H es base de V), el Corolario 2.6.3 asegura que $[H \setminus \{v_i\}] \cup \{v\}$ es base de V. □

Corolario 2.6.7 *Sea $V(\mathbb{K})$ un espacio vectorial finitamente generado y $U, W \leq V$ subespacios vectoriales suplementarios (es decir, $V = U \oplus W$). Entonces,* $\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} U + \dim_{\mathbb{K}} W$. *Además, si $\mathcal{B}_U, \mathcal{B}_W$ son bases de U, W respectivamente, el subconjunto $\mathcal{B}_U \cup \mathcal{B}_W$ es base de V.*

Demostración. Si $U = \{0\}$ entonces de $V = U \oplus W$ se deduce que $W = V$ luego $\dim_{\mathbb{K}} U + \dim_{\mathbb{K}} W = 0 + \dim_{\mathbb{K}} W = \dim_{\mathbb{K}} V$. Si $U = V$ entonces $W = \{0\}$ y el razonamiento es análogo. Así que supongamos que U, V son subespacios propios de V. Tomemos bases respectivas $\mathcal{B}_U$ de U y $\mathcal{B}_W$ de W, que existen porque ambos subespacios son finitamente generados y no nulos. Entonces,

$$V = U + W = L(\mathcal{B}_U) + \mathcal{B}_w) \overset{(\star)}{=} L(\mathcal{B}_U \cup \mathcal{B}_W),$$

donde en $(\star)$ hemos usado el Lema 2.2.1. Esto prueba que $\mathcal{B}_U \cup \mathcal{B}_W$ es un sistema de generadores de V.

Veamos ahora que $\mathcal{B}_U \cup \mathcal{B}_W$ es linealmente independiente: si no lo es, uno de sus vectores depende linealmente del resto. Podemos suponer que $\exists x \in \mathcal{B}_U$ que depende linealmente de $[\mathcal{B}_U \cup \mathcal{B}_W] \setminus \{x\}$. Por tanto, pordemos escribir $x = y + z$ donde $y \in L(\mathcal{B}_U \setminus \{x\})$, $z \in L(\mathcal{B}_W)$. Así, $x - y \in L(\mathcal{B}_U) = U$ es igual a $z \in W$. Como $U \cap W = \{0\}$, tenemos $x - y = z = 0$. En particular, $x = y$ luego $x \in L(\mathcal{B}_U \setminus \{x\})$, lo que implica que $\mathcal{B}_U$ es linealmente dependiente, contradición. Por tanto, $\mathcal{B}_U \cup \mathcal{B}_W$ es linealmente independiente.

Como $\mathcal{B}_U \cup \mathcal{B}_W$ es linealmente independiente y sistema de generadores de V, concluimos que $\mathcal{B}_U \cup \mathcal{B}_W$ es base de V. En particular, $\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} U + \dim_{\mathbb{K}} W$. □

Podemos terminar esta sección con un resultado en cierta manera recíproco al Corolario 2.6.7.

Corolario 2.6.8 *Sea $V(\mathbb{K})$ un espacio vectorial finitamente generado y $U \leq V$ con $\dim_{\mathbb{K}} U = m \leq n = \dim_{\mathbb{K}} V$. Dada una base $\mathcal{B}_U\{v_1, \ldots, v_m\}$ de U, existen $n - m$ vectores $v_{m+1}, \ldots, v_n \in V$ tales que $\mathcal{B} = \{v_1, \ldots, v_m, v_{m+1}, \ldots, v_n\}$ es una base de V, y el subespacio vectorial $W := L(\{v_{m+1}, \ldots, v_m\})$ es un suplementario de U en V, esto es, $V = U \oplus W$.*

Demostración. La existencia de vectores $v_{m+1}, \ldots, v_n \in V$ tales que $\mathcal{B} = \{v_1, \ldots, v_m, v_{m+1}, \ldots, v_n\}$ es base de V es consecuencia directa del Teorema de Ampliación de la Base (ver apartado 4 de la Nota 2.6.2). Queda ver que $W := L(\{v_{m+1}, \ldots, v_m\})$ cumple $V = U \oplus W$:

$\boxed{V = U + W:}$ $\mathcal{B} \subset U \cup V$ y por ser $\mathcal{B}$ sistema de generadores de V, $V = L(\mathcal{B}) \subset L(U \cup W) = L(U) + L(W) = U + W$.

$\boxed{U \cap W = \{0\}:}$ Esto es obvio si $U = \{0\}$ ó $W = \{0\}$, por lo que a partir de ahora suponemos $U \neq \{0\}$ y $W \neq \{0\}$. Sea $v \in U \cap W$. Como $v \in U = L(\mathcal{B}_U)$, $\exists a_1, \ldots, a_m \in \mathbb{K}$ tales que $v = a_1 v_1 + \ldots + a_m v_m$. Y como $v \in W = L(\{v_{m+1}, \ldots, v_n\})$, $\exists a_{m+1}, \ldots, a_n \in \mathbb{K}$ tales que $v = a_{m+1} v_{m+1} + \ldots + a_n v_n$. Restando ambas igualdades obtenemos

$$a_1 v_1 + \ldots + a_m v_m - a_{m+1} v_{m+1} + \ldots - a_n v_n = 0,$$

que es una combinación lineal igual a 0 de $\mathcal{B}$, que es linealmente independiente. Por tanto deducimos que $a_i = 0 \ \forall i = 1, \ldots, n$ luego $v = 0$. □

El Corolario 2.6.8 da un método práctico de construcción de subespacios suplementarios. Notemos que cada completación de una base $\mathcal{B}_U$ de U hasta una base de V da lugar a un subespacio suplementario posiblemente distinto. Por ejemplo, sea U el subespacio vectorial de $\mathbb{R}^2$ dado por $U = L(\{u\})$ con $u = (1, -2)$. Es claro que $\mathcal{B}_U := \{u\}$ es una base de U, luego $\dim_{\mathbb{R}} U = 1$. Consideremos el vector $w = (0, 1) \in \mathbb{R}^2$. Como $\mathcal{B} := \{u, w\}$ es una base de $\mathbb{R}^2$, $W := L(\{w\})$ es un suplementario de U en $\mathbb{R}^2$. Pero si tomamos $w' = (1, 0) \in \mathbb{R}^2$, también $\{u, w'\}$ es una base de $\mathbb{R}^2$ y $W' := L(\{w'\})$ es otro suplementario de U en $\mathbb{R}^2$. Es decir, $\mathbb{R}^2 = U \oplus W = U \oplus W'$ pero $W \neq W'$.

Definición 2.6.3 Sea $V(\mathbb{K})$ un espacio vectorial finitamente generado y $U \leq V$. Llamamos *codimensión* de U en V a la dimensión de cualquier subespacio suplementario:

$$\operatorname{codim}_{\mathbb{K}}(U) = \dim_{\mathbb{K}} V - \dim_{\mathbb{K}} U.$$

Si $\operatorname{codim}_{\mathbb{K}}(U) = 1$, diremos que U es un *hiperplano vectorial de* V.

2.6.1. Bases y dimensión de un espacio vectorial cociente

Sea $V(\mathbb{K})$ un espacio vectorial con $\dim_{\mathbb{K}} V = n \in \mathbb{N}$ y $U \leq V$. Veamos cómo calcular la dimensión de V/U y una base suya. Recordemos que por el Corolario 2.6.2, todos los subespacios vectoriales de V son finitamente generados (con dimensión lo más n) y por tanto, admiten bases (si son no nulos). En el caso $\dim_{\mathbb{K}} U = n$, el Corolario 2.6.4 asegura que $U = V$ luego $V/U = \{0 + U\}$ es el espacio vectorial nulo, que no tiene bases y tiene dimensión cero. De ahora en adelante supondremos que $\dim_{\mathbb{K}} U < \dim_{\mathbb{K}} V$.

Teorema 2.6.5 *Sea $V(\mathbb{K})$ un espacio vectorial finitamente generado y $U \leq V$, $\{0\} \neq U \neq V$. Si W es un subespacio suplementario de U y $\mathcal{B}_W = \{w_1, \ldots, w_k\}$ es una base de W, entonces*

$$\mathcal{B}_{V/U} := \{w_1 + U, \ldots, w_k + U\}$$

es una base de V/U. Por tanto, $\dim_{\mathbb{K}}(V/U) = \dim_{\mathbb{K}} V - \dim_{\mathbb{K}} U$.

Demostración. Llamemos $n = \dim_{\mathbb{K}} V$. Como W es un subespacio suplementario de U en V, se tiene $V = U \oplus W$. Tomemos una base $\mathcal{B}_U$ de U, que existe porque U es finitamente generado y no nulo (por esto mismo, sabemos que $\exists \mathcal{B}_W$). Por el Corolario 2.6.7, $\mathcal{B}_U \cup \mathcal{B}_W$ es base de V. En particular, la dimensión de U es $n - k$ así que podemos escribir $\mathcal{B}_U = \{u_1, \ldots, u_{n-k}\}$.

Veamos que $\mathcal{B}_{V/U}$ es sistema de generadores de V/U: Sea $x + U \in V/U$ y tomemos un representante x en dicha clase. Como $x \in V$ y $\mathcal{B}_U \cup \mathcal{B}_W$ es sistema de generadores de V, existen $a_1, \ldots, a_n \in \mathbb{K}$ tales que

$$x = \sum_{i=1}^{n-k} a_i u_i + \sum_{i=1}^{k} a_{n-k+i} w_i.$$

Tomando clases en V/U nos queda

$$x + U = \sum_{i=1}^{n-k} a_i (u_i + U) + \sum_{i=1}^{k} a_{n-k+i}(w_i + U) \overset{(\star)}{=} \sum_{i=1}^{k} a_{n-k+i}(w_i + U),$$

donde en $(\star)$ hemos usado que $\sum_{i=1}^{n-k} a_i(u_i + U) = \sum_{i=1}^{n-k} a_i(0 + U) = 0 + U$. Por tanto, $\mathcal{B}_{V/U}$ es sistema de generadores de V/U.

Finalmente, comprobemos que $\mathcal{B}_{V/U}$ es linealmente independiente: sean $b_1, \ldots, b_k \in \mathbb{K}$ tales que $0 + U = b_1(w_1 + U) + \cdots + b_k(w_k + U) = (b_1 w_1 + \ldots + b_k w_k) + U$. Esto quiere decir que $b_1 w_1 + \ldots + b_k w_k \in U$. Como $b_1 w_1 + \ldots + b_k w_k \in L(\mathcal{B}_W) = W$, tenemos que $b_1 w_1 + \ldots + b_k w_k \in U \cap W$, que es $\{0\}$ porque $V = U \oplus W$. Así, $b_1 w_1 + \ldots + b_k w_k = 0$ y como los vectores de $\mathcal{B}_W$ son linealmente independientes, concluimos que $b_1 = \ldots = b_k = 0$. Por tanto, $\mathcal{B}_{V/U}$ es linealmente independiente.

Como $\mathcal{B}_{V/U}$ es linealmente independiente y sistema de generadores de V/U, es base de V/U. □

Nota 2.6.3 El teorema anterior da un algoritmo para construir una base de V/U:

Paso 1: Se construye una base $\mathcal{B}_U = \{u_1, \ldots, u_m\}$ de U.

Paso 2: Ampliamos $\mathcal{B}_U$ a una base $\mathcal{B} = \{u_1, \ldots, u_m, v_{m+1}, \ldots, v_n\}$ de V.

Paso 3: El conjunto $\{v_{m+1} + U, \ldots, v_n + U\}$ es una base de V/U.

2.7. Coordenadas respecto de una base ordenada

Sea $V(\mathbb{K})$ un espacio vectorial y $\mathcal{B} = \{v_1, \ldots, v_n\}$ una base de V. Como $\mathcal{B}$ es un sistema de generadores de V, todo vector $v \in V$ se expresa como $v = a_1 v_1 + \ldots + a_n v_n$ para ciertos $a_1, \ldots, a_n \in \mathbb{K}$. Además, la independencia lineal de $\mathcal{B}$ junto con la Proposición 2.5.1 implican que estos escalares son únicos. En resumen, tenemos probado el siguiente resultado.

Teorema 2.7.1 (Existencia de coordenadas) *Sea $V(\mathbb{K})$ un espacio vectorial y $\mathcal{B} = \{v_1, \ldots, v_n\}$ una base de V. Entonces, para cada $v \in V$ $\exists! a_1, \ldots, a_n \in \mathbb{K}$ tales que $v = a_1 v_1 + \ldots + a_n v_n$.*

El recíproco del resultado anterior es cierto; incluso podemos decir algo más.

Proposición 2.7.1 *Sea $V(\mathbb{K})$ un espacio vectorial y $\mathcal{B} = \{v_1, \ldots, v_n\} \subset V \setminus \{0\}$. Entonces, son equivalentes:*

1. *$\mathcal{B}$ es una base de V.*
2. *$\forall v \in V$, $\exists! a_1, \ldots, a_n \in \mathbb{K}$ tales que $v = a_1 v_1 + \ldots + a_n v_n$.*
3. *$V = L(v_1) \oplus \ldots \oplus L(v_n)$.*

Demostración. $\boxed{1 \Leftrightarrow 2.}$ La existencia de los $a_i \in \mathbb{K}$ para cada $v \in V$ en el apartado 2 equivale a que $\mathcal{B}$ sea sistema de generadores, y la unicidad en ese mismo apartado equivale a que $\mathcal{B}$ sea linealmente independiente (Proposición 2.5.1).

$\boxed{2 \Leftrightarrow 3.}$ Por definición de suma directa, el apartado 3 de esta proposición equivale a se dé cualquiera de las dos condiciones de la Proposición 2.2.4. La condición 1 de la Proposición 2.2.4 es que para cada $x \in U_1 + \ldots + U_m$, $\exists! x_i \in U_i$, $i = 1, \ldots, m$, tales que $x = x_1 + \ldots + x_m$. Observemos que como $v_i \neq 0$, la existencia y unicidad de cada $x_i \in U_i$ equivale a la existencia y unicidad del escalar $a_i \in \mathbb{K}$ tal que $x_i = a_i v_i$. $\square$

El Teorema 2.7.1 nos dice que dada una base, tenemos una manera de asignar de forma unívoca a cada vector $v \in V$ una lista de coeficientes $(a_1, \ldots, a_n) \in \mathbb{K}^n$. Para que sepamos reconstruir v a partir de $(a_1, \ldots, a_n)$ necesitamos prefijar una ordenación de $\mathcal{B}$, es decir, aunque $\{v_1, v_2, \ldots, v_n\} = \{v_2, v_1, \ldots, v_n\}$ no es lo mismo $a_1 v_1 + a_2 v_2 + \ldots + a_n v_n$ que $a_1 v_2 + a_2 \cot v_1 + \ldots + a_n v_n$ como vectores de V. Esto nos lleva al concepto de base ordenada.

Definición 2.7.1 Sea $\mathcal{B}$ una base de un espacio vectorial $V(\mathbb{K})$ de dimensión $n \in \mathbb{N}$. A cada una de las $n!$ ordenaciones de los elementos de $\mathcal{B}$ se le llamará *base ordenada.* Por ejemplo, una de estas bases ordenadas creadas a partir de $\mathcal{B}$ es $B := (e_1, \ldots, e_n)$ (notemos la diferencia en la notación y en el uso de paréntesis).

Dado $v \in \mathbb{K}$, a la única n-úpla $v_B := (a_1, \ldots, a_n) \in \mathbb{K}^n$ tal que $v = a_1 v_1 + \ldots + a_n v_n$ se le llaman las *coordenadas de v respecto de B.*

Cuando usemos lenguaje matricial, nos convendrá escribir las coordenadas como columna:

$$v_B = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Por ejemplo, las bases ordenadas $B = (v_1, v_2, \ldots, v_n)$ y $B' = (v_2, v_1, \ldots, v_n)$ son reordenaciones distintas de la misma base $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ de V. Dado $v \in V$, si $v_B = (a_1, \ldots, a_n)$ entonces $v_{B'} = (a_2, a_1, \ldots, a_n)$. En particular, $v_B \neq v_{B'}$.

Sea $B = (v_1, \ldots, v_n)$ una base ordenada de $V(\mathbb{K})$. Podemos entonces definir una biyección

$$f_B \colon V \to \mathbb{K}^n, \qquad v \mapsto f_B(v) = v_B. \tag{2.12}$$

Es fácil comprobar que se cumple:

$$f_B(a\,u + b\,v) = a\,f_B(u) + b\,f_B(v), \quad \forall a, b \in \mathbb{K},\ \forall u, v \in V. \tag{2.13}$$

(esto es lo que en el próximo tema llamaremos un *isomorfismo de espacios vectoriales*). Notemos que esta manera de identificar V con $\mathbb{K}^n$ depende de B.

Nota 2.7.1 Una consecuencia directa de lo anterior es que $\mathbb{R}(\mathbb{Q})$ (ver la Nota 2.1.2) *no es finitamente generado*: si existiera una base B de $\mathbb{R}(\mathbb{Q})$ con $n \in \mathbb{N}$ vectores, la aplicación $f_B \colon \mathbb{R} \to \mathbb{Q}^n$ sería biyectiva, lo que contradice que $\mathbb{R}$ *no* es numerable.

Veamos algunos ejemplos de coordenadas en bases ordenadas.

1. En $\mathbb{K}^n$, la *base ordenada usual* es $B_u = (e_1, \ldots, e_n)$, obtenida a partir de $\mathcal{B}_u = \{e_1, \ldots, e_n\}$. Como cada vector $v = (x_1, \ldots, x_n) \in \mathbb{K}^n$ se expresa como $v = x_1\, e_1 + \ldots + x_n\, e_n$, las coordenadas de v respecto de B_u coinciden con v, $v_B = v$. Esta es una propiedad exclusiva de B_u que facilita mucho los cálculos.

2. En $\mathcal{M}_{m\times n}(\mathbb{K})$, la *base ordenada usual* es

$$B_u = (E_{11}, E_{12}, \ldots, E_{1n}, E_{21}, \ldots, E_{mn}),$$

que es una de las $(mn)!$ ordenaciones de la base usual $\mathcal{B}_u = \{E_{ij}\,|\, i = 1, \ldots, m,\ j = 1, \ldots, n\}$. Cada $A = (a_{ij})_{i,j} \in \mathcal{M}_{m\times n}(\mathbb{K})$ se escribe como $A = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij}\, E_{ij}$, luego las componentes de A coinciden con sus coordenadas en B_u, pero en A_{B_u} las entradas de A se disponen horizontalmente: primero la primera fila de A, seguida de la segunda, etc.

3. En $\mathbb{K}_n[x] = \{p(x) \in \mathbb{K}[x] \mid \text{grado}(p(x)) \leq n\}$, la *base ordenada usual* es

$$B_u = (p_0(x) = 1, p_1(x) = x, \ldots, p_n(x) = x^n).$$

En particular, $\dim_{\mathbb{K}} \mathbb{K}_n[x] = n+1$. Como cada $p(x) = a_0 + a_1\, x + \ldots + a_n\, x^n \in \mathbb{K}_n[x]$ se escribe $p(x) = a_0\, p_0(x) + a_1\, p_1(x) + \ldots + a_n\, p_n(x)$, concluimos que las coordenadas de $p(x)$ respecto de B_u coinciden con los coeficientes del polinomio ordenados de menor a mayor.

En general, el cálculo de las coordenadas de un vector respecto de una base ordenada equivale a resolver un SEL compatible determinado. Veámoslo con un ejemplo.

Ejemplo 2.7.1 En $\mathbb{R}^2$ consideramos los vectores $v_1 = (1, 0)$ y $v_2 = (-1, 1)$. Como claramente $\{v_1, v_2\}$ es linealmente independiente y $\dim_{\mathbb{R}} \mathbb{R}^2 = 2$, tenemos que $B = (v_1, v_2)$ es una base ordenada de $\mathbb{R}^2(\mathbb{R})$. Dado $v = (x, y) \in \mathbb{R}^2$, las coordenadas de v respecto de B son $v_B = (a, b) \in \mathbb{R}^2$ tales que $v = a\, v_1 + b\, v_2$. Operando y tomando componentes llegamos a la igualdad $(x, y) = (a - b, b)$, es decir, obtenemos el SEL

$$\left.\begin{array}{rrcl} a & -b & = & x \\ & b & = & y \end{array}\right\}$$

que es compatible determinado con soluciones $a = x + y$, $b = y$. Por tanto $v_B = (x + y, y)$.

Un mismo vector puede tener coordenadas distintas en distintas bases ordenadas (salvo el vector cero, cuyas coordenadas respecto a cualquier base ordenada son $(0, \ldots, 0)$). De hecho, dado un espacio vectorial $V(\mathbb{K})$ con $\dim_{\mathbb{K}} V = n \in \mathbb{N}$ y $v \in V \setminus \{0\}$, existe una base ordenada B de V tal que $v_B = (1, 0, \ldots, 0) \in \mathbb{K}^n$.

> ¿Qué relación existe entre las coordenadas de un mismo vector en dos bases ordenadas distintas?

Tomemos dos bases ordenadas $B = (v_1, \ldots, v_n)$ y $B' = (v'_1, \ldots, v'_n)$ de $V(\mathbb{K})$. Dado $v \in V$, queremos relacionar v_B y $v_{B'}$. Para ello, expresamos los vectores de B en combinación lineal de los de B':

$$v_j = \sum_{i=1}^{n} a_{ij} v'_i, \quad \forall j = 1, \ldots, n. \tag{2.14}$$

De esta forma, los coeficientes anteriores son únicos ya que $(v_j)_{B'} = (a_{1j}, \ldots, a_{nj}) \in \mathbb{K}^n$ son las coordenadas de v_j respecto de B'. Disponemos estas coordenadas **por columnas** en una matriz:

Definición 2.7.2 En las condiciones anteriores, la *matriz de cambio de base de B a B'* es

$$M(1_V, B, B') = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} = \begin{pmatrix} \boxed{(v_1)_{B'}} & \boxed{(v_2)_{B'}} & \ldots & \boxed{(v_n)_{B'}} \end{pmatrix}.$$

Por ejemplo:

- Si $B = B'$ entonces $M(1_V, B, B) := M(1_V, B) = I_n$.
- Dada una base ordenada B de $\mathbb{K}^n$, la matriz $M(I, B, B_u)$ es la que tiene por columnas a las componentes de los vectores de B.

Volviendo al caso general:

Proposición 2.7.2 (cambio de base) *Sean $B = (v_1, \ldots, v_n)$ y $B' = (v'_1, \ldots, v'_n)$ dos bases ordenadas de un espacio vectorial $V(\mathbb{K})$. Dado $v \in V$, la relación entre las coordenadas $v_B, v_{B'}$ es*

$$v_{B'} = M(1_V, B, B')\, v_B. \tag{2.15}$$

Demostración. Pongamos $v_B = (a_1, \ldots, a_n)$, $v_B = (a'_1, \ldots, a'_n) \in \mathbb{K}^n$. Entonces,

$$v = \sum_{j=1}^{n} a_j v_j = \sum_{j=1}^{n} a_j v_j \overset{(2.14)}{=} \sum_{j=1}^{n} a_j \sum_{i=1}^{n} a_{ij} v'_i = \sum_{i,j=1}^{n} a_{ij} a_j v'_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} a_j \right) v'_i,$$

luego

$$a'_i = \sum_{j=1}^{n} a_{ij} a_j, \qquad \forall i = 1, \ldots, n, \tag{2.16}$$

que matricialmente es (2.15). □

Definición 2.7.3 A cualquiera de las ecuaciones (2.15) o (2.16) se les llama las *ecuaciones de cambio de base de B a B'.*

Si hacemos las ecuaciones de cambio de base de B' a B de forma análoga a (2.15), obtendremos $v_B = M(1_V, B', B)\, v_{B'}$. Por tanto,

$$v_B = M(1_V, B', B)\, v_{B'} \overset{(2.15)}{=} M(1_V, B', B)\, M(1_V, B, B')\, v_B,$$

y como $v_B \in \mathbb{K}^n$ es arbitrario, deducimos que

$$M(1_V, B', B)\, M(1_V, B, B') = I_n. \tag{2.17}$$

Cambiando los papeles de B y B' se deduce igualmente que

$$M(1_V, B, B')\, M(1_V, B', B) = I_n. \tag{2.18}$$

De (2.17) y (2.18) deducimos lo siguiente.

Lema 2.7.1 *Sean $B = (v_1, \ldots, v_n)$ y $B' = (v'_1, \ldots, v'_n)$ dos bases ordenadas de un espacio vectorial $V(\mathbb{K})$. Entonces, la matriz de cambio de base $M(1_V, B', B)$ es regular, y su inversa es*

$$M(1_V, B', B)^{-1} = M(1_V, B, B').$$

Ejemplo 2.7.2 En $\mathbb{R}^2$ consideramos la base ordenada $B = (v_1, v_2)$ con $v_1 = (1, 0)$ y $v_2 = (-1, 1)$ del Ejemplo 2.7.1. Ya vimos que, para cada $v = (x, y) \in \mathbb{R}^2$ se tiene $v_B = (x+y, y)$. Esto se podría haber hecho usando un cambio de base: por la Proposición 2.7.2,

$$v_B = M(I, B_u, B)\, v_{B_u}, \text{ donde } M(I, B_u, B) = ((e_1)_B | (e_2)_B). \tag{2.19}$$

Pero es fácil comprobar que $(e_1)_B = (1, 0)$, $(e_2)_B = (1, 1)$ luego

$$M(I, B_u, B) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Usando lo anterior en (2.19),

$$v_B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + y \\ y \end{pmatrix},$$

y llegamos al mismo resultado de antes.

Lema 2.7.2 *Sean B, B', B'' tres bases ordenadas de un espacio vectorial $V(\mathbb{K})$. Entonces, $M(I, B, B'') = M(I, B', B'') \cdot M(I, B, B')$.*

Demostración. Pongamos $B = (v_1, \ldots, v_n)$, $B' = (v'_1, \ldots, v'_n)$, $B'' = (v''_1, \ldots, v''_n)$. Razonando como en (2.14)

$$\begin{aligned} v_j &= \sum_{i=1}^n a_{ij} v'_i, \quad \forall j = 1, \ldots, n, \\ v'_i &= \sum_{k=1}^n b_{ki} v''_k, \quad \forall j = 1, \ldots, n, \end{aligned}$$

luego $\quad \forall j = 1, \ldots, n,$

$$\begin{aligned} v_j &= \sum_{i=1}^n a_{ij} v'_i = \sum_{i=1}^n a_{ij} \sum_{k=1}^n b_{ki} v''_k = \sum_{k=1}^n \left(\sum_{i=1}^n b_{ki} a_{ij} \right) v''_k \\ &= \sum_{k=1}^n \big(M(1_V, B', B'') \cdot M(1_V, B, B') \big)_{kj} v''_k, \end{aligned}$$

de donde $M(I, B, B'') = M(I, B', B'') \cdot M(I, B, B')$. □

2.8. Fórmula de Grassmann

Teorema 2.8.1 (Fórmula de Grassmann) *Sea $V(\mathbb{K})$ un espacio vectorial y $U_1, U_2 \leq V$ finitamente generados. Entonces,*

$$\dim_{\mathbb{K}}(U_1 + U_2) = \dim_{\mathbb{K}} U_1 + \dim_{\mathbb{K}} U_2 - \dim_{\mathbb{K}}(U_1 \cap U_2).$$

Demostración. Llamemos $m = \dim_{\mathbb{K}}(U_1 \cap U_2)$ y $n_i = \dim_{\mathbb{K}} U_i$ para cada $i = 1, 2$. Queremos probar que $\dim_{\mathbb{K}}(U_1 + U_2) = n_1 + n_2 - m$, luego basta construir una base de $U_1 + U_2$ con $n_1 + n_2 - m$ vectores.

Por el momento supondremos que $m > 0$, después discutiremos cómo adaptar lo que sigue al caso $m = 0$. Sea $\mathcal{B}_{U_1 \cap U_2} = \{v_1, \ldots, v_m\}$ una base de $U_1 \cap U_2$. Aplicando el Teorema de Ampliación de la Base a $\mathcal{B}_{U_1 \cap U_2}$ viendo $U_1 \cap U_2$ como subespacio vectorial de U_i (aquí $i = 1, 2$), $\exists v^i_{m+1}, \ldots, v^i_{n_i} \in U_i$ tales que $\mathcal{B}_i := \{v_1, \ldots, v_m, v^i_{m+1}, \ldots, v^i_{n_i}\}$ es una base de U_i. Llamemos $W_i := L(\{v^i_{m+1}, \ldots, v^i_{n_i}\})$, que es un subespacio suplementario de $U_1 \cap U_2$ en U_i (si fuera $U_1 \cap U_2 = U_i$, entonces $W_i = \{0\}$), es decir $U_i = (U_1 \cap U_2) \oplus W_i$, para cada $i = 1, 2$. Veamos que

$$U_1 \cap W_2 = \{0\} \qquad \text{(y análogamente } U_2 \cap W_1 = \{0\}\text{):} \tag{2.20}$$

Por construcción de W_2, $\{0\} = (U_1 \cap U_2) \cap W_2 = U_1 \cap (U_2 \cap W_2) = U_1 \cap W_2$ luego tenemos probado (2.20).

Consideremos ahora el conjunto de $m + (n_1 - m) + (n_2 - m) = n_1 + n_2 - m$ vectores:

$$\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 = \{v_1, \ldots, v_m, v^1_{m+1}, \ldots, v^1_{n_1}, v^2_{m+1}, \ldots, v^2_{n_2}\}.$$

Veamos que $\mathcal{B}$ es una base de $U_1 + U_2$ y habremos terminado.
$\boxed{\mathcal{B} \text{ es sistema de generadores de } U_1 + U_2\text{:}}$ $L(\mathcal{B}) = L(\mathcal{B}_1 \cup \mathcal{B}_2) = L(\mathcal{B}_1) + L(\mathcal{B}_2) = U_1 + U_2$.
$\boxed{\mathcal{B} \text{ es linealmente independiente:}}$ Consideramos una combinación lineal

$$\sum_{i=1}^{m} a_i\, v_i + \sum_{i=m+1}^{n_1} b_i\, v^1_i + \sum_{i=m+1}^{n_2} c_i\, v^2_i = 0,$$

con $a_1, \ldots, a_m, b_{m+1}, \ldots, b_{n_1}, c_{m+1}, \ldots, c_{n_2} \in \mathbb{K}$. Claramente, la igualdad anterior es equivalente a:

$$\sum_{i=1}^{m} a_i\, v_i + \sum_{i=m+1}^{n_1} b_i\, v^1_i = -\sum_{i=m+1}^{n_2} c_i\, v^2_i, \tag{2.21}$$

El miembro izquierdo de (2.21) es un vector de U_1 y el derecho está en W_2. Usando (2.20), los dos miembros de (2.21) son cero:

$$\sum_{i=1}^{m} a_i\, v_i + \sum_{i=m+1}^{n_1} b_i\, v^1_i = 0 = \sum_{i=m+1}^{n_2} c_i\, v^2_i.$$

De esto deducimos que todos los coeficientes se anulan, ya que $\mathcal{B}_1$ es linealmente independiente y $\{v^2_{m+1}, \ldots, v^2_{n_2}\} \subset \mathcal{B}_2$, que también es linealmente independiente.

Queda explicar cómo adaptar el argumento anterior al caso $m = \dim_{\mathbb{K}}(U_1 \cap U_2) = 0$. En este caso, $U_1 \cap U_2$ no tiene bases y no aplicaremos el Teorema de Ampliación de la Base sino que tomaremos directamente bases $\mathcal{B}_i$ de U_i, $i = 1, 2$, con lo que el argumento sigue siendo válido con $W_i = U_i$. □

Como consecuencia directa de la fórmula de Grassmann tenemos el siguiente resultado.

Corolario 2.8.1 *Sea $V(\mathbb{K})$ un espacio vectorial finitamente generado. Dados $U_1, U_2 \leq V$ tales que $\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} U_1 + \dim_{\mathbb{K}} U_2$, son equivalentes:*

1. $V = U_1 \oplus U_2$.
2. $V = U_1 + U_2$.
3. $U_1 \cap U_2 = \{0\}$.

2.9. Subespacios de $\mathbb{K}^n$ a partir de un conjunto de generadores

Las siguientes propiedades se deducen directamente de la Proposición 2.4.1 y del apartado 1 de la Proposición 2.6.1.

Lema 2.9.1 *Sea $V\mathbb{K}$ un espacio vectorial, $H = \{v_1, \dots, v_m\} \subset V$ y $U = L(H)$.*

1. *Si $a \in \mathbb{K} \setminus \{0\}$ e $i = 1, \dots, m$, entonces $\{v_1, \dots, a\, v_i, \dots, v_m\}$ es un sistema de generadores de U.*

2. *Si $a \in \mathbb{K}$ y $1 \leq i < j \leq m$, entonces $\{v_1, \dots, v_i, \dots, v_j + a\, v_i, \dots, v_m\}$ es un sistema de generadores de U.*

Veamos cómo aplicar el lema previo para calcular una base de $U = L(H)$, donde $H = \{v_1, \dots, v_m\} \subset \mathbb{K}^n$. Disponemos los v_i por filas, creando una matriz $A \in \mathcal{M}_{m\times n}(\mathbb{K})$ cuya fila i-ésima es v_i, $i = 1, \dots, m$. El lema anterior nos dice que, aplicando a A transformaciones elementales por filas (incluido cambiar de orden dos filas) obtenemos un nuevo sistema de generadores de U. Procedemos como en el método de Gauss, realizando transformaciones por filas hasta conseguir la matriz de un SEL escalonado. Entonces, las filas no nulas de la matriz final producen vectores linealmente independientes que generan a U y por tanto son una base de U. Es número de estas filas linealmente independientes es $\dim_{\mathbb{K}} U$.

Ejemplo 2.9.1 Calculemos una base y la dimensión del subespacio vectorial de $\mathbb{R}^4$ dado por $U = L(H)$, donde $H = \{(1, -2, 1, 0), (2, 3, -2, 1), (4, -1, 0, 1)\}$. Escribiendo los generadores por filas asociamos la matriz

$$A = \begin{pmatrix} 1 & -2 & 1 & 0 \\ 2 & 3 & -2 & 1 \\ 4 & -1 & 0 & 1 \end{pmatrix}$$

Aplicamos transformaciones elementales por filas hasta conseguir la matriz de un SEL escalonado:

$$M \sim \begin{pmatrix} 1 & -2 & 1 & 0 \\ 0 & 7 & -4 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Como el vector nulo se puede eliminar de cualquier sistema de generadores, tenemos que $B_U = \{(1, -2, 1, 0), (0, 7, -4, 1)\}$ sigue siendo un sistema de generadores de U. Como B_U es claramente linealmente independiente, B_U es una base de U y $\dim_{\mathbb{R}} U = 2$.

Nota 2.9.1 El procedimiento anterior se podrá aplicar a cualquier sistema de generadores finito H de un subespacio vectorial U de cualquier espacio vectorial $V(\mathbb{K})$ finitamente generado: para esto fijaremos una base ordenada B de $V(\mathbb{K})$, tomaremos las coordenadas de los elementos de H en esa base y consideraremos el subespacio $U' \leq \mathbb{K}^n$ generado por estas listas de coordenadas. La base de U' que se obtenga mediante el procedimiento anterior proporciona las coordenadas en B de una base de U. Para dar una justificación rigurosa de esto, debemos esperar al tema siguiente.

2.10. Ecuaciones de un subespacio vectorial

Recordemos que si $V(\mathbb{K})$ es un espacio vectorial finitamente generado, y $U \leq V$, entonces U también es finitamente generado con $\dim_{\mathbb{K}} U \leq \dim_{\mathbb{K}} V$ (Corolario 2.6.2), y que $\dim_{\mathbb{K}} U = \dim_{\mathbb{K}} V$ si y sólo si $U = V$ (Corolario 2.6.4). Nuestro siguiente objetivo es caracterizar cuándo una elección de coordenadas respecto a una base ordenada B de V produce un vector de U. Resolveremos esto en el caso particular $V = \mathbb{K}^n$, a la espera de poder extenderlo a cualquier espacio vectorial $V^n(\mathbb{K})$ (y subespacio suyo) en el tema siguiente, vía el isomorfismo de espacios vectoriales $f_B \colon V \to \mathbb{K}^n$ asociado a una base ordenada de V.

2.10.1. Ecuaciones paramétricas de un subespacio de $\mathbb{K}^n$

Sea $U \leq \mathbb{K}^n$ con $\dim_{\mathbb{K}} U = k \geq 1$. Tomemos una base ordenada $B_U = (u_1, u_2, \ldots, u_k)$ de U. Como $U = L(B_U)$, los vectores de U son de la forma

$$v = \lambda_1 u_1 + \lambda_2 u_2 + \ldots + \lambda_k u_k \tag{2.22}$$

con $\lambda_i \in \mathbb{K}$ $\forall i = 1, \ldots, k$. Escribiendo $v = (x_1, x_2, \ldots, x_n)$ y $u_j = (c_{1j}, c_{2j}, \ldots, c_{nj})$ (coordenadas en la base usual), la igualdad (2.22) se escribe

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \lambda_1 \begin{pmatrix} c_{11} \\ c_{21} \\ \vdots \\ c_{n1} \end{pmatrix} + \cdots + \lambda_k \begin{pmatrix} c_{1k} \\ c_{2k} \\ \vdots \\ c_{nk} \end{pmatrix}$$

o, por componentes,

$$\left.\begin{array}{ll} x_1 & = c_{11}\,\lambda_1 + c_{12}\,\lambda_2 + \ldots + c_{1k}\,\lambda_k, \\ x_2 & = c_{21}\,\lambda_1 + c_{22}\,\lambda_2 + \ldots + c_{2k}\,\lambda_k, \\ \vdots & \qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ x_n & = c_{n1}\,\lambda_1 + c_{n2}\,\lambda_2 + \ldots + c_{nk}\,\lambda_k, \end{array}\right\} \tag{2.23}$$

(2.23) se llaman las *ecuaciones paramétricas de* U *respecto de la base ordenada* B_U *y la base usual de* $\mathbb{K}^n$. Notemos que

- Hay n ecuaciones paramétricas, con $k = \dim_{\mathbb{K}} U$ parámetros $\lambda_1, \ldots, \lambda_k$.
- Los coeficientes que acompañan a cada λ_i son las coordenadas de u_i por columnas en la base usual B_u.
- Cuando damos cada parámetro un valor concreto, obtenemos un vector $u \in U$, y u_{B_U} es la lista de valores de los parámetros. En particular, el vector i-ésimo de B_U se recupera a partir de las ecuaciones paramétricas tomando $\lambda_1 = \cdots = \lambda_{i-1} = 0$, $\lambda_i = 1$, $\lambda_{i+1} = \cdots = \lambda_k = 0$.

Nota 2.10.1 Para extender lo anterior a un subespacio vectorial $U \neq \{0\}$ de un espacio vectorial $V(\mathbb{K})$ de dimensión n, fijaremos una base ordenada B de V y usaremos el isomorfismo de espacios vectoriales $f_B \colon V \to \mathbb{K}^n$ (ver tema siguiente), que llevará U es un subespacio vectorial $f_B(U) \leq \mathbb{K}^n$ con $\dim_{\mathbb{K}} f_B(U) = \dim_{\mathbb{K}} U$. Si B_U es una base ordenada de U, $f_B(B_U)$ es una base ordenada de $f_B(U)$, y ya podremos aplicar el procedimiento anterior para calcular las ecuaciones paramétricas de $f_B(U)$. Estas son las *ecuaciones paramétricas de* U *respecto de las bases ordenadas* B_U, B.

2.10.2. Ecuaciones paramétricas de las soluciones de un SEL homogéneo

Consideremos un SEL homogéneo $A\,x = 0$, con matriz de coeficientes $A \in \mathcal{M}_{m\times n}(\mathbb{K})$ e incógnitas $x \in \mathbb{K}^n \equiv \mathcal{M}_{n\times 1}(\mathbb{K})$. Recordemos que

1. Las soluciones de $A\,x = 0$, forman un subespacio vectorial $U \subset \mathbb{K}^n$ (Ejemplo 8 de la Sección 2.2.1).
2. Las transformaciones elementales de ecuaciones del SEL producen nuevos SEL equivalentes (Proposición 1.2.2).
3. El SEL original es equivalente a uno escalonado (Método de Gauss) con $r \in \{1, \ldots, m\}$ ecuaciones no nulas. En este SEL escalonado los coeficientes por filas son linealmente independientes y r es el rango por filas de la matriz original A. Este SEL escalonado permite distinguir r incógnitas principales, que denotaremos por $x_1, \ldots, x_r$ (tras posiblemente renombrar las incógnitas) y $n - r$ secundarias, $x_{r+1}, \ldots, x_n$.
4. Todas las soluciones de $A\,x = 0$ (todo los elementos de U) se construyen tomando valores arbitrarios para las incógnitas secundarias (parámetros) $x_{r+1} = \lambda_1, \ldots, x_n = \lambda_{n-r} \in \mathbb{K}$, y despejando escalonadamente las incógnitas principales en términos de esos parámetros. Estas son las ecuaciones paramétricas del subespacio U.

2.10.3. Ecuaciones implícitas de un subespacio vectorial

Definición 2.10.1 Sea $V(\mathbb{K})$ un espacio vectorial con $\dim_{\mathbb{K}} V = n$ y $U \leq V$ un subespacio vectorial con $\dim_{\mathbb{K}} U = k$. Dada una base ordenada B de V, las *ecuaciones implícitas*[7] *de U respecto a B* es un SEL homogéneo $A\,x = 0$ cuyo conjunto de soluciones coincide con las coordenadas de los vectores de U respecto de B.

A continuación veremos cómo calcular las ecuaciones implícitas de U respecto a una base ordenada B de V, y comprobaremos que éstas forman un SEL homogéneo de $n-k$ ecuaciones linealmente independientes con n incógnitas.

Sea $B_U = (u_1, \ldots, u_k)$ una base de U. Consideremos la matriz $C \in \mathcal{M}_{n\times k}(\mathbb{K})$ cuyas columnas son las coordenadas respecto de B de los vectores u_i:

$$C = \left(\boxed{(u_1)_B} \;\; \boxed{(u_2)_B} \;\; \cdots \;\; \boxed{(u_k)_B} \right).$$

Sea $v \in V$. Como B_U es base de U, deducimos que $v \in U$ si y sólo si el rango por columnas de la matriz $(C|v_B^t) \in \mathcal{M}_{n\times(k+1)}(\mathbb{K})$ es k. Las ecuaciones implícitas de U respecto a B tienen la misión de asegurar que la línea de las incógnitas es combinación lineal de las de los vectores de B_U. Una forma de hallarlas es imponiendo que todos los menores de orden $k+1$ de $(C|v_B^t)$ tienen determinante nulo. En realidad, sólo hay que anular $n-k$ de estos determinantes, ya que como C tiene rango por columnas igual a k (porque los vectores de B_U son linealmente independientes), el rango de C por filas también es k (por el teorema del rango), luego existe un menor M de orden k en C con determinante distinto de cero; ahora las $n-k$ ecuaciones que componen nuestro sistema homogéneo se obtienen anulando los $n-k$ determinantes obtenidos al orlar M mediante una fila de $(C|v_B^t)$ elegida fuera de M (hay $n-k$ de estas filas) y la porción correspondiente de la columna v_B^t.

Ejemplo 2.10.1 Calculemos las ecuaciones implícitas de la recta vectorial $U = L((1,3,-2)) \leq \mathbb{R}^3$ en la base usual B_u: Tomamos la base $B_U = \{(1,3,-2)\}$ de U; la discusión anterior nos dice que habrán $n-k = 3-1 = 2$ ecuaciones cartesianas de U.

Un vector $v = (x_1, x_2, x_3) \in \mathbb{R}^3$ pertenecerá a U si y sólo si es proporcional a $(1,3,-2)$. Esto equivale a que la matriz

$$(C|v_{B_u}^t) = \left(\begin{array}{r|c} 1 & x_1 \\ 3 & x_2 \\ -2 & x_3 \end{array} \right)$$

[7] O *cartesianas*.

tenga rango 1. Claramente, el menor $(a_{11}) = (1)$ de C tiene determinante no nulo. Orlamos dicho menor imponiendo

$$\begin{vmatrix} 1 & x_1 \\ 3 & x_2 \end{vmatrix} = x_2 - 3x_1 = 0, \qquad \begin{vmatrix} 1 & x_1 \\ -2 & x_3 \end{vmatrix} = x_3 + 2x_1 = 0$$

luego las ecuaciones implícitas de U son

$$\left.\begin{array}{rrrcl} -3x_1 & +x_2 & & = & 0 \\ 2x_1 & & +x_3 & = & 0 \end{array}\right\}.$$

Ejemplo 2.10.2 Calculamos las ecuaciones implícitas de $W = L(\{(1,3,-2),(1,1,1)\}) \leq \mathbb{R}^3$ en la base usual. Claramente, $B_W = \{(1,3,-2),(1,1,1)\}$ es linealmente independiente, luego W es un plano vectorial y B_W es una base de W. Esto nos dice que sólo hay $n - k = 3 - 2 = 1$ ecuación implícita. Un vector $v = (x_1, x_2, x_3) \in \mathbb{R}^3$ pertenecerá W si es combinación lineal de B_W o equivalentemente, la matriz

$$(C|v^t_{B_u}) = \left(\begin{array}{rr|c} 1 & 1 & x_1 \\ 3 & 1 & x_2 \\ -2 & 1 & x_3 \end{array}\right)$$

tiene rango 2. El menor $\begin{pmatrix} 1 & 1 \\ 3 & 1 \end{pmatrix}$ tiene rango 2 (porque su determinante es $-2 \neq 0$). Orlamos dicho menor imponiendo

$$\begin{vmatrix} 1 & 1 & x_1 \\ 3 & 1 & x_2 \\ -2 & 1 & x_3 \end{vmatrix} = x_3 - 2x_2 + 3x_1 + 2x_1 - 3x_3 - x_2 = 5x_1 - 3x_2 - 2x_3 = 0,$$

que es la ecuación implícita de U.

2.10.4. Ecuaciones de $U + W, U \cap W$

Sean U, W subespacios vectoriales de un espacio vectorial $V(\mathbb{K})$ finitamente generado.

Para calcular las **ecuaciones implícitas de** $U + W$ en una base ordenada B de V hacemos lo siguiente:

1. Calculamos bases B_U, B_W de U y W, por ejemplo a partir de ecuaciones paramétricas de U y W.

2. $B_U \cup B_W$ es un sistema de generadores de $U + W$, de donde extraemos una base B_{U+W} de $U + W$.

3. Aplicamos el proceso de la Sección 2.10.3 para calcular las ecuaciones implícitas de $U + W$ respecto de B.

Para calcular las **ecuaciones paramétricas de** $U + W$**:**

1. Calculamos una base B_{U+W} de $U + W$ como en el procedimiento anterior.
2. Aplicamos lo explicado en la Sección 2.10.1.

O bien, si hemos calculado las ecuaciones implícitas de $U + W$, resolvemos el sistema homogéneo asignando incógnitas principales y secundarias.

Para calcular las **ecuaciones implícitas de** $U \cap W$**:**

1. Calculamos las ecuaciones implícitas de U y de W por separado (respecto de la misma base ordenada B).
2. Unimos las ecuaciones de ambos sistemas y eliminamos las ecuaciones linealmente dependientes.

Para calcular las **ecuaciones paramétricas de** $U \cap W$**,** calculamos las ecuaciones implícitas de $U \cap W$, y luego resolvemos el sistema homogéneo asignando incógnitas principales y secundarias.

2.11. Ejercicios.

1. Demostrar que si V es un espacio vectorial sobre $\mathbb{K}$ entonces se cumplen las igualdades:

$$a\,(u - v) = a\,u - a\,v,$$
$$(a - b)\,v = a\,v - b\,v,$$

para todo $a, b \in \mathbb{K}$ y todo $u, v \in V$.

2. La propiedad 6) de la Proposición 2.1.1 sólo involucra el grupo $(V, +)$, pero en su demostración se usó el producto por escalares. Probar esa propiedad 6) directamente de las propiedades de $(V, +)$.

3. Sea $(V, +)$ un grupo (no se supone abeliano). Supongamos que $\mathbb{K}$ es un cuerpo y $\ : \mathbb{K} \times V \to V$ es una ley de composición externa cumpliendo las dos propiedades distributivas, pseudoasociativa y modular. Demostrar que la suma $+$ en V es conmutativa.

4. Probar que las operaciones dadas en (2.1) y (2.2) están bien definidas, es decir, no dependen del representante elegido en las clases de equipolencia de vectores fijos del plano o del espacio. Demostrar que el conjunto de vectores libres dotado de esas operaciones es un espacio vectorial.

5. En $\mathbb{R}^3$ consideramos la suma usual y el siguiente producto por escalares reales:

$$a(x_1, x_2, x_3) = (ax_1, ax_2, 3ax_3).$$

¿Es $\mathbb{R}^3$ un espacio vectorial real con estas operaciones?

6. Sean V_1 y V_2 dos espacios vectoriales sobre un mismo cuerpo $\mathbb{K}$. Demostrar que el producto cartesiano $V_1 \times V_2 = \{(v_1, v_2) : v_1 \in V_1,\ v_2 \in V_2\}$ es un espacio vectorial sobre $\mathbb{K}$ cuando se define la suma y el producto por elementos de $\mathbb{K}$ como:

$$\begin{array}{rcl}(u_1, u_2) + (v_1, v_2) & = & (u_1 + v_1, u_2 + v_2), \\ a\,(v_1, v_2) & = & (a\,v_1, a\,v_2),\end{array}$$

para todo $(u_1, u_2), (v_1, v_2) \in V_1 \times V_2$ y todo $a \in \mathbb{K}$. A esta estructura se la llama *espacio vectorial producto*.

7. Probar que $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$ tiene estructura de espacio vectorial real con las siguientes operaciones $\oplus, \odot\mathbb{R}$:

$$\begin{array}{rcl}x \oplus y & = & x\,y, \\ a \odot x & = & x^a = e^{a \log x},\end{array}$$

¿Cuál es el neutro para la suma $\oplus$?

8. ¿Cuáles de los siguientes subconjuntos de $\mathbb{R}^3$ son subespacios vectoriales suyos?

   a) $U_1 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 + x_2 + 2x_3 = 0\}$.

   b) $U_2 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1^2 = x_2\}$.

   c) $U_3 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 + x_2 = 0 = x_1 - x_3 = 0\}$.

9. Probar que $\{A \in \mathcal{M}_n(\mathbb{K}) \mid \text{Traza}(A) = 0\}$ es un subespacio vectorial de $\mathcal{M}_n(\mathbb{K})$ (la traza de una matriz cuadrada se definió en (1.1)).

10. En $\mathcal{M}_3(\mathbb{C})$ considera el subconjunto $U = \{M \in \mathcal{M}_3(\mathbb{C}) \mid \overline{M} = M\}$. ¿Es U un subespacio vectorial de $\mathcal{M}_3(\mathbb{C})$ ¿Y de $(\mathcal{M}_3(\mathbb{C}), +, \cdot\mathbb{R})$?

11. Demostrar que un subconjunto U no vacío de un espacio vectorial $V(\mathbb{K})$ es un subespacio vectorial si y sólo si cumple

$$a\,u + v \in U, \quad \forall a \in \mathbb{K}, \forall u, v \in U. \tag{2.24}$$

12. Demostrar que $U_1 + U_2 = \mathbb{R}^2$, donde U_1 y U_2 son los subespacios dados por $U_1 = \{(x, y) \in \mathbb{R}^2 : y = 0\}$ y $U_2 = \{(x, y) \in \mathbb{R}^2 : x = 0\}$.

13. Sean U_1 y U_2 los subespacios de $\mathbb{R}^2$ del Ejercicio 12. Demostrar que $\mathbb{R}^2 = U_1 \oplus U_2$.

14. En $\mathcal{M}_2(\mathbb{R})$ se consideran las siguientes matrices:

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad M_4 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

   Probar que ninguna de ellas es combinación lineal de las otras tres.

15. En el espacio vectorial $V = \{f \colon \mathbb{R} \to \mathbb{R} \mid f \text{ es continua}\}$, probar que el vector $f(t) = \cos(2t)$ no se puede escribir como combinación lineal de los vectores $f_1(t) = \cos t$, $f_2(t) = \text{sen}t$.

16. En el espacio vectorial $\mathbb{C}^3(\mathbb{C})$, probar que cualquier vector es combinación lineal de los siguientes tres vectores:

$$v_1 = (i, 1, 0), \quad v_2 = (-i, 1, 0), \quad v_3 = (0, 0, 1 - i).$$

   Es lo anterior cierto si cambiamos $\mathbb{C}^3(\mathbb{C})$ por $\mathbb{C}^3(\mathbb{R})$?

17. Comprobar que la Proposición 2.4.1 es válida cuando H es infinito, obteniéndose que si $H \subset V$ es un sistema de generadores de V, se cumplen:

   a) Si $H' \subset V$ cumple $H \subset H'$, entonces H' es un sistema de generadores de V.

b) Si $v \in H$ y $v \in L(H \setminus \{v\})$, entonces $H \setminus \{v\}$ es un sistema de generadores de V.

18. Encontrar un sistema de generadores de las matrices simétricas $\mathcal{S}_n(\mathbb{K})$ y otro de las antisimétricas $\mathcal{A}_n(\mathbb{K})$.

19. En $\mathbb{C}^2$ se considera $U = \{(z_1, z_2) \in \mathbb{C}^2 \mid 2z_1 - z_2 = 0\}$.

    a) Probar que U es un subespacio vectorial de $\mathbb{C}^2(\mathbb{C})$ y de $\mathbb{C}^2(\mathbb{R})$.

    b) Encontrar sistemas de generadores de U visto como un espacio vectorial complejo y como espacio vectorial real.

20. Sean V, V' dos espacios vectoriales sobre el mismo cuerpo $\mathbb{K}$. En $V \times V'$ consideramos la estructura de espacio vectorial producto.

    a) Demostrar que si $H \subset V$, $H' \subset V'$ son sistemas de generadores de V y V' respectivamente, entonces

    $$\{(x, 0') \mid x \in H\} \cup \{(0, x') \mid x' \in H'\}$$

    es un sistema de generadores de $V \times V'$.

    b) Probar que si V y V' son finitamente generados, entonces $V \times V'$ también es finitamente generado y $\dim_{\mathbb{K}}(V \times V') = \dim_{\mathbb{K}} V + \dim_{\mathbb{K}} V'$.

21. En $\mathbb{R}_2[x]$, probar que los siguientes polinomios son linealmente independientes:

    $$P_1(x) = 1 + x + x^2, \quad P_2(x) = 1 + x, \quad P_3(x) = 1 - x.$$

22. En $\mathcal{S}_n(\mathbb{R})$, probar que las siguientes matrices son linealmente independientes:

    $$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

23. Sea V un espacio vectorial sobre $\mathbb{R}$. Supongamos que $\{x, y, z\} \subset V$ es linealmente independiente. Probar que $\{x, x + y, x + y - z\}$ es también linealmente independiente, y que el recíproco es cierto.

24. En el espacio vectorial $\mathcal{F}(\mathbb{R}, \mathbb{R})$ cuyos vectores son las aplicaciones $f : \mathbb{R} \to \mathbb{R}$ (con la suma y el producto por escalares usuales), se consideran las funciones $f, g, h \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ dadas por $f(x) = x^2 + 1$, $g(x) = 2x$, $h(x) = 3^x$, $\forall x \in \mathbb{R}$. ¿Es $\{f, g, h\}$ linealmente independiente?

25. Sea H un subconjunto del espacio vectorial de polinomios $\mathbb{R}[x]$, de forma que S no contiene al polinomio nulo y no hay en H dos polinomios con el mismo grado. Probar que H es linealmente independiente.

26. Demostrar que el conjunto $\{3, \sqrt{2}\}$ es linealmente independiente en $\mathbb{R}(\mathbb{Q})$ pero linealmente dependiente en $\mathbb{R}(\mathbb{R})$.

27. Estudiar si el conjunto $S = \{(1, 0, -1), (1, 2, 5), (-2, 1, 3)\}$ es una base de $\mathbb{R}^3$.

28. En $\mathcal{F}(\mathbb{R}, \mathbb{R})$, se consideran $U = \{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \mid f(-x) = f(x),\ \forall x \in \mathbb{R}\}$ (funciones pares) y $W = \{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \mid f(-x) = -f(x),\ \forall x \in \mathbb{R}\}$ (funciones impares). Probar que U, W son subespacios vectoriales de $\mathcal{F}(\mathbb{R}, \mathbb{R})$ y que $\mathcal{F}(\mathbb{R}, \mathbb{R}) = U \oplus W$.

29. Encontrar cuatro subconjuntos finitos $H_i \subset \mathbb{R}^2$ con $i = 1, 2, 3, 4$, tales que H_1 sea sistema de generadores pero no linealmente independiente, H_2 sea sistema de generadores y linealmente independiente, H_3 no sea sistema de generadores pero sí linealmente independiente y H_4 no sea sistema de generadores ni linealmente independiente (esto nos dice que no existe relación entre el concepto de sistema de generadores y el de conjunto linealmente independiente más allá del teorema de Steinitz).

30. Sea $V(\mathbb{K})$ un espacio vectorial finitamente generado y $H, H' \subset V$ dos subconjuntos finitos tales que $H' \subset H$, H es sistema de generadores y H' es linealmente independiente. Probar que existe una base $\mathcal{B}$ de V tal que $H' \subseteq \mathcal{B} \subset H$.

31. Probar con detalle la Proposición 2.3.1.

32. Probar que si $\{v_1, \ldots, v_n\}$ es base de un espacio vectorial $V(\mathbb{C})$, entonces
$$\{v_1, \ldots, v_n, iv_1, \ldots, iv_n\}$$
es base de $V(\mathbb{R})$. Relacionar las dimensiones de $V(\mathbb{C})$ y $V(\mathbb{R})$.

33. Sea $V(\mathbb{K})$ un espacio vectorial y $B = (v_1, \ldots, v_n)$ una base ordenada de V. ¿Qué coordenadas tiene el vector nulo respecto de B? ¿Y cada uno de los vectores v_i?

34. Sea $\mathbb{K}$ un cuerpo conmutativo con característica $\neq 2$. Calcular una base de $\mathcal{S}_n(\mathbb{K})$ y otra de $\mathcal{A}_n(\mathbb{K})$. ¿Qué dimensiones tienen estos espacios vectoriales? ¿Es $\mathcal{M}_n(\mathbb{K})$ suma directa de $\mathcal{S}_n(\mathbb{K})$ y $\mathcal{A}_n(\mathbb{K})$?

35. Probar que $\mathcal{M}_2(\mathbb{K})$ no es suma directa de $\mathcal{S}_2(\mathbb{R})$ y $W = \{A \in \mathcal{M}_n(\mathbb{R}) \mid \text{Traza}(A) = 0\}$, pero sí es suma.

36. Una matriz $A \in \mathcal{M}_n(\mathbb{K})$ se dice triangular superior si $a_{ij} = 0$ siempre que $i < j$, triangular inferior si $a_{ij} = 0$ siempre que $i > j$, y diagonal si $a_{ij} = 0$ siempre que $i \neq j$.

    a) Probar que si $\mathcal{T}_s, \mathcal{T}_i, \mathcal{D} \subset \mathcal{M}_n(\mathbb{K})$ denotan los subconjuntos respectivos de matrices triangulares superiores, inferiores y diagonales, entonces $\mathcal{T}_s, \mathcal{T}_i, \mathcal{D}$ son subespacios vectoriales de $\mathcal{M}_n(\mathbb{K})$.

b) Demostrar que $\mathcal{M}_n(\mathbb{K}) = \mathcal{T}_s + \mathcal{T}_i + \mathcal{D}$. ¿Es esta suma directa?

37. Sea V un espacio vectorial sobre $\mathbb{K}$ y $H = \{x_1, , \ldots, x_m\}$ un sistema de generadores de V tal que al quitarle cualquiera de sus vectores, el subconjunto resultante ya no es sistema de generadores de V. Probar que H es una base de V.

38. Usar la idea de la Nota 2.7.1 para demostrar que si $V(\mathbb{R})$ es un espacio vectorial con dim$_{\mathbb{R}}V > 0$, entonces $V(\mathbb{Q})$ no es finitamente generado.

39. Sea V un espacio vectorial sobre $\mathbb{K}$ y U, W dos subespacios vectoriales de V. Supongamos que $\{x_1, \ldots, x_m\}$ es una base de U y $\{x'_1, \ldots, x'_k\}$ una base de W.

    a) Probar que $V = U + W$ si y sólo si $\{x_1, \ldots, x_m, x'_1, \ldots, x'_k\}$ es un sistema de generadores de V.

    b) Probar que $V = U \oplus W$ si y sólo si $\{x_1, \ldots, x_m, x'_1, \ldots, x'_k\}$ es una base de V.

40. Sea $V(\mathbb{K})$ un espacio vectorial y $\{U_1, U_2, U\}$ subespacios de V, U finitamente generado, tales que $U_1, U_2 \subset U$. Demostrar que son equivalentes:

    (i) $U = U_1 \oplus U_2$.

    (ii) $\dim_{\mathbb{K}}(U) = \dim_{\mathbb{K}}(U_1) + \dim_{\mathbb{K}}(U_2)$.

    (iii) Para cada base de U_i, $i = 1, 2$, se tiene que $\mathcal{B}_1 \cup \mathcal{B}_2$ es una base de U.

    ¿Se puede obtener toda base de U como en el punto (iii)?

41. Sea V un espacio vectorial sobre $\mathbb{K}$ y U, W dos subespacios vectoriales de V. Probar que si $\dim_U + \dim_{\mathbb{K}} W > \dim_K V$, entonces $U \cap W$ contiene un vector no nulo. ¿Es el recíproco cierto?

42. Sea $V(\mathbb{K})$ un espacio vectorial y $U_1, \ldots U_k \leq V$ subespacios vectoriales finitamente generados de $V(\mathbb{K})$. Entonces:

$$\dim_{\mathbb{K}}\left(\sum_{i=1}^{k} U_i\right) + \sum_{i=1}^{k-1} \dim_{\mathbb{K}}\left[(U_1 + \ldots + U_j) \cap U_{j+1}\right] = \sum_{i=1}^{m} \dim_{\mathbb{K}} U_i.$$

43. Calcular dos subespacios suplementarios distintos en $\mathbb{K}^4$, del subespacio

$$U = \{(x_1, x_2, x_3, x_4) \in \mathbb{K}^4 \mid x_1 - x_4 = x_2 - x_3 = 0\},$$

    de manera que ambos contengan al vector $(1, 1, -1, -1)$.

44. Calcular un subespacio suplementario del subespacio $U = \{p(x) \in \mathbb{R}_3[x] \mid p(1) = p'(-1) = 0\}$ en $\mathbb{R}_3[x]$ que contenga al polinomio $q(x) = x^2$.

45. Calcular las coordenadas de los polinomios $P(x) = 2 - 2x + x^2, Q(x) = 1 - 5x$ de $\mathbb{C}_2[x]$ en la base ordenada $B = (1 + x, 1 - x, x^2)$.

46. En $V = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ es continua}\}$ se considera el subespacio generado por las funciones $f(t) = 1$, $h(t) = \cos(2t)$, $\forall t \in \mathbb{R}$.

    a) Demostrar que $\{f, h\}$ forman base de U.

    b) Probar que las funciones $\varphi(t) = \cos^2 t, \psi(t) = \text{sen}^2 t$ pertenecen a U.

    c) Calcular las coordenadas de φ y ψ respecto de la base ordenada (f, h).

47. Calcular dos bases de $\mathbb{C}^2(\mathbb{C})$ de manera que una de las matrices de cambio de base sea
$$\begin{pmatrix} 1-i & 2 \\ 1+i & 1 \end{pmatrix}.$$

48. En el espacio vectorial $\mathcal{A}_3(\mathbb{R})$, calcular dos bases que contengan a la matriz
$$\begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}.$$
Calcular también las correspondientes matrices de cambio de base.

49. En el espacio vectorial $V = \{p(x) \in \mathbb{R}[x] \mid \text{grado}(p(x)) \leq 3\}$, probar que $U = \{p[x] \in V \mid p'(1) = 0\}$ es un subespacio vectorial de V. Encontrar una base ordenada de V/U y en ella, calcular las coordenadas de $(1 + x) + U$.

50. Sea V un espacio vectorial sobre $\mathbb{K}$, $B = (x_1, \ldots, x_n)$ una base ordenada de V y $x \in V$ un vector de coordenadas $(a_1, \ldots, a_n) \in \mathbb{K}^n$. Dado $m \in \{1, \ldots, n\}$, encontrar un subespacio vectorial U de V y una base ordenada B' de V/U tales que $x + U$ tenga coordenadas $(a_1, \ldots, a_m)$ respecto de B'.

51. Se considera en $\mathcal{M}_2(\mathbb{K})$ el subespacio U formado por las matrices de traza nula.

    (a) Calcular una base ordenada $B_{V/U}$ de $\mathcal{M}_2(\mathbb{K})$ y las coordenadas de $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ en esa base.

    (b) Si B_u es la base usual de $\mathcal{M}_2(\mathbb{K})$ y $\pi : \mathcal{M}_2(\mathbb{K}) \to \mathcal{M}_2(\mathbb{K})/U$ la proyección canónica $\pi(A) = A + U$, calcular las coordenadas de cada uno de los elementos de $\pi(B_u)$ en la base ordenada $B_{V/U}$ obtenida en el punto anterior.

52. (Examen de Algebra Lineal y Geometría, septiembre de 1996). Consideremos la matriz $A = \begin{pmatrix} 1 & 2 \\ 3 & m \end{pmatrix}$.

a) ¿Pará qué valores de $m \in \mathbb{R}$ existe $B \in \mathcal{M}_2(\mathbb{R}) \setminus \{0\}$ tal que $A \cdot B = 0$?

b) Probar que para cada valor $m \in \mathbb{R}$, el subconjunto $U_m = \{C \in \mathcal{M}_2(\mathbb{R}) \mid A{\cdot}C = 0\}$ es un subespacio vectorial de $\mathcal{M}_2(\mathbb{R})$. Para cada valor de m obtenido en el apartado a), calcular una base y la dimensión de U_m.

Capítulo 3

Aplicaciones Lineales

Nuestro siguiente objetivo será estudiar aplicaciones entre distintos espacios vectoriales que respeten las operaciones propias de cada espacio. En adelante, siempre consideraremos dos espacios vectoriales $V(\mathbb{K})$, $V'(\mathbb{K})$ sobre el mismo cuerpo conmutativo $\mathbb{K}$.

3.1. Definición y primeras propiedades

Definición 3.1.1 Dados dos espacios vectoriales $V(\mathbb{K}), V'(\mathbb{K})$, una aplicación $f\colon V \to V'$ se dice *lineal*[1] si cumple:

1. $f\colon (V,+) \to (V',+)$ es un homomorfismo de grupos, es decir $f(u+v) = f(u)+f(v)$, $\forall u, v \in V$.
2. $f(a\,v) = a\,f(v)$, $\forall u \in V$, $\forall a \in \mathbb{K}$.

Podemos resumir las dos condiciones anteriores en una única condición.

Proposición 3.1.1 *Una aplicación $f\colon V \to V'$ es lineal si y sólo si*

$$f(a\,u + b\,v) = a\,f(u) + b\,f(v), \qquad \forall u, v \in V, \quad \forall a, b \in \mathbb{K}. \tag{3.1}$$

Demostración. Supongamos que f es lineal. Entonces,

$$f(a\,u+b\,v) \overset{(1)}{=} f(a\,u) + f(b\,v) \overset{(2)}{=} a\,f(u) + b\,f(v).$$

Recíprocamente, (1) se tiene timando $a = b = 1$ en (3.1), y (2) se tiene tomando $b = 0$ enn (3.1). $\square$

[1] También llamada *homomorfismo de espacios vectoriales.*

Definición 3.1.2 Sea $f\colon V \to V'$ una aplicación lineal. El *núcleo* de f es

$$\ker(f) = \{v \in V \mid f(v) = 0\}.$$

A la dimensión $n(f)$ de $\ker(f)$ la llamaremos *nulidad de* f. Y llamaremos *rango de* f a la dimensión de $\mathrm{Im}(f)$. Trivialmente $0 \leq n(f) \leq \dim_{\mathbb{K}} V$ y $0 \leq \mathrm{rango}(f) \leq \dim_{\mathbb{K}} V'$.

Algunas propiedades simples de las aplicaciones lineales son las siguientes:

Proposición 3.1.2 *Sea $f\colon V \to V'$ una aplicación lineal. Entonces,*

1. $f(0) = 0$.
2. $f(-v) = -f(v)$, $\forall v \in V$.
3. $f(\sum_{i=1}^{k} a_i\, u_i) = \sum_{i=1}^{k} a_i\, f(u_i)$, $\forall u_i \in V$, $\forall a_i \in \mathbb{K}$, $\forall i \in \{1, \ldots, k\}$.
4. *Si $H \subset V$, entonces*[2] $f(L(H)) = L(f(H))$.
5. *Si $U \leq V$, entonces $f(U) \leq V'$. En particular, la imagen* $\mathrm{Im}(f) = f(V)$ *es un subespacio vectorial de V'.*
6. *Si $U' \leq V'$, entonces*[3] $f^{-1}(U') \leq V$. *En particular, el núcleo* $\ker(f) = f^{-1}(\{0\})$ *es un subespacio vectorial de V.*
7. *f es inyectiva si y sólo si* $\ker(f) = \{0\}$, *si y sólo si la nulidad de f es* 0.
8. *f es sobreyectiva si y sólo si* $\mathrm{Im}(f) = V'$, *si y sólo si el rango de f es* $\dim_{\mathbb{K}} V'$ *(aquí estamos suponiendo que* $\dim_{\mathbb{K}} V'$ *es finita).*
9. *Sea $V''(\mathbb{K})$ un espacio vectorial y $g\colon V' \to V''$ una aplicación lineal. Entonces, la composición $g \circ f\colon V \to V''$ es lineal.*
10. *Si f es biyectiva entonces su inversa $f^{-1}\colon V' \to V$ también es lineal.*

Demostración. 1. $f(0) = f(0 + 0) = f(0) + f(0)$, donde en la última igualdad se usa la propiedad (i) de las aplicaciones lineales. Sumando $-f(0)$ a ambos miembros obtenemos lo pedido.

2. $f(v) + f(-v) = f(v + (-v)) = f(0) = 0$.

3. Aplicar (3.1) e inducción sobre el número de sumandos.

4. Si $H = \{u_1, \ldots, u_m\}$ es finito, el punto 3 anterior implica que la imagen de cualquier elemento en $L(H)$ es una combinación lineal de $f(H) = \{f(u_1), \ldots, f(u_m)\}$ y viceversa,

[2] Esto es un abuso de notación; rigurosamante debería haberse escrito $f_*(L(H)) = L(f_*(H))$.

[3] Otro abuso de notación; rigurosamante sería $f^*(U')$.

lo que prueba $f(L(H)) = L(f(H))$ por doble inclusión. Si H es infinito, el problema se reduce al caso finito porque en las combinaciones lineales de H y $L(H)$ sólo intervienen una cantidad finita de sumandos.

5. Aplicando el apartado anterior, $f(U) = f(L(U)) = L(f(U))$, que es un subespacio vectorial de V.

6. Dados $u, w \in f^{-1}(U')$, $\exists u', w' \in U'$ tales que $f(u) = u', f(w) = w'$. Sean $a, b \in \mathbb{K}$. Por la linealidad de f y por ser $U' \leq V'$, $f(au + bw) = af(u) + bf(w) = au' + bw' \in U'$. Por tanto, $au + bw \in f^{-1}(U')$.

7. $\boxed{\Rightarrow}$ Supongamos que f es inyectiva y sea $v \in \ker(f)$. Entonces, $f(v) = 0 = f(0)$ luego $v = 0$ por inyectividad.

$\boxed{\Leftarrow}$ Sean $x, y \in V$ tals que $f(x) = f(y)$. Entonces, $v := x - y$ está en el núcleo de f ya que $f(v) = f(x) - f(y) = 0$. Como $\ker(f) = \{0\}$, tenemos $v = 0$ luego $x = y$.

8. Trivial.

9. Dados $v, w \in V$ y $a, b \in \mathbb{K}$, $(g \circ f)(av + bw) = g(f(av + bw)) = g(af(v) + bf(w)) = ag(f(v)) + bg(f(w)) = a(g \circ f)(v) + b(g \circ f)(w)$.

10. Sean $v', w' \in V'$ y $a, b \in \mathbb{K}$. Para comprobar que $f^{-1}(av' + bw') = af^{-1}(v') + bf^{-1}(w')$, basta demostrar que las imágenes por f de ambos miembros coinciden (por inyectividad de f). $f(af^{-1}(v') + bf^{-1}(w')) = af(f^{-1}(v')) + bf(f^{-1}(w')) = av' + bw' = f(f^{-1}(av' + bw'))$. □

Veamos algunos ejemplos sencillos que nos aparecerán más veces.

1. La aplicación identidad $1_V \colon V \to V$, $1_V(v) := v \; \forall v \in V$, es claramente lineal en cualquier espacio vectorial $V(\mathbb{K})$, siempre que en el dominio y el codominio consideremos la misma estructura de espacio vectorial.

2. La aplicación nula $f_0 \colon V \to V'$, $f_0(v) := 0 \; \forall v \in V$, (que también denotaremos simplemente 0) es claramente lineal para todo par de espacios vectoriales.

3. La *homotecia de razón* $\lambda \in \mathbb{K} \setminus \{0, 1\}$, definida por $H_\lambda \colon V \to V$, $H_\lambda(v) = \lambda v, \forall v \in V$, es claramente lineal (aquí se usa la conmutatividad de $\mathbb{K}$).

4. Si $U \leq V$, las aplicaciónes inclusión $i \colon U \to V$, $i(u) = u \; \forall u \in U$, y proyección canónica $\pi \colon V \to V/U$, $\pi(v) = v + U$, son lineales.

5. Si $f \colon V \to V'$ es una aplicación lineal y $U \leq V$, entonces la restricción $f|_U \colon U \to V$ es lineal.

6. La i-ésima proyección $\pi_i \colon \mathbb{K}^n \to \mathbb{K}$, $\pi_i((x_1, \ldots, x_n)) = x_i \; \forall (x_1, \ldots, x_n) \in \mathbb{K}^n$, es lineal.

7. Ser lineal depende del cuerpo base: $\Re \colon \mathbb{C} \to \mathbb{R}$, $\Re(z) = a$ si $z = a + b\,i \in \mathbb{C}$ con $a, b \in \mathbb{R}$, es $\mathbb{R}$-lineal pero no $\mathbb{C}$-lineal.

8. Sea $A \in M_{m\times n}(\mathbb{K})$. Considerando los elementos de $\mathbb{K}^n$ y $\mathbb{K}^m$ como matrices columna, la aplicación $f_A \colon \mathbb{K}^n \to \mathbb{K}^m$ dada por $f_A(x) = A\,x$, es lineal. Como veremos más adelante, toda aplicación lineal de $\mathbb{K}^n$ en $\mathbb{K}^m$ se puede escribir de este modo.

9. Fijemos n vectores $v_1, \ldots, v_n \in V(\mathbb{K})$. La aplicación $f \colon \mathbb{K}^n \to V$ dada por $f(x_1, \ldots, x_n) = \sum_{i=1}^n x_i v_i$, es lineal.

3.2. Isomorfismos, monomorfismos y epimorfismos

Definición 3.2.1 Sean $V(\mathbb{K}), V'(\mathbb{K})$ espacios vectoriales. Una aplicación $f \colon V \to V'$ se dice *monomorfismo* (resp. epimorfismo, isomorfismo) de espacios vectoriales si es lineal e inyectiva (resp. sobreyectiva, biyectiva). f se dice *endomorfismo* si $V = V'$ y automorfismo si es isomorfismo y endomorfismo a la vez.

Como la composición de aplicaciones lineales es lineal y lo mismo ocurre con la composición de aplicaciones inyectivas (resp. sobreyectivas, biyectivas), deducimos directamente que la composición de monomorfismos (resp. epimorfismos, isomorfismos, endomorfismos, automorfismos) es un monomorfismo (resp. epimorfismo, isomorfismo, endomorfismo, automorfismo).

Definición 3.2.2 Sean $V(\mathbb{K}), V'(\mathbb{K})$ dos espacios vectoriales sobre el mismo cuerpo. Diremos que $V(\mathbb{K})$ es isomorfo a $V'(\mathbb{K})$ si $\exists f \colon V \to V'$ isomorfismo de espacios vectoriales.

Lema 3.2.1 *Sea $\mathbb{K}$ un cuerpo conmutativo, y $\mathcal{V}_{\mathbb{K}}$ el conjunto cuyos elementos son los espacios vectoriales sobre $\mathbb{K}$. Entonces, la relación "ser isomorfo a" es de equivalencia en $\mathcal{V}_{\mathbb{K}}$.*

Demostración. La propiedad reflexiva se expresa diciendo que todo espacio vectorial es isomorfo a sí mismo, lo que se deduce de que la identidad $1_V \colon V \to V$ es un isomorfismo.

La propiedad simétrica se deduce de que si $V(\mathbb{K})$ es isomorfo a $V'(\mathbb{K})$ entonces $\exists f \colon V \to V'$ isomorfismo. $f^{-1} \colon V' \to V$ es un isomorfismo, luego $V'(\mathbb{K})$ es isomorfo a $V(\mathbb{K})$.

Finalmente, la transitiva de deduce de ue la composición de isomorfismos es un isomorfismo. □

Como iremos viendo, los isomorfismos conservan todas las propiedades de los espacios vectoriales, así que dos espacios vectoriales isomorfos $V(\mathbb{K}), V'(\mathbb{K})$ se pueden identificar (escribiremos esto $V \cong V'$), y es conveniente tener criterios para saber cuándo dos espacios vectoriales son isomorfos.

3.2.1. Teoremas de isomorfía

Recordemos que toda aplicación $f\colon X \to Y$ entre dos conjuntos admite una descomposición canónica $f = i \circ b \circ \pi$ (Teorema 0.1.1), donde

- $\pi\colon X \to X/_{\sim}$ es la proyección canónica (sobreyectiva) al conjunto cociente de X por la relación de equivalencia $x \sim x'$ si y sólo si $f(x) = f(x')$ (aquí $x, x' \in X$),
- $b\colon X/_{\sim} \to \mathrm{Im}(f)$ es la biyección dada por $b([x]) = f(x)$, para todo $x \in X$.
- $i\colon \mathrm{Im}(f) \to Y$ es la inclusión (inyectiva).

Recordemos también (Sección 2.3) que si $U \leq V(\mathbb{K})$ entonces la relación binaria $v \sim' w$ si y sólo si $v - w$ es de equivalencia en V y el cociente $V/U = V/_{\sim'}$ tiene estructura de espacio vectorial.

Veamos cómo se unen estos dos hechos cuando la aplicación es lineal.

Teorema 3.2.1 (Primer teorema de isomorfía) *Sea $f\colon V \to V'$ una aplicación lineal entre dos espacios vectoriales sobre $\mathbb{K}$, y sea $\sim$ la relación de equivalencia en V dada por $v \sim w$ si y sólo si $f(v) = f(w)$. Entonces,*

$$\forall v, w \in V,\ v \sim w \Leftrightarrow v - w \in \ker(f), \qquad \textit{esto es}, \qquad [v] = v + \ker(f),\ \forall v \in V. \tag{3.2}$$

Además, $f = i \circ b \circ \pi$ donde:

1. *$\pi\colon V \to V/\ker(f)$ es un epimorfismo de espacios vectoriales.*
2. *$b\colon V/\ker(f) \to \mathrm{Im}(f)$ es un isomorfismo de espacios vectoriales.*
3. *$i\colon \mathrm{Im}(f) \to V'$ es un monomorfismo de espacios vectoriales.*

En particular, $V/\ker(f) \cong \mathrm{Im}(f)$.

Demostración. Empezamos demostrando (3.2):

$$v \sim w \Leftrightarrow f(v) = f(w) \Leftrightarrow f(v - w) = 0 \Leftrightarrow v \in \ker(f),$$

donde en la segunda equivalencia se usa la linealidad de f.

La descomposición $f = i \circ b \circ \pi$ estaba demostrada para toda aplicación f, lineal o no. La linealidad de f asegura que también lo son tanto la inclusión i como la proyección π (ejemplo 4 de la Sección 3.1). Veamos que b es lineal:

$$\begin{aligned} b\left[(a(v + \ker(f)) + c(w + \ker(f))\right] &= b\left[(av + cw) + \ker(f)\right] = f(av + cw) \\ &= af(v) + cf(w) = a\, b\left[v + \ker(f)\right] + c\, b\left[w + \ker(f)\right], \end{aligned}$$

$\forall v + \ker(f), w + \ker(f) \in V/\ker(f)$, $\forall a, c \in |K$, donde se ha usado la definición de las operaciones en V/U, la definición de b, la linealidad de f y de nuevo la definición de b. □

Teorema 3.2.2 (Segundo teorema de isomorfía) *Sea $V(\mathbb{K})$ un espacio vectorial sobre $\mathbb{K}$, y $U, W \leq V$. Entonces, $U/(U \cap W) \cong (U+W)/W$.*

Demostración. Consideremos la aplicación inclusión $i\colon U \to U+W$ y la proyección canónica $\pi\colon U+W \to (U+W)/W$ (notemos que $W \leq U+W$). Entonces, la composición $f := \pi \circ i\colon U \to (U+W)/W$ es lineal. Aplicando a f el Primer Teorema de Isomorfía, tenemos $V/\ker(f) \cong \operatorname{Im}(f)$. Pero

$$\begin{aligned}
\ker(f) &= \{u \in U \mid (\pi \circ i)(u) = 0 + W\} = \{u \in U \mid \pi(u) = 0 + W\} \\
&= \{u \in U \mid u + W = 0 + W\} = \{u \in U \mid u \in W\} = U \cap W, \\
\operatorname{Im}(f) &= \{(\pi \circ i)(u) \mid u \in U\} = \{\pi(u) \mid u \in U\} = \{u + W \mid u \in U\} \\
&= \{(u+w) + W \mid u \in U,\ w \in W\} = \{(u+w) + W \mid u + w \in U + W\} \\
&= (U+W)/W.
\end{aligned}$$

□

Teorema 3.2.3 (Tercer teorema de isomorfía, o teorema del doble cociente) *Sea $V(\mathbb{K})$ un espacio vectorial sobre $\mathbb{K}$, y $U \leq W \leq V$. Entonces, $(V/U)/(W/U) \cong V/W$.*

Demostración. Consideremos la aplicación $f\colon V/U \to V/W$ dada por $f(v+U) = v+W$. Primero veamos que f está bien definida: sean $v, v' \in V$ tales que $v+U = v'+U$. Debemos comprobar que $v+W = v'+W$. Como $v+U = v'+U$, por definición $v - v' \in U$. Como $U \subset W$, se tiene $v - v' \in W$ luego $v + W = v' + W$ y f está bien definida.

A continuación veamos que f es lineal: Dados $v+U, v'+U \in V/U$ y $a, b \in \mathbb{K}$, $f[a(v+U) + b(v'+U)] = f[(av+bv') + U) = (av+bv') + W = a(v+W) + b(v'+W) = af(v+U) + bf(v'+U)$, luego f es lineal.

Aplicando a f el Primer Teorema de Isomorfía, tenemos $(V/U)/\ker(f) \cong \operatorname{Im}(f)$. Pero

$$\begin{aligned}
\ker(f) &= \{v + U \in V/U \mid f(v+U) = 0 + W\} = \{v + U \in V/U \mid v + W = 0 + W\} \\
&= \{v + U \in V/U \mid v \in W\} = W/U, \\
\operatorname{Im}(f) &= \{f(v+U) \mid v + U \in V/U\} = \{v + W \mid v \in V\} = V/W.
\end{aligned}$$

□

El próximo resultado muestra que en la clase de equivalencia de cada espacio vectorial finitamente generado existe un espacio vectorial del tipo $\mathbb{K}^n(\mathbb{K})$.

Proposición 3.2.1 *Sea $V(\mathbb{K})$ un espacio vectorial de dimensión $n \in \mathbb{N}$ y $B = (v_1, \ldots, v_n)$ una base ordenada de V. Entonces, la aplicación*

$$b_B\colon \mathbb{K}^n \to V, \qquad b_B(x_1, \ldots, x_n) := \sum_{i=1}^{n} x_i v_i, \qquad \forall (x_1, \ldots, x_n) \in \mathbb{K}^n$$

es un isomorfismo de espacios vectoriales. En particular, $V \cong \mathbb{K}^n$, y dos espacios $V, V' \in \mathcal{V}_{\mathbb{K}}$ de dimensión finita son isomorfos si y sólo si $\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} V'$.

Demostración. Es inmediato comprobar que b_B es la aplicación inversa de la biyección f_B definida en (2.12). Además, f_B es lineal por (2.13). Aplicando el apartado 10 de la Proposición 3.1.2, b_B es lineal y por tanto un isomorfismo. □

Nota 3.2.1 Lo anterior nos dice que cada clase de isomorfía de $\mathcal{V}_{\mathbb{K}}$ para dimensión finita tiene un representante privilegiado, $\mathbb{K}^n$. Esto no ocurre en dimensión infinita, donde hay espacios no isomorfos.

3.3. Construcción de aplicaciones lineales extendiendo por linealidad

Veremos a continuación que toda aplicación lineal queda determinada al prescribr las imágenes de los vectores de una base del dominio, y construiremos explícitamente la aplicación.

Teorema 3.3.1 *Sea $V(\mathbb{K}), V'(\mathbb{K})$ espacios vectoriales y $\mathcal{B} = \{v_1, \ldots, v_n\}$ una base de V. Dados $v'_1, \ldots, v'_n \in V'$, $\exists! f\colon V \to V'$ aplicación lineal tal que $f(v_i) = v'_i$ para todo $i \in \{1, \ldots, n\}$. Además,*

1. *f es monomorfismo si y sólo si $\{v'_1, \ldots, v'_n\}$ es linealmente independiente.*
2. *f es epimorfismo si y sólo si $\{v'_1, \ldots, v'_n\}$ es un sistema de generadores de V'.*
3. *f es isomorfismo si y sólo si $\{v'_1, \ldots, v'_n\}$ es base de V'.*

Demostración. Empecemos notando que si f existe entonces es única: como cada $v \in V$ se escribe $v = \sum_{i=1}^n a_i v_i$ para ciertos escalares $a_i \in \mathbb{K}$ (únicos porque $\mathcal{B}$ es base de V), se tiene

$$f(v) = f\left(\sum_{i=1}^n a_i v_i\right) = \sum_{i=1}^n a_i f(v_i) = \sum_{i=1}^n a_i v'_i,$$

lo que determina f. Para la existencia usaremos la fórmula anterior:

$$f(v) = \sum_{i=1}^n a_i v'_i, \ \forall v \in V.$$

Es claro que $f(v_i) = v'_i$ para cada i. Para comprobar que f es lineal, tomamos un segundo vector genérico $w = \sum_{i=1}^n b_i v_i$ y dos escalares cualesquiera $a, b \in \mathbb{K}$. Entonces,

$$av + bw = a\sum_{i=1}^n a_i v_i + b\sum_{i=1}^n b_i v_i = \sum_{i=1}^n (aa_i + bb_i) v_i,$$

luego,

$$f(av+bw)=\sum_{i=1}^{n}(aa_i+bb_i)w_i'=a\sum_{i=1}^{n}a_iw_i'+b\sum_{i=1}^{n}b_iw_i'=af(v)+bf(w),$$

la primera y tercera igualdades por la definición de f, con lo que f es lineal.

Veamos ahora los apartados del teorema. Para el apartado 1, notemos que

$$\ker(f)=\{v\in V \mid f(v)=0\}=\left\{\sum_{i=1}^{n}a_iv_i\in V \mid \sum_{i=1}^{n}a_iv_i'=0\right\}.$$

Si $\{v_1',\dots,v_n'\}$ es linealmente independiente, la única forma de que $\sum_{i=1}^{n}a_iv_i'$ se anule es con todos los $a_i=0$, luego $\ker(f)=\{0\}$. Recíprocamente, supongamos que $\ker(f)=\{0\}$ y veamos que $\{v_1',\dots,v_n'\}$ es linealmente independiente: si $\sum_{i=1}^{n}a_iv_i'=0$ entonces $\sum_{i=1}^{n}a_iv_i\in\ker(f)=\{0\}$. Por tanto, $\sum_{i=1}^{n}a_iv_i=0$. Como $\mathcal{B}$ es linealmente independiente, concluimos que $a_1=\ldots=a_n=0$.

El apartado 2 se deduce directamente de

$$\mathrm{Im}(f)=f(V)=f(L(\mathcal{B}))=L(f(\mathcal{B}))=L(\{v_1',\dots,v_n'\}). \tag{3.3}$$

El apartado 3 es consecuencia directa de 1 y 2. □

Nota 3.3.1

1. La ecuación (3.3) implica que para $v_1',\dots,v_n'\in V'$ generales, se tiene $\mathrm{Im}(f)=L(\{v_1',\dots,v_n'\})$.
2. Al procedimiento constructivo de f en el Teorema 3.3.1 se le llama *extensión por linealidad de los valores de f sobre la base $\mathcal{B}$.*
3. Del teorema se deduce que dos aplicaciones lineales $f,g\colon V\to V'$ son iguales si coinciden en alguna base de V. Además, el teorema permite construir **todas** las aplicaciones lineales de V en V'.

Corolario 3.3.1 *Sea $f\colon V\to V'$ una aplicación lineal, siendo $V\mathbb{K})$ de dimensión finita. Entonces, cada una de las tres afirmaciones a,b,c en las ternas siguientes son equivalentes (A,B,C no son equivalentes):*

(A.a) f es un monomorfismo de espacios vectoriales.

(A.b) f lleva subconjuntos linealmente independientes de V en linealmente independientes de V'.

(A.c) Existe una base $\mathcal{B}$ de V tal que $f(\mathcal{B})$ es linealmente independiente en V'.

(B.a) *f es un epimorfismo de espacios vectoriales.*

(B.b) *f lleva sistemas de generadores de V en sistemas de generadores de V'.*

(B.c) *Existe un sistema de generadores $H \subset V$, tal que $f(H)$ es sistema de generadores de V'.*

(C.a) *f es un isomorfismo de espacios vectoriales.*

(C.b) *f lleva bases de V en bases de V'.*

(C.c) *Existe una base $\mathcal{B}$ de V tal que $f(\mathcal{B})$ es base de V'.*

Demostración. En cada una d elas dos primeras ternas demostraremos cíclicamente *a)* $\Rightarrow$ *b)* $\Rightarrow$ *c)* $\Rightarrow$ *a)*. La tercera terna se deduce directamente de las dos primeras.
$\boxed{\textit{A. a)} \Rightarrow \textit{b)}}$. Sea $\{w_1, \ldots, w'_m\} \subset V$ un subconjunto linealmente independiente y $w'_i = f(w_i)\ \forall i = 1, \ldots, m$. Tomemos una combinación lineal del tipo

$$0 = a_1 w'_1 + \cdots + a_n w'_m = a_1 f(w_1) + \cdots + a_n f(w_m) = f(a_1 w_1 + \cdots + a_n w_m).$$

Como $f(0) = 0$ y f es inyectiva, tenemos $a_1 w_1 + \cdots + a_n w_m = 0$. Como H es linealmente independiente, todos a_i son cero, luego $f(H)$ es linealmente independiente.
$\boxed{\textit{A. b)} \Rightarrow \textit{c)}}$. Tomar una base $\mathcal{B}$ de V (que existe por el Teeorema 2.6.2) y aplicarle el apartado *a)*.
$\boxed{\textit{A. c)} \Rightarrow \textit{a)}}$. Es el apartado 1 del Teorema 3.3.1.
$\boxed{\textit{B. a)} \Rightarrow \textit{b)}}$. El argumento que sigue es una adaptación del de la demostración del apartado 2 del Teorema 3.3.1: Sea $H \subset V$ un sistema de generadores de V. Entonces, $V' = \mathrm{Im}(f) = f(V) = f(L(H)) = L(f(H))$, luego $f(H)$ es sistema de generadores de V'.
$\boxed{\textit{B. b)} \Rightarrow \textit{c)}}$. Trivial.
$\boxed{\textit{B. c)} \Rightarrow \textit{a)}}$. Supongamos que $H \subset V$ es un sistema de generadores de V y que $f(H)$ es sistema de generadores de V'. Entonces, $V' = L(f(H)) = f(L(H)) = f(V)$ luego f es sobreyectiva. □

Corolario 3.3.2 *Sea $f\colon V \to V'$ una aplicación lineal siendo $V(\mathbb{K})$ de dimensión finita.*

1. *Si f es inyectiva, entonces* $\dim_{\mathbb{K}} V \leq \dim_{\mathbb{K}} V'$.
2. *Si Si f es sobreyectiva, entonces* $\dim_{\mathbb{K}} V \geq \dim_{\mathbb{K}} V'$.
3. *Si f es biyectiva, entonces* $\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} V'$.

Demostración. Tomemos una base $\mathcal{B}$ de V.
Veamos el apartado 1. Si f es inyectiva, por el apartado (A.b) del Corolario 3.3.1 tenemos que $f(\mathcal{B})$ es linealmente independiente en V'. Si $\dim_{\mathbb{K}} V' = \infty$ no hay nada que probar, puesto que $\dim_{\mathbb{K}} V < \infty = \dim_{\mathbb{K}} V'$. Supongamos que $\dim_{\mathbb{K}} V'$ es finita. Entonces,

$$\dim_{\mathbb{K}} V = \text{cardinal}(\mathcal{B}) = \text{cardinal}(f(\mathcal{B})) \leq \dim_{\mathbb{K}} V',$$

donde en la segunda igualdad se ha usado que f es inyectiva y la última desigualdad es por el Corolario 2.6.1 aplicado a V' con $H = f(\mathcal{B})$.
Para el apartado 2, si f es sobreyectiva, por el apartado (B.b) del Corolario 3.3.1 tenemos que $f(\mathcal{B})$ es un sistema de generadores de V'; en particular $V'(\mathbb{K})$ es finitamente generado. Por el Corolario 2.6.1 aplicado a V' con $H' = f(\mathcal{B})$, tenemos

$$\dim_{\mathbb{K}} V' \leq \text{cardinal}(f(\mathcal{B})) \leq \text{cardinal}(\mathcal{B}) = \dim_{\mathbb{K}} V.$$

El apartado 3 es consecuencia directa de los dos primeros apartados. □

Veamos una especie de recíproco del Corolario 3.3.2.

Corolario 3.3.3 *Sean $V(\mathbb{K}), V'(\mathbb{K})$ espacios vectoriales de dimensiones $n, m \in \mathbb{N}$, respectivamente. Entonces:*

1. *Existe un monomorfismo de V en V' si y sólo si $n \leq m$.*
2. *Existe un epimorfismo de V en V' si y sólo si $n \geq m$.*
3. *Existe un isomorfismo de V a V' si y sólo si $n = m$.*

Demostración. Las implicaciones hacia la derecha de ls tres apartados son los correspondientes apartados del Corolario 3.3.2. Veamos las implicaciones hacia la izquierda de los dos primeros apartados (la del tercero es consecuencia de los dos primeros).

Tomemos bases $\mathcal{B} = \{v_1, \ldots, v_n\}$ y $\mathcal{B}' = \{v'_1, \ldots, v'_m\}$ de $V(\mathbb{K})$ y $V'(\mathbb{K})$, respectivamente.

Para el apartado 1, si $n \leq m$ podemos aplicar el Teorema 3.3.1 para concluir que existe $f \colon V \to V'$ lineal tal que $f(v_i) = v'_i$ $\forall i = 1, \ldots n$. Como $\{v'_1, \ldots, v'_n\}$ es linealmente independiente (por ser subcojunto de $\mathcal{B}'$), el apartado 2 del Teorema 3.3.1 asegura que f es un monomorfismo.

Para el apartado 2, supongamos $n \geq m$. Aplicamos el Teorema 3.3.1 para concluir que existe $f \colon V \to V'$ lineal tal que

$$\begin{aligned} f(v_i) &= v'_i \quad \forall i = 1, \ldots m, \\ f(v_i) &= 0 \quad \forall i = m+1, \ldots n, \end{aligned}$$

Como $\text{Im}(f) = L(f(\mathcal{B})) = L(\mathcal{B}' \cup \{0\}) = L(\mathcal{B}') = V'$, concluimos que f es un epimorfismo.
□

El apartado 3 del Corolario 3.3.3 nos dice que

Corolario 3.3.4 *1. Dos espacios vectoriales de dimensiones finitas son isomorfos si y sólo si tienen la misma dimensión.*

2. Si $f\colon V \to V'$ es un isomorfismo de espacios vectorales y $U \leq V$ tiene dimensión finita, entonces $\dim_{\mathbb{K}} U = \dim_{\mathbb{K}} f(U)$.

Nota 3.3.2 1. El apartado 1 del Corolario 3.3.4 reduce el estudio (salvo isomorfismos) de los espacios vectoriales finitamente generados al caso de $\mathbb{K}^n(\mathbb{K})$. Sin embargo, en general los isomorfismos existentes entre dos espacios vectoriales de la misma dimensión dependerán de las bases elegidas en ambos para construirlo vía el Teorema 3.3.1. Esto se expresa diciendo que el isomorfismo en cuestión es *no natural.* No obstante, veremos que en algunos casos muy especiales[4] se pueden establecer isomorfismos entre dos espacios vectoriales independientes de bases, llamados *isomorfismos naturales.*

2. Otra consecuencia del Teorema 3.3.1 es que para construir un isomorfismo entre dos espacios vectoriales V, V' basta elegir bases $\mathcal{B}$ de V y $\mathcal{B}'$ de V' y llevarse los vectores de $\mathcal{B}$ en los de $\mathcal{B}'$ tras haberlos ordenado, y que hay tantos isomorfismos de V en V' como formas tengamos de hacer esta construcción, es decir, como pares de bases ordenadas en V, V'. Como hay infinitas bases ordenadas en V, V' (estamos suponiendo $\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} V' \in \mathbb{N}$), tendremos infinitos isomorfismos distintos de V en V'.

Ahora podemos extraer consecuencias de los Teoremas de isomorfía en términos de dimensiones.

Teorema 3.3.2 (Fórmula de la nulidad y el rango) *Sea $f\colon V \to V'$ una aplicación lineal, siendo $\dim_{\mathbb{K}} V$ finita. Entonces,*

$$\dim_{\mathbb{K}} V = \dim_{\mathbb{K}}(\ker(f)) + \dim_{\mathbb{K}}(Im(f)).$$

Demostración. Por el Primer Teorema de Isomorfía, $V/\ker(f) \cong \mathrm{Im}(f)$. Tomando dimensiones, $\dim_{\mathbb{K}} V - \dim_{\mathbb{K}} \ker(f) = \dim_{\mathbb{K}}(V/\ker(f)) = \dim_{\mathbb{K}} \mathrm{Im}(f)$.

Veamos una forma directa de probar la fórmula de la nulidad y el rango, sin pasar por el primer Teorema de Isomorfía: Tomemos una base del núcleo de f, $\mathcal{B}_{\ker(f)} = \{v_1, \ldots, v_{n(f)}\}$ (aquí $n(f)$ es la nulidad de f) y la ampliamos a una base $\mathcal{B} = \{v_1, \ldots, v_{n(f)}, v_{n(f)+1}, \ldots, v_n\}$ de $V(\mathbb{K})$ (Teorema 2.6.4). Como $f(\mathcal{B})$ es un sistema de generadores de $\mathrm{Im}(f)$ y los vectores v_i con $i \leq n(f)$ se aplican por f en 0, tenemos que el conjunto $\{f(v_{n(f)+1}), \ldots, f(v_n)\}$ es un sistema de generadores de $\mathrm{Im}(f)$. Como este conjunto tiene $n - n(f)$ vectores, la fórmula de la nulidad y el rango se tendrá una vez que probemos que basta con comprobar que

[4] Teorema 4.3.1.

$\{f(v_{n(f)+1}),\ldots,f(v_n)\}$ es linealmente independiente. Tomemos una combinación lineal suya igualada a 0:

$$0 = a_{n(f)+1}f(v_{n(f)+1}) + \cdots + a_n f(v_n) = f(a_{n(f)+1}v_{n(f)+1} + \cdots + a_n v_n).$$

Entonces, $a_{n(f)+1}v_{n(f)+1} + \cdots + a_n v_n \in \ker(f)$, luego este vector se puede escribir como combinación lineal de los elementos de $\mathcal{B}_{\ker(f)}$: $\exists b_1,\ldots,b_{n(f)} \in \mathbb{K}$ tales que

$$a_{n(f)+1}v_{n(f)+1} + \cdots + a_n v_n = b_1 v_1 + \cdots + b_{n(f)}v_{n(f)}.$$

Pasando los términos del segundo miembro al primero, se tiene una combinación lineal de la base $\mathcal{B}$ igual a 0. Por tanto, todos los coeficientes de la combinación deben ser cero; en particular, $a_{n(f)+1} = \cdots = a_n = 0$. □

Los otros dos teoremas de isomorfía dan consecuencias ya conocidas sobre dimensiones: el Segundo Teorema de Isomorfía ($U/(U\cap W) \cong (U+W)/W$ siempre que $U,W \leq V$) redemuestra la fórmula de Grassmann (Teorema 2.8.1), y el Tercer Teorema de Isomorfía ($(V/U)/(W/U) \cong V/W$ siempre que $U \leq W \leq V$) da $\dim_{\mathbb{K}}(V/U) - \dim_{\mathbb{K}}(W/U) = \dim_{\mathbb{K}}(V/W)$, que tampoco es nada nuevo ya que ambos miembros de la igualdad son iguales a $\dim_{\mathbb{K}} V - \dim_{\mathbb{K}} W$.

La fórmula de la nulidad y el rango tiene una importante consecuencia:

Corolario 3.3.5 *Sea $f\colon V \to V'$ una aplicación lineal entre espacios vectoriales finitamente generados de la misma dimensión. Entonces, son equivalentes:*

1. *f es biyectiva.*
2. *f es inyectiva (es decir, $\ker(f) = \{0\}$)*
3. *f es sobreyectiva (es decir, $\mathrm{rango}(f) = \dim_{\mathbb{K}} V' = \dim_{\mathbb{K}} V$).*

En consecuencia, supongamos que $g\colon V' \to V$ es una aplicación lineal.

(A) Si $g\circ f\colon V \to V$ es un isomorfimo, entonces g y f son isomorfismos.

(B) Si $g\circ f = 1_V$ entonces $g = f^{-1}$.

Demostración. Llamemos $n = \dim_{\mathbb{K}} V = \dim_{\mathbb{K}} V' < \infty$. Si $n = 0$, tanto V como V' son $\{0\}$ y no hay nada que probar f se reduce a $f(0) = 0$. A partir de ahora supondremos $n \in \mathbb{N}$. Sean $n(f)$ la nulidad de f y $r(f)$ su rango. De la igualdad $n = n(f)+r(f)$ se deduce que f es inyectiva (esto es, $n(f) = 0$), si y sólo si $r(f) = n$ (esto es, f es sobreyectiva). Esto prueba que los apartados 1 y 2 son equivalentes, y por tanto también lo son con el apartado 3.

Para el apartado *(A)*, si $g\circ f$ es un isomorfismo entonces $g\circ f$ es biyectiva. Por los apartados primero y segundo del Lema 0.1.1, f es inyectiva y g es sobreyectiva y por la equivalencia $1 \Leftrightarrow 2 \Leftrightarrow 3$ ya demostrada, *(A)* está probado (también podemos usar los apartados b) y c) del Ejercicio 15). El apartado *(B)* es trivial aplicando *(A)*. □

3.4. Matrices de una aplicación lineal

Otra consecuencia directa del Teorema 3.3.1 es que si $f\colon V \to V'$ es un isomorfismo y $B = (v_1, \dots, v_n)$ es una base ordenada de V, entonces las coordenadas de cualquier $v \in V$ respecto de B coinciden con las coordenadas de $f(B)$ respecto de $f(B)$, es decir,

$$v_B = f(v)_{f(B)} \qquad \forall v \in V.$$

Veamos cómo podemos generalizar esto.

Sea $f\colon V^n \to V^m$ una aplicación lineal entre dos espacios vectoriales de dimensiones respectivas $n, k \in \mathbb{N}$. Supongamos que $B = (v_1, \dots, v_n)$, $B' = (v'_1, \dots, v'_m)$ son dos bases ordenadas en V, V'.

Dado $v \in V$, ¿qué relación hay entre las coordenadas $v_B \in \mathbb{K}^n$ y $f(v)_{B'} \in \mathbb{K}^m$?

Primero notemos que los vectores $f(v_1), \dots, f(v_n)$ determinan unívocamente f, por el Teorema 3.3.1. Esto nos dice que si escribimos

$$f(v_j) = \sum_{i=1}^{m} a_{ij}\, v'_i, \quad \forall j = 1, \dots, n, \tag{3.4}$$

entonces los $m \cdot n$ escalares $a_{ij} \in \mathbb{K}$ determinan unívocamente f.

Definición 3.4.1 Sea $f\colon V \to V'$ una aplicación lineal y $B = (v_1, \dots, v_n)$, $B' = (v'_1, \dots, v'_m)$ bases ordenadas de V y V'. La *matriz de f en B y B'* es

$$M(f, B, B') = (a_{ij})_{i,j} = \begin{pmatrix} \boxed{f(u_1)_{f(B)}} & \boxed{f(u_2)_{f(B)}} & \cdots & \boxed{f(u_k)_{f(B)}} \end{pmatrix} \in \mathcal{M}_{m\times n}(\mathbb{K}). \tag{3.5}$$

Nota 3.4.1
1. A veces, a $M(f, B, B')$ se la denota por $M(f, B' \leftarrow B)$, aunque nosotros no usaremos esta notación.
2. Ahora tiene sentido la primera igualdad de la Definición 2.7.2: la matriz de cambio de base $M(1_V, B, B')$ es la matriz de la aplicación identidad 1_V respecto de B, B' (allí B' también era una base ordenada de V).

Lo anterior nos dice que si $v \in V$ tiene coordenadas $v_B = (a_1, \dots, a_n) \in \mathbb{K}^n$ respecto a B y $f(v) \in V'$ tiene coordenadas $f(v)_{B'} = (a'_1, \dots, a'_m) \in \mathbb{K}^m$ respecto a B', entonces

$$f(v) = f\left(\sum_{j=1}^{n} a_j v_j\right) = \sum_{j=1}^{n} a_j f(v_j) \overset{(3.4)}{=} \sum_{j=1}^{n} a_j \sum_{i=1}^{m} a_{ij}\, v'_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij} a_j\right) v'_i,$$

luego

$$a'_i = \sum_{j=1}^{n} a_{ij} a_j, \qquad \forall i = 1, \ldots, m. \tag{3.6}$$

A se les llama las *ecuaciones analíticas de f respecto de B y B'.* Si expresamos (3.6) matricialmente, obtenemos

Proposición 3.4.1 (Ecuaciones analíticas de f en B y B') *Sea $f\colon V \to V'$ una aplicación lineal y $B = (v_1, \ldots, v_n)$, $B' = (v'_1, \ldots, v'_m)$ bases ordenadas de V y V'. Entonces,*

$$f(v)_{B'} = M(f, B, B') \cdot v_B \qquad \forall v \in V. \tag{3.7}$$

Nota 3.4.2 Las ecuaciones de cambio de base (2.15) no son más que un caso particular de (3.7), ver el punto 2 de la Nota 3.4.1.

Ejemplo 3.4.1 Recordemos que dada una matriz $A \in \mathcal{M}_{m\times n}(\mathbb{K})$, teníamos la aplicación lineal $f_A\colon \mathbb{K}^n \to \mathbb{K}^m$, $f_A(x) = Ax$ (ejemplo 8 de la Sección 3.1). Aplicando lo anterior, se tiene

$$M(f_A, B_u^n, B_u^m) = A, \tag{3.8}$$

donde B_u^n, B_u^m son las bases ordenadas usuales de $\mathbb{K}^n, \mathbb{K}^m$ respectivamente.

Definición 3.4.2 Dados dos espacios vectoriales V, V' sobre el mismo cuerpo, denotaremos por

$$\mathrm{Hom}_{\mathbb{K}}(V, V') = \{f\colon V \to V' \mid f \text{ es lineal}\}.$$

Proposición 3.4.2 $\mathrm{Hom}_{\mathbb{K}}(V, V')$ *tiene estructura de espacio vectorial con las operaciones*

$$\begin{array}{rccc} +\colon & \mathrm{Hom}_{\mathbb{K}}(V,V') \times \mathrm{Hom}_{\mathbb{K}}(V,V') & \to & \mathrm{Hom}_{\mathbb{K}}(V,V') \\ & (f,g) & \mapsto & f+g\colon V \to V' \\ \cdot\colon & \mathbb{K} \times \mathrm{Hom}_{\mathbb{K}}(V,V') & \to & \mathrm{Hom}_{\mathbb{K}}(V,V') \\ & (a,g) & \mapsto & a\,f\colon V \to V' \end{array}$$

donde $(f + g)(x) = f(x) + f'(x)$ y $(a\,f)(x) = a\,f(x)$, $\forall x \in V$, $a \in \mathbb{K}$.

Además, si $\dim_{\mathbb{K}} V = n$, $\dim_{\mathbb{K}} V' = m$ y B, B' son bases ordenadas de V, V' respectivamente, la aplicación

$$\begin{array}{rccc} F_{B,B'}\colon & \mathrm{Hom}_{\mathbb{K}}(V,V') & \to & \mathcal{M}_{m\times n}(\mathbb{K}) \\ & f & \mapsto & M(f,B,B') \end{array}$$

es un isomorfismo de espacios vectoriales. En particular, $\dim_{\mathbb{K}} \mathrm{Hom}_{\mathbb{K}}(V, V') = m \cdot n$.

Demostración. Las propiedades de espacio vectorial en $\mathrm{Hom}_{\mathbb{K}}(V,V')$ son un cálculo directo y se dejan como ejercicio. Que $F_{B,B'}$ es biyectiva se deduce directamente de la existencia y unicidad de aplicaciones lineales a partir del Teorema 3.3.1. Por último, veamos que $F_{B,B'}$ es lineal: dados $a,b\in\mathbb{K}$ y $f,g\colon V\to V'$ aplicaciones lineales,

$$F_{B,B'}(a\,f+b\,g)=M(a\,f+b\,g,B,B')=a\,M(f,B,B')+b\,M(g,B,B')\stackrel{(\star)}{=}a\,F_{B,B'}(f)+b\,F_{B,B'}(g).$$

donde $(\star)$ se deduce directamente de la definición de matriz de una aplicación lineal. $\square$

El siguiente resultado muestra una importante compatibilidad entre el producto de matrices y la composición de aplicaciones lineales.

Proposición 3.4.3 *Sean $V(\mathbb{K}),V'(\mathbb{K}),V''(\mathbb{K})$ espacios vectoriales con dimensiones $n,m,k\in\mathbb{N}$ y B,B',B'' bases ordenadas en cada uno.*

1. *Si $V\stackrel{f}{\to}V'\stackrel{g}{\to}V''$ son aplicaciones lineales, entonces*

$$M(g\circ f,B,B'')=M(g,B',B'')\cdot M(f,B,B'). \tag{3.9}$$

2. *f es un isomorfismo si y sólo si $M(f,B,B')$ es regular. En este caso,*

$$M(f^{-1},B',B)=M(f,B,B')^{-1}.$$

Demostración. La demostración del apartado 1 es análoga a la del Lema 2.7.2; pongamos $B=(v_1,\ldots,v_n)$, $B'=(v_1',\ldots,v_m')$, $B''=(v_1'',\ldots,v_p'')$. Usando las ecuaciones analíticas de f y g,

$$f(v_j) = \sum_{i=1}^{m} a_{ij}v_i', \quad \forall j=1,\ldots,n, \tag{3.10}$$

$$g(v_i') = \sum_{k=1}^{p} b_{ki}v_k'', \quad \forall j=1,\ldots,m, \tag{3.11}$$

donde $M(f,B,B')=(a_{i,j})_{i,j}\in\mathcal{M}_{m\times n}(\mathbb{K})$ y $M(g,B',B'')=(b_{i,j})_{i,j}\in\mathcal{M}_{p\times m}(\mathbb{K})$. Así que $\forall j=1,\ldots,n$,

$$\begin{aligned}
(g\circ f)(v_j) &= g(f(v_j))\stackrel{(3.10)}{=}g\left(\sum_{i=1}^{n}a_{ij}v_i'\right)=\sum_{i=1}^{n}a_{ij}\,g(v_i')\\
&\stackrel{(3.11)}{=}\sum_{i=1}^{n}a_{ij}\sum_{k=1}^{n}b_{ki}v_k''=\sum_{k=1}^{n}\left(\sum_{i=1}^{n}b_{ki}a_{ij}\right)v_k''\\
&=\sum_{k=1}^{n}\big(M(g,B',B'')\cdot M(f,B,B')\big)_{kj}\,v_k'',
\end{aligned}$$

de donde se deduce (3.9)

Para el apartado 2, si f es un isomorfismo, aplicamos el apartado 1 a $f \circ f^{-1} = 1_V$ para obtener $M(f^{-1}, B', B') \cdot M(f, B, B') = M(1_V, B, B) = I_n$y lo mismo con $f^{-1} \circ f$. Por tanto, $M(f, B, B') \in Gl(n, \mathbb{K})$ y su inversa es $M(f^{-1}, B, B')$.

Recíprocamente, si $M(f, B, B') \in Gl(n, \mathbb{K})$ entonces existe su inversa $A \in Gl(n, K)$. Por la Proposición 3.4.2,

$$\begin{array}{rccl} F_{B',B}\colon & \mathrm{Hom}_{\mathbb{K}}(V', V) & \to & \mathcal{M}_n(\mathbb{K}) \\ & g & \mapsto & M(g, B', B) \end{array}$$

es un isomorfismo de espacios vectoriales. Como $A \in \mathcal{M}_n(\mathbb{K})$, existe una única aplicación lineal $g\colon V' \to V$ tal que $F_{B',B}(g) = M(g, B', B) = A$. Por tanto,

$$M(g \circ f, B, B) \overset{(3.9)}{=} M(g, B', B) \cdot M(f, B, B') = A \cdot M(f, B, B') = I_n = M(1_V, B, B),$$

luego $g \circ f = 1_V$. Análogamente se prueba que $f \circ g = 1_{V'}$, así que f es un isomorfismo y $g = f^{-1}$ (también podríamos haber usado el apartado *(B)* del Corolario 3.3.5). □

En el caso $V = V'$, $\mathrm{Hom}_{\mathbb{K}}(V, V)$ consiste en los endomorfismos de V en sí mismo. Este caso tendrá mucha importancia en lo que sigue.

Definición 3.4.3 Dados un espacio vectorial $V(\mathbb{K})$, denotaremos por

$$\mathrm{End}_{\mathbb{K}} V = \{f\colon V \to V \mid f \text{ es lineal}\}.$$

al conjunto de los endomorfismos de V, y

$$\mathrm{Aut}_{\mathbb{K}} V = \{f \in \mathrm{End}_{\mathbb{K}} V \mid f \text{ es biyectiva}\}.$$

Proposición 3.4.4 $\mathrm{End}_{\mathbb{K}} V$ *tiene estructura de espacio vectorial con la suma y producto por escalares inducidos del caso general* $\mathrm{Hom}_{\mathbb{K}}(V', V)$*, y de anillo unitario con la composición. Además, si* $\dim_{\mathbb{K}} V = n$ *y* B *es una base ordenada de* V*, se tienen:*

(A) La aplicación

$$\begin{array}{rccl} F_B\colon & \mathrm{End}_{\mathbb{K}} V & \to & \mathcal{M}_n(\mathbb{K}) \\ & f & \mapsto & M(f, B) = M(f, B, B) \end{array}$$

es un isomorfismo de espacios vectoriales y de anillos. Así, $\dim_{\mathbb{K}} \mathrm{Hom}_{\mathbb{K}}(V, V') = n^2$.

(B) Dado $f \in \mathrm{End}_{\mathbb{K}} V$*,* f *es biyectiva (es decir,* $f \in \mathrm{Aut}_{\mathbb{K}} V$*) si y sólo si* $M(f, B) \in Gl(n, \mathbb{K})$*. En este caso,* $M(f, B)^{-1} = M(f^{-1}, B)$.

Demostración. La estructura de espacio vectorial de $\text{End}_{\mathbb{K}} V$, que F_B sea un isomorfismo de espacios vectoriales y la dimensión de $\text{End}_{\mathbb{K}} V$ son casos particulares del caso $\text{Hom}_{\mathbb{K}}(V', V)$. Que $\text{End}_{\mathbb{K}} V$ es un anillo es consecuencia de que la composición de endomorfismos es un enfomorfismo, y de las propiedades asociativa de la composición y distributiva de la composición respecto a la suma de endomorfismos. Que F_B es un homomorfismo de anillos es consecuencia directa de (3.9), y F_B es biyectiva porque es isomorfismo de espacios vectoriales. El apartado (B) es consecuencia del apartado 2 de la Proposición 3.4.3 tomando $B = B'$. □

3.5. Matrices equivalentes, rango

En esta sección responderemos las siguientes dos preguntas:

> ¿Qué tienen en común todas las matrices de una misma aplicación lineal si cambiamos las bases ordenadas en dominio y codominio?
>
> ¿Cuándo una matriz y una aplicación lineal prefijadas son una la matriz de la otra en un par de bases del dominio y codominio?

Corolario 3.5.1 *Sea $f : V \to V'$ una aplicación lineal, $B, \widetilde{B}$ dos bases ordenadas de V y $B', \widetilde{B}'$ dos bases ordenadas de V'. Entonces,*

$$M(f, \widetilde{B}, \widetilde{B}') = M(1_{V'}, B', \widetilde{B}') \cdot M(f, B, B') \cdot M(1_V, \widetilde{B}, B).$$

Demostración. Basta aplicar el apartado 1 de la Proposición 3.4.3 a $f = 1_{V'} \circ f \circ 1_V$. □

Las matrices $M(1_V, \widetilde{B}, B), M(1_{V'}, B', \widetilde{B}')$ que aparecen en el Corolario 3.5.1 son matrices de cambio de base entre bases ordenadas de V, V' respectivamente. En particular, son matrices regulares (Lemma 2.7.1). Es conveniente disponer del recíproco de esta propiedad.

Lema 3.5.1 *Sea $V(\mathbb{K})$ un espacio vectorial con $\dim_{\mathbb{K}} V = n \in \mathbb{N}$ y B una base ordenada de V. Dada $A \in Gl(n, \mathbb{K})$, existe una única base ordenada $\widetilde{B}$ de V tal que $A = M(1_V, \widetilde{B}, B)$.*

Demostración. Llamemos $A = (a_{i,j})_{i,j}$ y $B = (v_1, \ldots, v_n)$.
$\boxed{\text{Existencia.}}$ Como $A \in Gl(n, \mathbb{K})$, existe un único $f \in \text{Aut}_{\mathbb{K}} V$ tal que $M(f, B) = A$ (por la Proposición 3.4.4). Como f es automorfismo, $f(B)$ es una base ordenada de V (por el Corolario 3.3.1). Ahora consideremos la matriz de cambio de base $M(1_V, f(B), B)$. Por definición de matriz de una aplicación lineal, se tiene $M(1_V, f(B), B) = M(f, B)$ y por tanto, podemos tomar $\widetilde{B} := f(B)$.
$\boxed{\text{Unicidad.}}$ Supongamos que B' es una base ordenada de V tal que $A = M(1_V, B', B)$ y veamos que $B' = \widetilde{B}$: Por hipótesis, $M(1_V, B', B) = A = M(1_V, \widetilde{B}, B)$. Como las columnas

de ambas matrices coinciden, las coordenadas de los vectores de B' y de $\widetilde{B}$ respecto de B coinciden, por tanto, $B' = \widetilde{B}$. $\square$

Definición 3.5.1 Dos matrices $A, B \in \mathcal{M}_{m\times n}(\mathbb{K})$ se dicen *equivalentes* si $\exists P \in Gl(n, \mathbb{K})$, $Q \in Gl(m, \mathbb{K})$ tales que $B = Q^{-1} \cdot A \cdot P$.

Es fácil comprobar que lo anterior es una relación de equivalencia en $\mathcal{M}_{m\times n}(\mathbb{K})$: la propiedad reflexiva se deduce de que $I_n \in Gl(n, \mathbb{K})$, la simétrica de que la inversa de una matriz regular es regular, y la transitiva de que el producto de dos matrices regulares es regular.

Del Corolario 3.5.1 se deduce directamente el siguiente enunciado.

Corolario 3.5.2 *Sea $f: V \to V'$ una aplicación lineal, $B, \widetilde{B}$ dos bases ordenadas de V y $B', \widetilde{B}'$ dos bases ordenadas de V'. Entonces, $M(f, \widetilde{B}, \widetilde{B}')$ y $M(f, B, B')$ son matrices equivalentes.*

Veamos ahora el recíproco del Corolario 3.5.2.

Proposición 3.5.1 *Sea $f: V \to V'$ una aplicación lineal, y B, B' bases ordenadas de V y V' respectivamente. Dada $C \in \mathcal{M}_{m\times n}(\mathbb{K})$ equivalente a $A := M(f, B, B')$, existen bases ordenadas $\widetilde{B}$ de V y $\widetilde{B}$ de V' tales que $C = M(f, \widetilde{B}, \widetilde{B}')$.*

Demostración. Como A y C son matrices equivalentes, $\exists P \in Gl(n, \mathbb{K})$, $Q \in Gl(m, \mathbb{K})$ tales que $C = Q^{-1} \cdot A \cdot P$. Aplicando el Lema 3.5.1, existen (únicas) bases ordenadas $\widetilde{B}$ de V y $\widetilde{B'}$ de V' tales que $P = M(1_V, \widetilde{B}, B)$, $Q = M(1_{V'}, \widetilde{B}', B')$. Así,

$$C = M(1_{V'}, \widetilde{B}', B')^{-1} \cdot M(f, B, B') \cdot M(1_V, \widetilde{B}, B) = M(1_{V'}, B', \widetilde{B}') \cdot M(f, \widetilde{B}, B') = M(f, \widetilde{B}, \widetilde{B}').$$

$\square$

Hemos visto que una primera característica común de todas las matrices que representan a la misma aplicación lineal es que son equivalentes, y que dos matrices equivalentes representan a la misma aplicación lineal. Es decir, podemos identificar cada aplicación lineal con una clase de equivalencia de matrices. Otra característica común es la siguiente:

Proposición 3.5.2 *El rango $r(f)$ de una aplicación lineal $f: V \to V'$ coincide con el rango (por columnas) de su matriz $M(f, B, B')$ en cualesquiera bases ordenadas B de V y B' de V'.*

Demostración. Sean $B = (v_1, \ldots, v_n)$, $B' = (v'_1, \ldots, v'_m)$ bases ordenadas de V, V'. Sabemos que $r(f)$ es la dimensión de $L(\{f(v_1), \ldots, f(v_n)\}) \leq V'$. Como la aplicación

$b_{B'}\colon \mathbb{K}^m \to V', (x_1,\dots,x_m) \mapsto \sum_{i=1}^m x_i v_i'$ es un isomorfismo de espacios vectoriales (Proposición 3.2.1), tenemos que

$$\dim_{\mathbb{K}} L(\{f(v_1),\dots,f(v_n)\}) = \dim_{\mathbb{K}} L(\{b_{B'}^{-1}(f(v_1)),\dots,b_{B'}^{-1}(f(v_n))\})$$

Pero cada $b_{B'}^{-1}(f(v_i))$ es la columna i-ésima de $M(f,B,B')$. Así que el rango por columnas de $M(f,B,B')$ es $r(f)$. □

El siguiente paso es descubrir cuál es la matriz "más sencilla" de una aplicación lineal:

Proposición 3.5.3 *Sea $f\colon V \to V'$ una aplicación lineal, con $\dim_{\mathbb{K}} V = n$, $\dim_{\mathbb{K}} V' = m$. Entonces, existen bases ordenadas B de V y B' de V' tales que*

$$M(f,B,B') = \left(\begin{array}{c|c} I_r & O_{r\times(n-r)} \\ \hline O_{(m-r)\times r} & O_{(m-r)\times(n-r)} \end{array}\right), \tag{3.12}$$

donde r es el rango de f.

Demostración. Tomemos una base ordenada de V $B = (v_1,\dots,v_r,v_{r+1},\dots v_n)$ donde los últimos $n-r$ vectores forman base de $\ker(f)$ (los primeros r vectores se obtienen aplicando el Teorema de Ampliación de la Base en V a $\{v_{r+1},\dots v_n\}$, aquí se está usando la fórmula de la nulidad y el rango). Por la demostración de la fórmula de la nulidad y el rango, el conjunto $\{f(v_1),\dots,f(v_r)\}$ es es linealmente independiente. Aplicando a este mismo conjunto el Teorema de Ampliación de la Base en V', encontramos $m-r$ vectores $v'_{r+1},\dots,v'_m \in V'$ tales que $B' := (f(v_1),\dots,f(v_r),v'_{r+1},\dots,v'_m)$ es una base ordenada de V'. Aplicando la definición de matriz de una aplicación lineal en un par de bases ordenadas se comprueba fácilmente que $M(f,B,B')$ es de la forma requerida. □

Recordemos (Definición 1.5.1) que el rango por columnas de una matriz $A \in \mathcal{M}_{m\times n}(\mathbb{K})$ es el número máximo de columnas de A linealmente independientes. Por tanto, el rango por columnas de la matriz de la derecha en (3.12) es r.

Proposición 3.5.4 *Sea $A \in \mathcal{M}_{m\times n}(\mathbb{K})$. Supongamos que $A = M(f,B,B') = M(\widetilde{f},\widetilde{B},\widetilde{B}')$ para dos aplicaciones lineales $f\colon V \to V'$, $\widetilde{f}\colon \widetilde{V} \to \widetilde{V}'$, siendo $V,V',\widetilde{V},\widetilde{V}'$ espacios vectoriales sobre $\mathbb{K}$ con $\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} \widetilde{V} = n$ y $\dim_{\mathbb{K}} V' = \dim_{\mathbb{K}} \widetilde{V}' = m$, y $B,B',\widetilde{B},\widetilde{B}'$ bases ordenadas respectivas en $V,V',\widetilde{V},\widetilde{V}'$. Entonces,* rango$(f)$=rango$(\widetilde{f})$.

Demostración. Por la Proposición 3.4.2, existen aplicaciones lineales $h\colon V \to \widetilde{V}$, $h'\colon \widetilde{V}' \to V'$ tales que $M(h,B,\widetilde{B}) = M(h',\widetilde{B}',B') = I_n$. Tanto h como h' llevan bases en bases, luego ambas aplicaciones son isomorfismos. Veamos que $h'\circ\widetilde{f}\circ h = f$:

$$\begin{aligned} M(h'\circ\widetilde{f}\circ h,B,B') &= M(h',\widetilde{B}',B')\cdot M(\widetilde{f}\circ h,B,\widetilde{B}') = I_m\cdot M(\widetilde{f}\circ h,B,\widetilde{B}') \\ &= M(\widetilde{f}\circ h,B,\widetilde{B}') = M(\widetilde{f},\widetilde{B},\widetilde{B}')\cdot M(h,B,\widetilde{B}) = M(\widetilde{f},\widetilde{B},\widetilde{B}')\cdot I_n \\ &= M(\widetilde{f},\widetilde{B},\widetilde{B}') = A = M(f,B,B') \end{aligned}$$

luego $h' \circ \widetilde{f} \circ h = f$ por ser biyectiva la aplicación $F_{B,B'}$ de la Proposición 3.4.2. Usando ahora los apartados b), c) del Ejercicio 15, concluimos que rango($h' \circ \widetilde{f} \circ h$)=rango($\widetilde{f}$), y por tanto rango($f$)=rango($\widetilde{f}$). $\square$

Como consecuencia directa del Corolario y de la ecuación (3.8) tenemos:

Corolario 3.5.3 *El rango por columnas de una matriz $A \in \mathcal{M}_{m\times n}(\mathbb{K})$ coincide con el rango de la aplicación lineal $f_A \colon \mathbb{K}^n \to \mathbb{K}^m$, $f_A(x) = A \cdot x$, y también con el rango de cualquier aplicación lineal $f \colon V \to V'$ tal que $A = M(f, B, B')$, donde V, V' son cualesquiera espacios vectoriales sobre $\mathbb{K}$ con $\dim_{\mathbb{K}} V = n$ y $\dim_{\mathbb{K}} V' = m$ y B, B' son bases ordenadas respectivas en V, V'.*

Demostración. Por la Definición 1.5.1, el rango por columnas de A es el número de columnas de A linealmente independientes. Usando la ecuación (3.8), el número de columnas linealmente independientes de A coincide con el rango de f_A (porque las columnas de A son las imágenes por f_A de los vectores de la base ordenada usual de $\mathbb{K}^n$). La segunda parte del corolario es consecuencia directa de la Proposición 3.5.4. $\square$

Corolario 3.5.4

1. *Toda matriz $A \in \mathcal{M}_{m\times n}(\mathbb{K})$ es equivalente a una del tipo $\left(\begin{array}{c|c} I_r & O \\ \hline O & O \end{array}\right)$, donde r es el rango de A por columnas.*
2. *Dos matrices en $\mathcal{M}_{m\times n}(\mathbb{K})$ son equivalentes si y sólo si ambas lo son a la misma matriz del tipo $\left(\begin{array}{c|c} I_r & O \\ \hline O & O \end{array}\right)$, y si y sólo si tienen el mimo rango.*

Demostración. Para el apartado 1, sean V, V' dos espacios vectoriales sobre $\mathbb{K}$ con $\dim_{\mathbb{K}} V = n$ y $\dim_{\mathbb{K}} V' = m$. Tomemos bases ordenadas B de V y B' de V'. Por la Proposición 3.4.2, existe una única aplicación lineal $f \colon V \to V'$ tal que $M(f, B, B') = A$. Aplicando a f la Proposición 3.5.3, existen bases ordenadas $\widetilde{B}$ de V y $\widetilde{B}'$ de V' tales que $M(f, \widetilde{B}, \widetilde{B}')$ es de la forma (3.12), siendo $r = \text{rango}(f)$. Por el Corolario 3.5.2, A y $M(f, \widetilde{B}, \widetilde{B}')$ son equivalentes. Además, r es el rango de A por columnas, por el Corolario 3.5.3.

Para el apartado 2, si dos matrices $A, C \in \mathcal{M}_{m\times n}(\mathbb{K})$ son equivalentes, entonces por la Proposición 3.5.1 A, C son matrices *de la misma* aplicación lineal $f \colon V \to V'$, siendo V, V' espacios vectoriales con $\dim_{\mathbb{K}} V = n$, $\dim_{\mathbb{K}} V' = m$. Por el Corolario 3.5.3, el rango de A por columnas coincide con el rango de f, y lo mismo con el rango de C por columnas. Luego A, C tienen el mismo rango por columnas. Recíprocamente, supongamos que los rangos de A y C por columnas coinciden. Por el apartado 1 de este corolario, tanto A como C son equivalentes a la misma matriz del tipo $\left(\begin{array}{c|c} I_r & O \\ \hline O & O \end{array}\right)$. Por transitividad, A es equivalente a C. $\square$

Definición 3.5.2 El *núcleo* de una matriz $A \in \mathcal{M}_{m\times n}(\mathbb{K})$ es el subespacio de $\mathbb{K}^n$ dado por las soluciones del SEL homogéneo $A\,x = 0$, es decir:

$$\ker(A) = \{x \in \mathcal{M}_{m\times n}(\mathbb{K}) \,|\, A\,x = 0\} = \ker(f_A).$$

La *imagen de* A es el subespacio de $\mathbb{K}^m$

$$\mathrm{Im}(A) = \mathrm{Im}(f_A).$$

Por la fórmula de la nulidad y el rango, el número de columnas de A coincide con la suma $\dim_{\mathbb{K}} \ker(A) + \mathrm{rango}(A)$ (ya que) $\dim_{\mathbb{K}} \ker(A) = \mathrm{nulidad}(f_A)$ y $\mathrm{rango}(A) = \mathrm{rango}(f_A)$).

Corolario 3.5.5 *Consideremos el SEL* $A\,x = b$*, donde* $A \in \mathcal{M}_{m\times n}(\mathbb{K})$ *es la matriz de coeficientes y* $b \in \mathbb{K}^m \equiv \mathcal{M}_{m\times 1}(\mathbb{K})$ *la columna de términos independientes. Entonces:*

1. $A\,x = b$ *es compatible si y sólo si* $b \in \mathrm{Im}(f_A)$*, y en tal caso, sus soluciones coinciden con* $f_A^{-1}(\{b\})$ *(imagen recíproca de* b*).*

2. *En el caso compatible, el conjunto de soluciones se escribe*

$$f_A^{-1}(\{b\}) = x_0 + \ker(A) := \{x_0 + y \,|\, y \in \ker(A)\}, \tag{3.13}$$

siendo x_0 *cualquier solución del sistema homogéneo asociado* $A\,x = 0$*. Además ,* $A\,x = b$ *es compatible determinado si y sólo si* $\ker(A) = \{0\}$*, si y sólo si* f_A *es inyectiva.*

Demostración. La única afirmación no trivial es la primera igualdad de (3.13). La vemos por doble inclusión:
$\boxed{\supseteq}$. Dado $y \in \ker(A) = \ker(f_A)$, $f_A(x_0 + y) = f_A(x_0) + f_A(y) = b + 0 = b$ luego $x_0 + y \in f_A^{-1}(\{b\})$.
$\boxed{\subseteq}$. Sea $y \in f_A^{-1}(\{b\})$. Para comprobar que $y \in x_0 + \ker(A)$ tenemos que ver que $x_0 - y \in \ker(A)$. Esto se deduce de que $f_A(x_0 - y) = f_A(x_0) - f_A(y) = b - b = 0$. $\square$

Habíamos caracterizado cuándo una matriz cuadrada es regular por que su determinante fuera no nulo (Nota 1.4.2 y Proposición 1.4.4). Ahora podemos caracterizarlo por que su rango por columnas.

Proposición 3.5.5 *Sea* $A \in \mathcal{M}_n(\mathbb{K})$*. Entonces,* $A \in Gl(n, \mathbb{K})$ *si y sólo si su rango por columnas es* n*.*

Demostración. Sea $V(\mathbb{K})$ un espacio vectorial de dimensión n y B una base ordenada de V (por ejemplo, $\mathbb{K}^n$ y B_u). Como la aplicación F_B de la Proposición 3.4.4 es biyectiva, existe una única $f \in \mathrm{End}_{\mathbb{K}} V$ tal que $M(f, B) = A$.

El apartado (B) de la Proposición 3.4.4 asegura que Como $A \in Gl(n, \mathbb{K})$ si y sólo si $f \in \mathrm{Aut}_{\mathbb{K}} V$. Esta última condición es equivalente a que el rango de f sea n, por el Corolario 3.3.5. Por último, de $M(f, B) = A$ se deduce que rango(A) = rango(f), lo que termina de probar la Proposición. □

Vimos en la Proposición 3.4.2 que si V, V' son espacios vectoriales sobre $\mathbb{K}$ con dimensiones respectivas n, m, entonces $\mathrm{Hom}_{\mathbb{K}}(V, V')$ tiene estructura de espacio vectorial sobre $\mathbb{K}$ con dimensión $m \cdot n$ y había un isomorfismo (no natural) $F_{B,B'}$ entre $\mathrm{Hom}_{\mathbb{K}}(V, V')$ y $\mathcal{M}_{m\times n}(\mathbb{K})$ cada vez que fijamos bases ordenadas B, B' de V, V'. Usaremos este isomorfismo para calcular una base explícita de $\mathrm{Hom}_{\mathbb{K}}(V, V')$.

Teorema 3.5.1 *Sean $V(\mathbb{K}), V'(\mathbb{K})$ espacios vectoriales con dimensiones $n, m \in \mathbb{N}$ y B, B' bases ordenadas en cada uno. Entonces, el conjunto $\{f_{ij} \mid i = 1, \ldots, m,\ j = 1, \ldots, n\}$ es una base de $\mathrm{Hom}_{\mathbb{K}}(V, V')$, donde cada f_{ij} viene determinada por*

$$f_{ij}(v_k) = \delta_{jk} v'_i, \ \forall k = 1, \ldots, n. \tag{3.14}$$

Demostración. Recordemos que la base usual de $\mathcal{M}_{m\times n}(\mathbb{K})$ es $\{E_{ij} \mid i = 1, \ldots, m,\ j = 1, \ldots n\}$, donde cada E_{ij} tiene un 1 en la posición (i, j) y cero el resto de entradas. Como la aplicación $f \in \mathrm{Hom}_{\mathbb{K}}(V, V') \mapsto F_{B,B'}(f) = M(f, B, B') \in \mathcal{M}_{m\times n}(\mathbb{K})$ es un isomorfismo de espacios vectoriales, tanto $F_{B,B'}$ como su inversa llevan bases en bases (Corolario 3.3.1). Por tanto, $\{f_{i,j} := F^{-1}_{B,B'}(E_{ij}) \mid i = 1, \ldots, m,\ j = 1, \ldots n\}$ es base de $\mathrm{Hom}_{\mathbb{K}}(V, V')$. Queda comprobar (3.14): Fijamos $i = 1, \ldots, m,\ j = 1, \ldots n$. Dado $k \in 1, \ldots, n$, la imagen por f_{ij} de v_k tiene por coordenadas respecto de B' a la k-ésima columna de E_{ij}. Si $k \neq j$, esta columna es nula, mientras que si $k = j$, la columna tiene un 1 en la posición i y ceros en el resto de posiciones; este 1 afecta, como coordenada al vector i-ésimo de B', es decir, a v'_i. Por tanto, $f_{ij}(v_k) = \delta_{jk} v'_i$. □

3.6. Matrices semejantes

Como $\mathrm{End}_{\mathbb{K}} V = \mathrm{Hom}_{\mathbb{K}}(V, V)$ y $\mathcal{M}_n(\mathbb{K}) = \mathcal{M}_{n\times n}(\mathbb{K})$, todos los resultados vistos hasta ahora para $\mathrm{Hom}_{\mathbb{K}}(V, V')$ y $\mathcal{M}_{n\times n}(\mathbb{K})$ siguen siendo válidos para $\mathrm{End}_{\mathbb{K}} V$ y $\mathcal{M}_n(\mathbb{K})$, con el extra dado por la estructura de anillo de estos dos últimos (Proposición 3.4.4). En particular, tenemos la relación de matrices equivalentes en $\mathcal{M}_n(\mathbb{K})$ y su relación con el rango de endomorfimos.

Para endomorfismos y matrices cuadradas, el Corolario 3.5.1 adopta una forma especial cuando las bases ordenadas inicial y final coinciden (esto último está justificado por el isomorfismo F_B de la Proposición 3.4.4):

Lema 3.6.1 *Sea $f : V \to V$ un endomorfismo y $B, \widetilde{B}$ dos bases ordenadas de V. Entonces,*

$$M(f, \widetilde{B}) = M(1_V, B, \widetilde{B}) \cdot M(f, B) \cdot M(1_V, \widetilde{B}, B).$$

Demostración. Tomar $V' = V$, $B' = B$ y $\widetilde{B}' = \widetilde{B}$ en el Corolario 3.5.1. $\square$

Notemos que $M(1_V, \widetilde{B}, B) \in Gl(n, \mathbb{K})$ (aquí $n = \dim_{\mathbb{K}} V$) y $M(1_{V'}, B, \widetilde{B}) = M(1_V, \widetilde{B}, B)^{-1}$.

Definición 3.6.1 Dos matrices $A, B \in \mathcal{M}_n(\mathbb{K})$ se dicen *semejantes* si $\exists P \in Gl(n, \mathbb{K})$ tal que $B = P^{-1} \cdot A \cdot P$.

De nuevo es fácil comprobar que "ser semejante a" es una relación de equivalencia en $\mathcal{M}_n(\mathbb{K})$ (el argumento es el mismo que el que probaba que "ser equivalente a" es una relación de equivalencia en $\mathcal{M}_{m\times n}(\mathbb{K})$).

Proposición 3.6.1 *Sea $f\colon V \to V$ un endomorfismo y B una base ordenada de V.*

1. *Dada una base ordenada $\widetilde{B}$ de V, las matrices $M(f, B)$ y $M(f, \widetilde{B})$ son semejantes.*
2. *Recíprocamente, sea $C \in \mathcal{M}_n(\mathbb{K})$ semejante a $A := M(f, B)$. Entonces, existe una base ordenada $\widetilde{B}$ de V tal que $C = M(f, \widetilde{B})$.*

Demostración. El apartado 1 es consecuencia directa del Lema 3.6.1.

Para probar el apartado 2 adaptamos la Demostración de la Proposición 3.5.1: como A y C son matrices semejantes, $\exists P \in Gl(n, \mathbb{K})$ tal que $C = P^{-1} \cdot A \cdot P$. Aplicando el Lema 3.5.1, existe una (única) base ordenada $\widetilde{B}$ de V tal que $P = M(1_V, \widetilde{B}, B)$. Así,

$$C = M(1_V, \widetilde{B}, B)^{-1} \cdot M(f, B) \cdot M(1_V, \widetilde{B}, B) = M(1_V, B, \widetilde{B}) \cdot M(f, \widetilde{B}, B) = M(f, \widetilde{B}).$$

$\square$

Es claro que si dos matrices cuadradas son semejantes, entonces son equivalentes. El recíproco no es cierto, porque la única matriz semejante a I_n es la propia I_n, pero cualquier matriz regular de orden n tiene rango n, luego es equivalente a I_n.

De la misma forma que identificábamos una aplicación lineal con una clase de equivalencia de matrices, ahora podemos identificar un endomorfismo con una clase de semejanza de matrices. Esto es así como consecuencia de la Proposición 3.6.1 y del isomorfismo F_B dado en el apartado (A) de la Proposición 3.4.4. Además, esta identificación de endomorfismos con clases de semejanza de matrices distingue los automorfismos y las matrices regulares, indentificándolos entre sí (apartado (B) de la Proposición 3.4.4).

A diferencia de lo que ocurría con el rango y la equivalencia de matrices, ahora no hay un invariante numérico que caracterice cuándo dos matrices cuadradas son semejantes. Sí hay alguna condición necesaria (pero no suficiente):

Proposición 3.6.2 *Sean $A, C \in M_n(\mathbb{K})$ dos matrices semejantes. Entonces sus trazas y sus determinantes coinciden.*

Demostración. Como A, C son semejantes, $\exists P \in Gl(n, \mathbb{K})$ tal que $C = P^{-1} \cdot A \cdot P$. Por el apartado 10 de la Proposición 1.1.1,

$$\text{Traza}(C) = \text{Traza}\left[P^{-1}\,(A\,P)\right] = \text{Traza}\left[(A\,P)\,P^{-1}\right] = \text{Traza}\left[A\,(P\,P^{-1})\right] = \text{Traza}(A).$$

Para el determinante, usamos el apartado 10 de la Proposición 1.4.2:

$$\det C = \det\left(P^{-1}\,A\,P\right) = \det(P^{-1})\,\det A\,\det P = (\det P)^{-1}\,\det A\,\det P = \det A.$$

□

Nota 3.6.1 Las matrices $A = I_2$ y $C = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ muestran que el recíproco de la Proposición 3.6.2 no es cierto.

La Proposición 3.6.2 permite definir la traza de cualquier endomorfismo de un espacio vectorial finitamente generado[5]:

Definición 3.6.2 Sea $V(\mathbb{K})$ un espacio vectorial finitamente generado y $f \in \text{End}_{\mathbb{K}}(V)$. Se define la *traza* de f como la traza de cualquier matriz $M(f, B)$ en una base ordenada B de $V(\mathbb{K})$.

[5]Sin embargo, no debemos usar un razonamiento similar para definir el determinante de un endomorfismo, porque el apartado 10 de la Proposición 1.4.2 se justificó a partir de propiedades del determinante de un endomorfismo. Para no caer en un razonamiento circular aquí, deberemos definir de otra forma el determinante de un endomorfismo $f\colon V \to V$, y demostrar que con esa definición se tienen $\det(g \circ f) = \det(g) \cdot \det(f)$ y $\det(f) = \det M(f, B)$, siempre que $g \in \text{End}_{\mathbb{K}} V$ y B sea una base ordenada de V.

3.7. Ejercicios.

1. Sean $V(\mathbb{K}), V'(\mathbb{K})$ espacios vectoriales. Dado $v'_0 \in V'$, consideremos la aplicación constante igual a v'_0, $f_{v'_0} \colon V \to V'$, $f_{v'_0}(v) := v'_0$, $\forall v \in V$. Probar que si $f_{v'_0}$ es lineal, entonces $v_0 = 0$.

2. Sea $F(\mathbb{R}, \mathbb{R})$ el conjunto de todas las aplicaciones de $\mathbb{R}$ en $\mathbb{R}$ y U el conjunto de todas las aplicaciones de $\mathbb{R}$ en $\mathbb{R}$ que son derivables en todo punto (que es un subespacio vectorial de $\mathcal{F}(\mathbb{R}, \mathbb{R})$. Demostrar que la aplicación $D \colon U \to \mathcal{F}(\mathbb{R}, \mathbb{R})$, que a cada función h le hace corresponder su función derivada h' es lineal.

3. Sean V, V' espacios vectoriales sobre un cuerpo $\mathbb{K}$ y $f \colon V \to V'$ una aplicación. Demostrar que f es lineal si y sólo si su grafo es un subespacio vectorial del producto $V \times V'$ con la estructura de espacio vectorial producto.

4. Sean V, V' dos espacios vectoriales sobre un cuerpo $\mathbb{K}$, y $V \times V'$ su producto cartesiano con la estructura de espacio vectorial producto.

   a) Probar que las proyecciones $\pi_1 \colon V \times V' \to V$, $\pi_2 \colon V \times V' \to V'$ dadas por $(x, x') = (\pi_1(x, x'), \pi_2(x, x'))$ son epimorfismos de espacios vectoriales.

   b) Probar que las aplicaciones $i \colon V \to V \times V'$, $i' \colon V' \to V \times V'$ dadas por $i(x) = (x, 0')$, $i'(x') = (0, x')$ son monomorfismos de espacios vectoriales y que $V \times V' = \mathsf{Im}(i) \oplus \mathsf{Im}(i')$.

5. Sea $f \in \mathrm{End}_{\mathbb{K}} V$ un endomorfismo de un espacio vectorial V, tal que $f \circ f = f$. Demostrar que $V = \ker(f) \oplus \mathsf{Im}(f)$.

6. Sea $f \in \mathrm{End}_{\mathbb{K}} V$ un endomorfismo tal que $f \circ f = 1_V$. Probar que $V = \{x \in V \mid f(x) = x\} \oplus \{x \in V \mid f(x) = -x\}$.

7. Sea $V = \mathbb{R}_2[x]$ (polinomios con coeficientes reales y de grado ≤ 2). Para cada $r \in \mathbb{R}$, se define $f_r \colon V \to V$ mediante $f_r(a_0 + a_1 x + a_2 x^2) = a_0 + a_1 x + r\, a_2 x^2$.

   a) Probar que para cada $r \in \mathbb{R}$, f_r es un endomorfismo de V.

   b) ¿Pará qué valores de r es f_r un automorfismo?

8. Sea V un espacio vectorial real que admite un endomorfismo j cumpliendo $j \circ j = -1_V$.

   a) Probar que si $V(\mathbb{R})$ es finitamente generado, entonces $\dim_{\mathbb{R}} V$ es par.

   b) Definimos un producto por escalares complejos $\mathbb{C} \times V \to V$ mediante

   $$(a + bi)x := ax + b\, j(x), \quad \forall x \in V,\ \forall a + bi \in \mathbb{C}.$$

   Probar que V con este producto por escalares es un espacio vectorial complejo. ¿Qué tienen que ver $\dim_{\mathbb{C}} V$ y $\dim_{\mathbb{R}} V$?

9. Sea V un espacio vectorial real con dimensión par. Probar que existe un endomorfismo $j \in \mathrm{End}_{\mathbb{R}} V$ tal que $j \circ j = -1_V$. Deducir que $V(\mathbb{R})$ admite una estructura de espacio vectorial complejo.

10. Sea $V(\mathbb{K})$ un espacio vectorial y $U, W \subset V$ dos subespacios tales que $V = U \oplus W$. Definir explícitamente un isomorfismo de espacios vectoriales de V/W en U.

11. Encontrar un automorfismo f de $\mathbb{R}^3(\mathbb{R})$ de forma que $f_*(U) = U'$, siendo

$$U = \{(a, b, 0) \mid a, b \in \mathbb{R}\}, \quad U' = \{(0, c, d) \mid c, d \in \mathbb{R}\}.$$

¿Es posible encontrar más de un automorfismo en estas condiciones?

12. Sea $f \colon \mathbb{R}^4 \to \mathbb{R}^3$ la aplicación lineal dada por

$$f(a_1, a_2, a_3, a_4) = (a_1 + a_3 - a_4, a_2 + a_4, a_1 + a_2 + a_3).$$

a) Hallar la ecuación matricial de f respecto de las bases ordenadas $B = (x_1, x_2, x_3, x_4)$ de $\mathbb{R}^4$, $x_1 = (-1, 0, 0, 0)$, $x_2 = (1, -1, 0, 0)$, $x_3 = (1, 1, -1, 0)$, $x_4 = (1, 1, 1, -1)$, y $B' = (x'_1, x'_2, x'_3)$ de $\mathbb{R}^3$, $x'_1 = (0, 1, 1)$, $x'_2 = (1, 0, 1)$, $x'_3 = (1, 1, 0)$.

b) Encontrar bases ordenadas $\widetilde{B}, \widetilde{B}'$ de $\mathbb{R}^4$ y $\mathbb{R}^3$ respectivamente, tales que

$$M(f, \widetilde{B}, \widetilde{B}') = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

c) Calcular el rango de f. ¿Es f sobreyectiva?

13. Consideremos los subespacios vectoriales de $\mathbb{R}^3$

$$U = L(\{(1, 1, 1)\}), \qquad W = \{(a, b, c) \in \mathbb{R}^3 \mid a + b + c = 0\}.$$

a) Encontrar un endomorfismo f de $\mathbb{R}^3$ tal que $\ker(f) = U$ e $\mathrm{Im}(f) = W$.

b) Calcular la ecuación matricial de f respecto de la base ordenada usual B_u de $\mathbb{R}^3$.

c) Elegir una base ordenada B' de $\mathbb{R}^3/\ker(f)$ y respecto de B' y B_u, encontrar la ecuación matricial de la aplicación lineal $\mathbb{R}^3/\ker(f) \to \mathbb{R}^3$, $x + \ker(f) \mapsto f(x)$.

14. Sea $f, g \colon V \to V'$ aplicaciones lineales.

a) Probar que rango$(f + g) \leq$ rango$(f) +$ rango(g).

b) Encontrar un ejemplo en el que se dé la igualdad, y otro en que la desigualdad sea estricta.

15. Sea $f: V \to V'$, $g: V' \to V''$ dos aplicaciones lineales.

    a) Probar que rango$(g \circ f) \leq \text{mín}\{\text{rango}(g), \text{rango}(f)\}$.

    b) Si suponemos que f es un isomorfismo, probar que rango$(g \circ f) =$ rango(g).

    c) Si suponemos que g es un isomorfismo, probar que rango$(g \circ f) =$ rango(f).

    d) Traducir todo lo anterior a rango de matrices.

    e) Encontrar un ejemplo en el que se dé la igualdad en el apartado a), y otro en que la desigualdad sea estricta.

16. Encontrar contrajemplos en $\mathcal{M}_2(\mathbb{R})$ que prueben que $(A+B)^2 \neq A^2 + 2AB + B^2$ y que $(A-B)(A+B) \neq A^2 - B^2$.

17. Sea $A \in \mathcal{M}_n(\mathbb{K})$ tal que $A^2 + A + I_n = 0$. Probar que A es regular.

18. Calcular la traza del endomorfismo $f: \mathbb{R}^2 \to \mathbb{R}^2$, $f(a,b) = (a+b, a-b)$.

19. Sea $A \in \mathcal{M}_n(\mathbb{K})$ tal que $A^2 = A$. Probar que la traza y el rango de A coinciden.

20. Sea $A \in \mathcal{M}_n(\mathbb{K})$ tal que $AB = BA$ para toda $B \in \mathcal{M}_n(\mathbb{K})$. Probar que A es un múltiplo de la identidad. Deducir la propiedad correspodiente para endomorfismos.

21. Calcular, en función del parámetro $a \in \mathbb{R}$, el rango de la matriz:

$$A = \begin{pmatrix} a & 1 & a \\ 1 & 1 & 1 \end{pmatrix}.$$

22. Sean $A, B \in \mathcal{M}_n(\mathbb{K})$ matrices semejantes. Probar que si $aA^2 + bA^2 + cI_n = 0$ para $a, b, c \in \mathbb{K}$, entonces $aB^2 + bB + cI_n = 0$.

23. Hallar todas las matrices $X \in \mathcal{M}_n(\mathbb{K})$ tales que $X^2 = X$.

24. Hallar todas las matrices $X \in \mathcal{M}_n(\mathbb{K})$ tales que $X^2 = I_n$.

25. Hallar todas las matrices $X \in \mathcal{M}_n(\mathbb{K})$ tales que $X^2 = 2X$.

26. Sea $V(\mathbb{R})$ un espacio vectorial de dimensión 2, y $f \in \text{End}_{\mathbb{R}} V$ un endomorfismo tal que $f \circ f = f_0$.

    a) Probar que $f = f_0$ o es posible encontrar una base ordenada B de V tal que

$$M(f, B) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

    b) Generalizar a mayores dimensiones.

c) Hallar todas las matrices $X \in \mathcal{M}_2(\mathbb{R})$ tales que $X^2 = 0$.

27. Hallar todas las matrices $X \in \mathcal{M}_{2n+1}(\mathbb{R})$ tales que $X^2 = -I_{2n+1}$.

28. Hallar todas las matrices $X \in \mathcal{M}_{2n}(\mathbb{R})$ tales que $X^2 = -I_{2n}$.

29. Sea $V(\mathbb{C})$ un espacio vectorial complejo y $f \in \mathrm{End}_{\mathbb{C}}V$ tal que $f \circ f = -1_V$.

    a) Demostrar que $U = \{x \in V \mid f(x) = i\,x\}$, $W = \{x \in V \mid f(x) = -i\,x\}$ son subespacios vectoriales de V, y que $V = U \oplus W$.

    b) Hallar todas las matrices $X \in \mathcal{M}_3(\mathbb{C})$ tales que $X^2 = -I_3$.

30. Encontrar un endomorfismo $f \in \mathrm{End}_{\mathbb{R}}\mathbb{R}^4$ tal que $\mathrm{Im}(f) = L(\{e_1 - e_2, e_1 + e_4\})$, $f \circ f = f$ y $\mathrm{Traza}(f) = 2$.

31. (Examen de Algebra Lineal y Geometría, septiembre de 1994). Consideremos el espacio de matrices complejas $\mathcal{M}_2(\mathbb{C})$, y la aplicación $f\colon \mathcal{M}_2(\mathbb{C}) \to \mathcal{M}_2(\mathbb{C})$ dada por $f(A) = \overline{A}$, donde $\overline{A}$ es la matriz cuyas entradas son los complejos conjugados de las entradas de A.

    a) ¿Es f un endomorfismo del espacio vectorial complejo $\mathcal{M}_2(\mathbb{C})$?

    b) Consideremos la estructura de espacio vectorial real que $\mathcal{M}_2(\mathbb{C})$ posee de forma natural. Comprobar que f es un automorfismo de $\mathcal{M}_2(\mathbb{C})$ con esta estructura real y hallar explícitamente f^{-1}.

Capítulo 4

Espacio dual

El espacio dual de un espacio vectorial $V(\mathbb{K})$ es un caso particular de $\mathrm{Hom}_{\mathbb{K}}(V, V')$ poniendo $V' = \mathbb{K}$. Todo lo que sabemos sobre $\mathrm{Hom}_{\mathbb{K}}(V, V')$ es aplicable a V^*, pero este espacio tiene propiedades adicionales, que os permitirán interpretar la trasposición de matrices y demostrar el Teorema del Rango.

A lo largo de este tema, $V(\mathbb{K})$ será un espacio vectorial finitamente generado y llamaremos n a su dimensión.

4.1. Definición y primeras propiedades

Definición 4.1.1 Dado un espacio vectorial $V(K)$, su *espacio dual* es el espacio vectorial

$$V^* = V^*(\mathbb{K}) := \mathrm{Hom}_{\mathbb{K}}(V, \mathbb{K}) = \{\varphi\colon V \to \mathbb{K} \mid \varphi \text{ es lineal}\}.$$

A cada elemento $\varphi \in V^*$ se le llamará *forma lineal sobre* V. Al 0 de V^* le llamaremos *forma lineal nula*, φ_0.

Por la Proposición 3.4.2, V^* es un espacio vectorial sobre $\mathbb{K}$ y $\dim_{\mathbb{K}} V^* = n$. En particular, V^* es isomorfo a V (apartado 1 del Corolario 3.3.4).

Fijemos una base ordenada $B = (v_1, \ldots, v_n)$ de $V(\mathbb{K})$ y tomemos $\{1\}$ como base en $\mathbb{K}(\mathbb{K})$. Para cada $\varphi \in V^*$ podemos calcular su matriz en $B, \{1\}$:

$$M(\varphi, B, \{1\}) = (\varphi(v_1) \ldots \varphi(v_n)). \tag{4.1}$$

Las ecuaciones analíticas de φ en B y $\{1\}$ (ecuación (3.7)) se escriben

$$\varphi(v) = M(\varphi, B, \{1\}) \cdot v_B \qquad \forall v \in V. \tag{4.2}$$

Si $v = \sum_{i=1}^{n} a_i v_i \in V$, entonces (4.1) y (4.2) implican

$$\varphi(v) = (\varphi(v_1) \dots \varphi(v_n)) \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \sum_{i=1}^{n} \varphi(v_i) a_i \in \mathbb{K}.$$

Proposición 4.1.1 *Sea $\varphi \in V^*(\mathbb{K})$.*

1. *Si $\varphi \neq \varphi_0$, entonces* $\ker(\varphi)$ *es un hiperplano vectorial, esto es,* $\dim_{\mathbb{K}} \ker(\varphi) = n - 1$.
2. *Si $U \leq V$ es un hiperplano vectorial, entonces existe una forma lineal $\varphi \in V^*$ tal que* $\ker(\varphi) = U$.
3. *Dos formas lineales $\varphi, \phi \neq \varphi_0$ son proporcionales si y sólo si sus núcleos coinciden.*

Demostración. Probemos el apartado 1. Como $\mathrm{Im}(\varphi)$ es un subespacio de $\mathbb{K}$ y $\dim_{\mathbb{K}} \mathbb{K} = 1$, tenemos que o bien $\mathrm{Im}(\varphi) = \{0\}$ (esto no puede darse, porque $\varphi \neq \varphi_0$) o bien $\mathrm{Im}(\varphi) = \mathbb{K}$. En este último caso, la Fórmula de la Nulidad y el Rango nos dice que $\dim_{\mathbb{K}} \ker(\varphi) = n - \dim_{\mathbb{K}} \mathrm{Im}(\varphi) = n - 1$.

Para el apartado 2, sea $\mathcal{B}_U = \{v_1, \dots, v_{n-1}\}$ una base de U. Por el Teorema de Ampliación de la Base, podemos elegir un vector $v_n \in V$ tal que $\mathcal{B} := \{v_1, \dots, v_{n-1}, v_n\}$ es base de V. Por el Teorema 3.3.1, existe una única forma lineal $\varphi \in V^*$ tal que

$$\varphi(v_1) = \dots = \varphi(v_{n-1}) = 0, \qquad \varphi(v_n) = 1.$$

Es claro que $U \subset \ker(\varphi)$. Tomando dimensiones, $n - 1 = \dim_{\mathbb{K}} U \leq \dim_{\mathbb{K}} \ker(\varphi) = n - 1$, donde en la última igualdad hemos usado que $\varphi \neq \varphi_0$ y el apartado 1. Así, $\dim_{\mathbb{K}} U = \dim_{\mathbb{K}} \ker(\varphi)$ luego $U = \ker(\varphi)$.

Finalmente veamos el apartado 3. Como $\varphi, \phi \neq \varphi_0$ son proporcionales, tenemos $\phi = a\,\varphi$ para algún $a \in \mathbb{K} \setminus \{0\}$. Por tanto, $\ker(\varphi) \subset \ker(\phi)$, y como $a \neq 0$, también se verifica la inclusión contraria, luego $\ker(\varphi) = \ker(\phi)$. Recíprocamente, llamemos $U := \ker(\varphi) = \ker(\phi)$. Por la demostración del apartado 2, podemos construir una base ordenada B de V ampliando una base ordenada de U. Aplicando (4.1),

$$\begin{array}{ll} M(\varphi, B, \{1\}) = (0, \dots, 0, \varphi(v_n)), & \varphi(v_n) \neq 0, \\ M(\psi, B, \{1\}) = (0, \dots, 0, \psi(v_n)), & \psi(v_n) \neq 0, \end{array}$$

de donde deducimos que tomando $a = \psi(v_n) \cdot \varphi(v_n)^{-1} \in \mathbb{K}$ se tiene $\psi = a\,\varphi$. $\square$

Ejemplo 4.1.1 (El espacio dual de $\mathcal{M}_{n\times 1}(\mathbb{K})$) Dada $a = (a_1, \ldots, a_n) \in \mathcal{M}_{1\times n}(\mathbb{K})$, llamemos

$$\varphi_a \colon \mathcal{M}_{n\times 1}(\mathbb{K}) \to \mathbb{K}, \quad \varphi_a \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = (a_1, \ldots, a_n) \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \sum_{i=1}^{n} a_i b_i.$$

Por las propiedades básicas del producto de matrices, φ_a es lineal y por tanto, $\varphi_a \in \mathcal{M}_{n\times 1}(\mathbb{K})^*$. Esto nos permite definir una aplicación

$$\chi \colon \mathcal{M}_{1\times n}(\mathbb{K}) \to \mathcal{M}_{n\times 1}(\mathbb{K})^*, \qquad \chi(a) = \varphi_a.$$

De nuevo por las propiedades básicas del producto de matrices, χ es lineal. Además, χ es inyectiva, porque si $a \in \ker(\chi)$ entonces $\varphi_a = 0$ (forma lineal nula sobre $\mathcal{M}_{n\times 1}(\mathbb{K})$), luego $\varphi_a(b) = 0\ \forall b \in \mathcal{M}_{n\times 1}(\mathbb{K})$. Tomando b como $(0, \ldots, 1, \ldots, 0)$ con el 1 en la posición i-ésima, se obtiene $a_i = 0$. Así que $a = 0$ y $\ker(\chi) = \{0\}$, luego χ es inyectiva. Como $\dim_{\mathbb{K}} \mathcal{M}_{1\times n}(\mathbb{K}) = \dim_{\mathbb{K}} \mathcal{M}_{n\times 1}(\mathbb{K})^*$, deducimos que χ es un isomorfismo de espacios vectoriales. Esto nos permite identificar el espacio dual de las matrices columna $\mathcal{M}_{n\times 1}(\mathbb{K})$ con las matrices fila $\mathcal{M}_{1\times n}(\mathbb{K})$.

4.2. Base dual

Teorema 4.2.1 *Dada una base ordenada $B = (v_1, \ldots, v_n)$ de V, existe una única base $B^* = (\varphi^1, \ldots, \varphi^n)$ de V^* (la base ordenada* dual de B*) tal que*

$$\varphi^i(v_j) = \delta_{ij} \quad \forall i, j \in \{1, \ldots, n\}, \qquad (\delta_{ij} = \textit{delta de Kronecker}). \tag{4.3}$$

Demostración. El Teorema 3.3.1 asegura que para cada $i \in \{1, \ldots, n\}$, la asignación $\varphi^i(v_j) = \delta_{ij} \in \mathbb{K}\ \forall j = 1, \ldots, n$ define una única forma lineal $\varphi^i \in V^*$.

El conjunto $\mathcal{B}^* = \{\varphi^1, \ldots, \varphi^n\}$ es base de V porque coincide con la base $\{f_{ij} \mid i = 1, \ldots, m,\ j = 1, \ldots, n\}$ de $\mathrm{Hom}_{\mathbb{K}}(V, V')$ para el caso particular $V' = \mathbb{K}$, $B' = \{1\}$ (Teorema 3.5.1). Damos una demostración directa de que $\mathcal{B}^*$ es base:

$\boxed{\text{Independencia lineal.}}$ Sean $a_1, \ldots, a_n \in \mathbb{K}$ tales que $\varphi_0 = a_1\, \varphi^1 + \ldots + a_n\, \varphi^n$. Aplicando ambos miembros de la igualdad a cada v_j de B, tenemos

$$0 = \sum_{i=1}^{n} a_i \varphi^i(v_j) = \sum_{i=1}^{n} a_i \delta_{ij} = a_j,$$

como se quería.

$\boxed{\text{Sistema de generadores}}$ (en realidad esto no es necesario porque $\mathcal{B}^*$ es linealmente independiente y $\dim_{\mathbb{K}} V^* = n$, pero lo hacemos para obtener una fórmula que será útil más adelante). Sea $\varphi \in V^*$. Veamos que

$$\varphi = \sum_{i=1}^{n} \varphi(v_i)\, \varphi^i. \tag{4.4}$$

Por el Teorema 3.3.1, basta probar que ambos miembros de (4.4) coinciden sobre los vectores de B. Dado $j = 1, \ldots, n$,

$$\left(\sum_{i=1}^{n} \varphi(v_i)\, \varphi^i \right)(v_j) = \sum_{i=1}^{n} \varphi(v_i)\, \varphi^i(v_j) = \sum_{i=1}^{n} \varphi(v_i)\, \delta_{ij} = \varphi(v_j),$$

lo que prueba (4.4). □

Ejemplo 4.2.1 Siguiendo con lo visto en el Ejemplo 4.1.1, la base dual de la base usual de $\mathcal{M}_{n\times 1}(\mathbb{K})$, vista en $\mathcal{M}_{1\times n}(\mathbb{K})$ mediante el isomorfismo χ, es la base usual de $\mathcal{M}_{1\times n}(\mathbb{K})$.

Corolario 4.2.1 *Si $v \in V$ cumple $\varphi(v) = 0\ \forall \varphi \in V^*$, entonces $v = 0$.*

Demostración. Razonando por reducción al absurdo, si $v \neq 0$ podemos ampliar $\{v\}$ a una base ordenada $B = (v = v_1, v_2, \ldots, v_n)$ de V. El primer elemento φ^1 de la base ordenada dual B^* de B cumple $\varphi^1(v) = 1 \neq 0$, contradicción. □

Corolario 4.2.2 *Sea $B = (v_1, \ldots, v_n)$ una base ordenada de V y $B^* = (\varphi^1, \ldots, \varphi^n)$ su base ordenada dual. Entonces,*

$$v_B = (\varphi^1(v), \ldots, \varphi^n(v)) \tag{4.5}$$

$$\varphi_{B^*} = (\varphi(v_1), \ldots \varphi(v_n)). \tag{4.6}$$

Demostración. (4.6) se obtiene directamente reescribiendo (4.4). Para comprobar (4.5) basta probar que $w := v - \sum_{i=1}^{n} \varphi^i(v)\, v_i$ es el vector nulo de V. Por el Corolario 4.2.1, esto se tendrá si probamos que $\varphi(w) = 0\ \forall \varphi \in V^*$. Ya que B^* es sistema de generadores de V^*, basta demostrar que $\varphi^j(w) = 0\ \forall j = 1, \ldots, n$.

$$\begin{aligned} \varphi^j(w) &= \varphi^j\left(v - \sum_{i=1}^{n} \varphi^i(v)\, v_i \right) = \varphi^j(v) - \sum_{i=1}^{n} \varphi^i(v) \varphi^j(v_i) = \varphi^j(v) - \sum_{i=1}^{n} \varphi^i(v) \delta_{ji} \\ &= \varphi^j(v) - \varphi^j(v) = 0. \end{aligned}$$

□

Nota 4.2.1 Para los elementos de B^* tenemos

$$\begin{array}{ccc} M(\varphi^1, B, \{1\}) & \overset{(4.1)}{=} & (1, 0, \dots, 0) \\ \vdots & & \vdots \\ M(\varphi^n, B, \{1\}) & \overset{(4.1)}{=} & (0, 0, \dots, 1), \end{array}$$

que vuelve a decirnos que la base dual $\mathcal{B}^*$ coincide con la base $\{f_{ij}\}_{i,j}$ de $\mathrm{Hom}_{\mathbb{K}}(V, V')$ para el caso particular $V' = \mathbb{K}$, $B' = \{1\}$ (Teorema 3.5.1).

4.2.1. Cambio de base en el espacio dual

Sean $B = (v_1, \dots, v_n)$, $B' = (v'_1, \dots, v'_n)$ dos bases ordenadas de V y $B^* = (\varphi_1, \dots, \varphi_n)$, $B'^* = (\varphi'_1, \dots, \varphi'_n)$ sus respectivas bases duales. Supongamos que

$$v'_j = \sum_{i=1}^{n} a_{ij} v_i, \qquad \forall j \in \{1, \dots, n\} \tag{4.7}$$

es decir,

$$M(1_V, B', B) = (a_{ij})_{i,j}. \tag{4.8}$$

Dado $v \in V$, lo escribimos en combinación lineal de B y B':

$$v = \sum_{i=1}^{n} a_i v_i = \sum_{j=1}^{n} a'_j v'_j.$$

Así,

$$\sum_{j=1}^{n} a'_j v'_j \overset{(4.7)}{=} \sum_{j=1}^{n} a'_j \sum_{i=1}^{n} a_{ij} v_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} a'_j \right) v_i,$$

de donde

$$a_i = \sum_{i=1}^{n} a_{ij}\, a'_j, \qquad \forall i = 1, \dots, n.$$

Esto es,

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = M(1_V, B', B) \cdot \begin{pmatrix} a'_1 \\ \vdots \\ a'_n \end{pmatrix}.$$

Queremos saber la relación entre este cambio de base en V y el de las bases duales respectivas en V^*. Escribimos ahora

$$\varphi_i = \sum_{j=1}^{n} b_{ji}\varphi'_j, \tag{4.9}$$

es decir,

$$M(1_{V^*}, B^*, B'^*) = (b_{ji})_{j,i}.$$

Dado $\varphi \in V^*$, lo escribimos en combinación lineal de B^* y B'^*:

$$\varphi = \sum_{i=1}^{n} b_i\varphi_i = \sum_{j=1}^{n} b'_j\varphi'_j.$$

Así,

$$\sum_{i=1}^{n} b_i\varphi_i \overset{(4.9)}{=} \sum_{i=1}^{n} b_i \sum_{j=1}^{n} b_{ji}\varphi'_j = \sum_{j=1}^{n}\left(\sum_{i=1}^{n} b_{ji}b_i\right)\varphi'_j,$$

de donde

$$b'_j = \sum_{i=1}^{n} b_{ji}\, b_i, \qquad \forall j = 1, \ldots, n.$$

Esto es,

$$\begin{pmatrix} b'_1 \\ \vdots \\ b'_n \end{pmatrix} = M(1_{V^*}, B^*, B'^*) \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.$$

Evaluando (4.9) en v'_h,

$$\varphi_i(v'_h) = \sum_{j=1}^{n} b_{ji}\varphi'_j(v'_h) = \sum_{j=1}^{n} b_{ji}\delta_{jh} = b_{hi},$$

luego

$$b_{hi} = \varphi_i(v'_h) \overset{(4.7)}{=} \varphi_i\left(\sum_{l=1}^{n} a_{lh}v_l\right) = \sum_{l=1}^{n} a_{lh}\varphi_i(v_l) = \sum_{l=1}^{n} a_{lh}\delta_{il} = a_{ih}.$$

En resumen:

Proposición 4.2.1 *Con la notación anterior,*

$$M(1_{V^*}, B^*, B'^*) = M(1_V, B', B)^t. \tag{4.10}$$

4.3. Teorema de Reflexividad

Sean $V(\mathbb{K})$ un espacio vectorial y V^* su espacio dual. Podemos considerar el dual de V^*, llamado *bidual* $V^{**} = (V^*)^*$ *de* V,

$$V^{**} := \mathrm{Hom}_{\mathbb{K}}(V^*, \mathbb{K}) = \{\Gamma\colon V^* \to \mathbb{K} \mid \Gamma \text{ es lineal}\}.$$

Los tres espacios vectoriales V, V^*, V^{**} tienen la misma dimensión (finita), y por tanto, son isomorfos. Los isomorfismos existentes entre V y V^* dependen de bases (vía el Teorema 3.3.1), y lo mismo entre V^* y V^{**}. Sin embargo, veremos a continuación que hay un isomorfismo natural (independiente de bases) entre V y V^{**}. Esto nos permitirá identificar V con V^{**} sin recurrir a elementos auxiliares, y evita tener que considerar sucesivos duales $V^{***}, \ldots$ (por ejemplo, V^{***} de isomorfo de forma natural a V^*).

Lema 4.3.1 *Fijado un vector $v \in V$, la aplicación*

$$\begin{array}{rccc} \Phi_v\colon & V^* & \to & \mathbb{K} \\ & \varphi & \mapsto & \varphi(v) \end{array} \tag{4.11}$$

es lineal y, por tanto, pertenece al bidual V^{**} de V.

Demostración. Aplicando (4.11), $\Phi_v(a\,\varphi + b\,\psi) = (a\,\varphi + b\,\psi)(v) = a\,\varphi(v) + b\,\psi(v) = a\,\Phi_v(\varphi) + b\,\Phi_v(\psi)$, $\forall \varphi, \psi \in V^*$, $\forall a, b \in \mathbb{K}$. □

Teorema 4.3.1 (de Reflexividad) *Sea $V(\mathbb{K})$ un espacio vectorial de dimensión finita. Entonces, la aplicación*

$$\begin{array}{rccc} \Phi\colon & V & \to & V^{**} \\ & v & \mapsto & \Phi(v) = \Phi_v \end{array} \tag{4.12}$$

es un isomorfismo de espacios vectoriales.

Demostración. Por el Lema 4.3.1, Φ tiene codominio V^{**}. Veamos que Φ es lineal: sean $v, w \in V$, $a, b \in \mathbb{K}$. Queremos comprobar que $\Phi_{a\,v+b\,w}$ coincide con $a\,\Phi_v + b\,\Phi_w$. Como ambas son formas lineales sobre V^*, las aplicamos a cualquier $\varphi \in V^*$:

$$\begin{array}{rcl} \Phi_{a\,v+b\,w}(\varphi) & = & \varphi(a\,v + b\,w) = a\,\varphi(v) + b\,\varphi(w), \\ (a\,\Phi_v + b\,\Phi_w)(\varphi) & = & a\,\Phi_v(\varphi) + b\,\Phi_w(\varphi) = a\,\varphi(v) + b\,\varphi(w), \end{array}$$

luego Φ es lineal.
Veamos que Φ es biyectiva: como $\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} V^{**}$ (finita), basta comprobar que

$\ker(\Phi) = \{0\}$. Sea $v \in \ker(\Phi)$, es decir, $\Phi_v = \Gamma_0 \in V^{**}$, siendo esta la forma lineal nula sobre V^*. Por tanto, $\forall \varphi \in V^*$ se tiene

$$0 = \Phi_v(\varphi) \overset{(4.11)}{=} \varphi(v),$$

lo que implica que $v = 0$ por el Corolario 4.2.1. $\square$

Corolario 4.3.1 *Toda base de V^* es la base dual de una única base B de V.*

Demostración. Tomemos una base ordenada $B' = (\varphi_1, \ldots, \varphi_n)$ de V^*. Consideremos su base dual $B'^* = (\Gamma_1, \ldots, \Gamma_n) \subset V^{**}$. Como Φ dada por (4.12) es un isomorfismo de espacios vectoriales, para cada $i = 1, \ldots, n$ existe un único $v_i \in V$ tal que $\Gamma_i = \Phi(v_i) = \Phi_{v_i}$, y $B := (v_1, \ldots, v_n)$ es una base ordenada de V. Dados $i, j = 1, \ldots, n$,

$$\varphi_i(v_j) \overset{(4.11)}{=} \Phi_{v_j}(\varphi_i) = \Gamma_j(\varphi_i) = \delta_{ji} = \delta_{ij},$$

luego la base ordenada dual de B es B'. $\square$

Nota 4.3.1 El significado del Teorema de Reflexividad puede entenderse como sigue. Sean B, B' dos bases de $V(\mathbb{K})$. Sabemos que existe un único isomorfismo $F : V \to V^*$ que, de manera ordenada, aplica B en B^* y, análogamente, un único isomorfismo $G : V^* \to V^{**}$ que aplica B^* en su base dual B^{**}. De igual modo, con B' obtenemos isomorfismos $\overline{F} : V \to V^*$, $\overline{G} : V^* \to V^{**}$. En general, $F \neq \overline{F}$ y $G \neq \overline{G}$. Sin embargo, las composiciones $G \circ F, \overline{G} \circ \overline{F} : V \to V^{**}$ sí verifican $G \circ F = \overline{G} \circ \overline{F}$; de hecho, por el corolario 4.3.1 ambos coinciden con el isomorfismo que proporciona el Teorema de Reflexividad.

4.4. Anuladores

Definición 4.4.1 Sea $V(\mathbb{K})$ un espacio vectorial y $H \subset V$. Se define el *anulador de H* como el subconjunto de V^*

$$\mathrm{an}(H) = \{\varphi \in V^* \mid \varphi(v) = 0, \forall v \in H\}.$$

Lema 4.4.1 *El anulador verifica las siguientes propiedades (no se necesita que $V(\mathbb{K})$ tenga dimensión finita):*

1. *Dado $H \subset V$, $\mathrm{an}(S)$ es un subespacio vectorial de V^*.*
2. *Si $H \subset H' \subset V$, entonces $\mathrm{an}(H') \leq \mathrm{an}(H)$.*
3. *Dado $H \subset V$, $\mathrm{an}(H) = \mathrm{an}(L(H))$.*

4. *$\mathrm{an}(\{0\}) = V^*$ y $\mathrm{an}(V) = \{\varphi_0\}$ (forma lineal nula).*

Demostración. Veamos el apartado 1. Sean $\varphi, \psi \in \mathrm{an}(H)$, $a, b \in \mathbb{K}$. Para cualquier vector $v \in H$, $(a\,\varphi + b\,\psi)(v) = a\,\varphi(v) + b\,\psi(v) = a\,0 + b\,0 = 0$, luego $a\,\varphi + b\,\psi \in \mathrm{an}(H)$.

Supongamos que $H \subset H'$; basta comprobar que $\mathrm{an}(H') \subset \mathrm{an}(H)$ para que sea $\mathrm{an}(H') \leq \mathrm{an}(H)$, así que tomemos $\varphi \in \mathrm{an}(H')$. Como φ anula a todos los elementos de H' y $H \subset H'$, φ anulará a todos los elementos de H, es decir, $\varphi \in \mathrm{an}(H)$.

Para el apartado 3, la inclusión $\mathrm{an}(H) \supseteq \mathrm{an}(L(H))$ es consecuencia del apartado 2. Para la otra inclusión, $\varphi \in \mathrm{an}(H)$ y $w \in L(H)$. Como $w = \sum_{i=1}^m a_i\, v_i$ con $v_1, \ldots, v_m \in H$ y $a_1, \ldots, a_m \in \mathbb{K}$, tenemos $\varphi(w) = \varphi(\sum_{i=1}^m a_i\, v_i) = \sum_{i=1}^m a_i\, \varphi(v_i) = \sum_{i=1}^m a_i\, 0 = 0$.

Como toda forma lineal anula al vector 0, $\mathrm{an}(\{0\}) = V^*$. Que $\mathrm{an}(V) \supseteq \{\varphi_0\}$ es trivial ya que $\mathrm{an}(H)$ es siempre un subespacio vectorial. Recíprocamente, si $\varphi \in \mathrm{an}(V)$ entonces φ anula a todos los vectores de V, es decir, $\varphi = \varphi_0$. □

Definición 4.4.2 Sea $V(\mathbb{K})$ un espacio vectorial con dimensión finita y $H \subset V^*$. Aplicando la Definición 4.4.1 a H, deberíamos definir el anulador de H como

$$\widetilde{\mathrm{an}}(H) = \{\Gamma \in V^* \mid \Gamma(\varphi) = 0, \forall \varphi \in H\} \leq V^*.$$

Usando el isomorfismo Φ dado por el Teorema de Reflexividad, definimos el anulador de H como

$$\mathrm{an}(H) := \Phi^{-1}(\widetilde{\mathrm{an}}(H)) = \{v \in V \mid \varphi(v) = 0, \forall \varphi \in H\} \leq V. \tag{4.13}$$

Teorema 4.4.1 *Sea $V(\mathbb{K})$ un espacio vectorial con $\dim_{\mathbb{K}} V = n$ y $U \leq V$ con $\dim_{\mathbb{K}} U = m \leq n$. Se tienen:*

1. *$\dim_{\mathbb{K}} \mathrm{an}(U) = n - m$.*

2. *Si $H \subset V$, entonces $\mathrm{an}\,(\mathrm{an}(H)) = L(H)$. En particular, $\mathrm{an}\,(\mathrm{an}(U)) = U$.*

3. *Dado $W \leq V$, se tiene que $U = W$ si y sólo si $\mathrm{an}(U) = \mathrm{an}(W)$.*

Demostración. Para el apartado 1, tomemos una base ordenada $B = (v_1, \ldots, v_n)$ de V, de forma que $B_U := (v_1, \ldots, v_m)$ es base ordenada de U. Sea $B^* = (\varphi_1, \ldots, \varphi_n)$ la base ordenada dual de B. La condición (4.3) implica que $\varphi_{m+1}, \ldots, \varphi_n \in \mathrm{an}(U)$. Como $\{\varphi_{m+1}, \ldots, \varphi_n\}$ es un conjunto linealmente independiente, si probamos que es sistema de generadores de $\mathrm{an}(U)$ será base de $\mathrm{an}(U)$ y podremos concluir el apartado 1. Sea $\varphi \in \mathrm{an}(U)$. Escribimos φ en combinación lineal de B^*, $\varphi = b_1\,\varphi_1 + \ldots + b_m\,\varphi_m + b_{m+1}\,\varphi_{m+1} + \ldots + b_n\,\varphi_n$. Por (4.6), $b_i = \varphi(v_i)$. Como $v_i \in U$ para $i = 1, \ldots, m$ y $\varphi \in \mathrm{an}(U)$, deducimos que $b_i = 0$ $\forall i = 1, \ldots, m$. Así que $\varphi \in L(\{\varphi_{m+1}, \ldots, \varphi_n\})$.

Para el apartado 2, la definición (4.13) nos dice que

$$\mathrm{an}\,(\mathrm{an}(H)) = \{v \in V \mid \varphi(v) = 0, \forall \varphi \in \mathrm{an}(H)\}.$$

Dado $v \in H$, se tiene que $\varphi(v) = 0\ \forall \varphi \in \mathrm{an}(H)$, luego $H \subset \mathrm{an}\,(\mathrm{an}(H))$. Como $\mathrm{an}\,(\mathrm{an}(H)) \leq V$ (por el apartado 1 del Lema 4.4.1) y $L(H)$ es el menor subespacio de V que contiene a H, deducimos que $L(H) \subset \mathrm{an}\,(\mathrm{an}(H))$. Llamemos $k := \dim_{\mathbb{K}} L(H)$. Por el apartado 1 de este teorema, $\dim_{\mathbb{K}} \mathrm{an}(L(H)) = n - k$. Como los isomorfismos de espacios vectoriales conservan dimensiones,

$$\begin{aligned} \dim_{\mathbb{K}} \mathrm{an}\,(\mathrm{an}(H)) &\overset{(4.13)}{=} \dim_{\mathbb{K}} \Phi^{-1}\left[\widetilde{\mathrm{an}}\,(\mathrm{an}(H))\right] = \dim_{\mathbb{K}} \widetilde{\mathrm{an}}\,(\mathrm{an}(H)) \\ &\overset{(\star)}{=} \dim_{\mathbb{K}} V^* - \dim_{\mathbb{K}} \mathrm{an}(H) = n - (n-k) = k, \end{aligned}$$

donde en $(\star)$ hemos aplicado el apartado 1 al subespacio $\mathrm{an}(H) \leq V^*$. Así, $L(H)$ es un subespacio vectorial de $\mathrm{an}\,(\mathrm{an}(H))$ y ambos tienen la misma dimensión finita. Esto prueba que $L(H) = \mathrm{an}\,(\mathrm{an}(H))$.

Para el apartado 3, si $U = W$ es trivial que $\mathrm{an}(U) = \mathrm{an}(W)$. Recíprocamente, si $\mathrm{an}(U) = \mathrm{an}(W)$ tomamos anuladores en ambos miembros y aplicamos el apartado 2, con lo que $U = \mathrm{an}\,(\mathrm{an}(U)) = \mathrm{an}\,(\mathrm{an}(W)) = W$. $\square$

Nota 4.4.1 Es importante destacar que la demostración del apartado 1 del Teorema 4.4.1 da un algoritmo para construir explícitamente una base del anulador de un subespacio $U \subset V$:

Paso 1. Calculamos una base ordenada $B_U = \{v_1, \ldots, v_m\}$ de U.

Paso 2. Ampliamos B_U a una base ordenada $B = (v_1, \ldots, v_m, v_{m+1}, \ldots, v_n)$ de V.

Paso 3. Calculamos la base ordenada dual $B^* = (\varphi_1, \ldots, \varphi_m, \varphi_{m+1}, \ldots, \varphi_n)$ de B.

Paso 4. Nos quedamos con $\{\varphi_{m+1}, \ldots, \varphi_n\}$, que es base de $\mathrm{an}(U)$.

4.5. Soluciones de un SEL homogéneo como anulador de formas

Consideremos un SEL homogéneo

$$\left\{ \begin{array}{ccccccccc} a_{11}\,x_1 & + & a_{12}\,x_2 & + & \ldots & + & a_{1n}\,x_n & = & 0 \\ a_{21}\,x_1 & + & a_{22}\,x_2 & + & \ldots & + & a_{2n}\,x_n & = & 0 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{m1}\,x_1 & + & a_{m2}\,x_2 & + & \ldots & + & a_{mn}\,x_n & = & 0 \end{array} \right. \tag{4.14}$$

Viendo los coeficientes de cada ecuación como una matriz fila

$$a_i := (a_{i1}, \ldots, a_{in}) \in \mathcal{M}_{1\times n}(\mathbb{K}),$$

y ésta como una forma lineal $\varphi_{a_i} \in \mathcal{M}_{n\times 1}(\mathbb{K})^*$ (Ejemplo 4.1.1), tenemos que el conjunto de soluciones del SEL es

$$\{\text{Soluciones de (4.14)}\} = \text{an}(\{\varphi_{a_1}, \ldots, \varphi_{a_m}\}).$$

Por tanto, la dimensión del conjunto de soluciones del SEL es la dimensión del anulador anterior. Usando el apartado 1 del Teorema 4.4.1, concluimos que

Corolario 4.5.1 *La dimensión del conjunto de soluciones de un SEL homogéneo con m ecuaciones y n incógnitas es $n-k$, siendo k el número de ecuaciones linealmente independientes.*

4.6. Traspuesta de una aplicación lineal

Sean V, V' dos espacios vectoriales sobre un cuerpo conmutativo $\mathbb{K}$ y $f : V \to V'$ una aplicación lineal. Para cada $\varphi' \in V'^*$ podemos considerar la composición $\varphi' \circ f\colon V \to \mathbb{K}$, que es lineal por ser composición de lineales. Por tanto, $\varphi' \circ f \in V^*$.

Definición 4.6.1 Dada una aplicación lineal $f\colon V \to V'$, su *aplicación traspuesta* se define como

$$\begin{aligned} f^t : V'^* &\to V^* \\ \varphi' &\mapsto f^t(\varphi') := \varphi' \circ f. \end{aligned}$$

Proposición 4.6.1 *Sea $f\colon V \to V'$ una aplicación lineal.*

1. *f^t es lineal.*
2. *$(1_V)^t = 1_{V^*}$.*
3. *Si $g\colon V \to V'$ es lineal, entonces $(f+g)^t = f^t + g^t$ y $(a\,f)^t = a\,f^t$.*
4. *Si $h : V' \to V''$ es lineal, entonces $(h\circ f)^t = f^t \circ h^t$.*
5. *A partir de ahora supongamos que* $\dim_{\mathbb{K}} V = n$, $\dim_{\mathbb{K}} V' = m$ *son finitas. Entonces, la aplicación* trasposición

$$\begin{array}{rccc} t\colon & \text{Hom}_{\mathbb{K}}(V, V') & \to & \text{Hom}_{\mathbb{K}}(V'^*, V^*) \\ & f & \mapsto & f^t \end{array}$$

es un isomorfismo de espacios vectoriales. Además,

$$f = (\Phi')^{-1} \circ (f^t)^t \circ \Phi \qquad \textit{(esto se simplifica escribiendo } f = (f^t)^t\textit{)}, \tag{4.15}$$

donde $\Phi\colon V \to V^{**}$ *y* $\Phi'\colon V' \to V'^{**}$ *son los isomorfismos dados por el Teorema de Reflexividad.*

Demostración. Para el apartado 1, sean $\varphi', \psi' \in V'^*$ y $a, b \in \mathbb{K}$. Entonces, $f^t(a\,\varphi' + b\,\psi') = (a\,\varphi' + b\,\psi') \circ f = a\,(\varphi' \circ f) + b\,(\psi' \circ f) = a\,f^t(\varphi') + b\,f^t(\psi')$.
Veamos el apartado 2. Dada $\varphi \in V^*$, $(1_V)^t(\varphi) = \varphi \circ 1_V = \varphi$.
Para el apartado 3, tanto $(f+g)^t$ como $f^t + g^t, (a\,f)^t$ y $a\,f^t$ son aplicaciones lineales de V'^* en V^*. Dada $\varphi \in V'^*$,

$$\begin{array}{rcl}(f+g)^t(\varphi') & = & \varphi' \circ (f+g) = (\varphi' \circ f) + (\varphi' \circ g) = f^t(\varphi') + g^t(\varphi') = (f^t + g^t)(\varphi'). \\ (a\,f)^t(\varphi') & = & \varphi' \circ (a\,f) = a\,(\varphi' \circ f) = a\,f^t(\varphi') = (a\,f^t)(\varphi').\end{array}$$

Para el apartado 4, notemos que tanto $(h \circ f)^t$ como $f^t \circ h^t$ son aplicaciones de V''^* en V^*. Dada $\varphi'' \in V''^*$,

$$(h \circ f)^t(\varphi'') \;\; = \;\; \varphi'' \circ (h \circ f) = (\varphi'' \circ h) \circ f = f^t(\varphi'' \circ h) = f^t(h^t(\varphi'')) = (f^t \circ h^t)(\varphi'').$$

Finalmente, para el apartado 5 supondremos que $\dim_{\mathbb{K}} V = n$ y $\dim_{\mathbb{K}} V' = m$. En el apartado 3 probamos que la aplicación trasposición t es lineal. Como $\dim_{\mathbb{K}} \mathrm{Hom}_{\mathbb{K}}(V, V') = n \cdot m = \mathrm{Hom}_{\mathbb{K}}(V'^*, V^*)$, basta probar que t es inyectiva. Para ver esto último, basta construir una inversa a izquierda de t, es decir, una aplicación

$$\Psi\colon \mathrm{Hom}_{\mathbb{K}}(V'^*, V^*) \to \mathrm{Hom}_{\mathbb{K}}(V, V')$$

tal que $\Psi \circ t = 1_{\mathrm{Hom}_{\mathbb{K}}(V,V')}$. Definimos Ψ así: dada $g \in \mathrm{Hom}_{\mathbb{K}}(V'^*, V^*)$, sabemos que $g^t \in \mathrm{Hom}_{\mathbb{K}}(V^{**}, V'^{**})$, luego tiene sentido definir

$$\Psi(g) := (\Phi')^{-1} \circ g \circ \Phi\colon V \to V', \tag{4.16}$$

que está en $\mathrm{Hom}_{\mathbb{K}}(V, V')$ por ser composición de aplicaciones lineales. Ahora tomemos $f \in \mathrm{Hom}_{\mathbb{K}}(V, V')$, queremos ver que $(\Psi \circ t)(f) = f$, es decir, que $(\Phi')^{-1} \circ (f^t)^t \circ \Phi = f$ (esta es la igualdad que aparece en el apartado 5). Dado $x \in V$,

$$[(\Phi')^{-1} \circ (f^t)^t \circ \Phi](x) = [(\Phi')^{-1} \circ (f^t)^t](\Phi_x) = (\Phi')^{-1}((f^t)^t(\Phi_x)) = (\Phi')^{-1}(\Phi_x \circ f^t),$$

luego debemos comprobar que $(\Phi')^{-1}(\Phi_x \circ f^t) = f(x)$, o lo que es lo mismo, que $\Phi_x \circ f^t = \Phi'_{f(x)}$. Tanto $\Phi_x \circ f^t$ como $\Phi'_{f(x)}$ son formas lineales sobre V'^*, así que tomemos $\varphi' \in V'^*$.

$$(\Phi_x \circ f^t)(\varphi') = \Phi_x(f^t(\varphi')) = \Phi_x(\varphi' \circ f) = (\varphi' \circ f)(x) = \varphi'(f(x)) = \Phi'_{f(x)}(\varphi').$$

Esto prueba el apartado 5. □

Ahora relacionaremos las matrices de f y f^t en un par de bases ordenadas, lo cual justifica el nombre de traspuesta para f^t.

Proposición 4.6.2 *Sean V, V' espacios vectoriales sobre un cuerpo conmutativo $\mathbb{K}$ con $\dim_{\mathbb{K}} V = n$, $\dim_{\mathbb{K}} V' = m$ (finitas), y sea $f\colon V \to V'$ lineal. Dadas bases ordenadas B, B' de V, V' respectivamente y sus bases ordenadas duales B^*, B'^*, se tiene*

$$M(f^t, B'^*, B^*) = M(f, B, B')^t. \tag{4.17}$$

Demostración. Fijemos la notación, llamando

$$B = (v_1, \ldots, v_n),\ B' = (v'_1, \ldots, v'_m),\ B^* = (\varphi_1, \ldots, \varphi_n),\ B'^* = (\varphi'_1, \ldots, \varphi'_m).$$

Sea $(a_{ij})_{ij} = M(f, B, B') \in \mathcal{M}_{m\times n}(\mathbb{K})$ y $(b_{kh})_{kh} = M(f^t, B'^*, B^*) \in \mathcal{M}_{n\times m}(\mathbb{K})$. Así,

$$\begin{aligned} f(v_j) &= \sum_{i=1}^{n} a_{ij} v'_i, \quad \forall j = 1, \ldots, n, \\ f^t(\varphi'_h) &= \sum_{k=1}^{n} b_{kh} \varphi_k, \quad \forall h = 1, \ldots, m. \end{aligned}$$

Aplicando (4.6) a $f^t(\varphi'_h) \in V^*$, tenemos que su coordenada j-ésima respecto a B^* es

$$\begin{aligned} b_{jh} &= [f^t(\varphi'_h)](v_j) = (\varphi'_h \circ f)(v_j) = \varphi'_h(f(v_j)) = \varphi'_h\left(\sum_{i=1}^{n} a_{ij} v'_i\right) \\ &= \sum_{i=1}^{n} a_{ij} \varphi'_h(v'_i) = \sum_{i=1}^{n} a_{ij} \delta_{hi} = a_{jh}, \end{aligned}$$

lo que prueba la proposición. □

Nota 4.6.1

1. Tomando $f = 1_V$ en (4.17) se redemuestra la fórmula de cambio de base (4.10).
2. Usando la relación entre $\mathrm{Hom}_{\mathbb{K}}(V, V')$ y $\mathcal{M}_{m\times n}(\mathbb{K})$, entre $\mathrm{Hom}_{\mathbb{K}}(V'^*, V^*)$ y $\mathcal{M}_{n\times m}(\mathbb{K})$, y usando (4.17) tenemos que la aplicación $A \in \mathcal{M}_{m\times n}(\mathbb{K}) \mapsto A^t \in \mathcal{M}_{n\times m}(\mathbb{K})$ es un isomorfismo de espacios vectoriales. Además, la fórmula (4.15) y el apartado 4 de la Proposición 4.6.1 redemuestran los apartados 8 y 9 de la Proposición 1.1.1.

Recordemos que teníamos pendiente una demostración del Teorema del Rango (los rangos por filas y por columnas de cualquier matriz coinciden). Ya podemos demostrarlo.

Teorema 4.6.1 *Sean $V, V'(\mathbb{K})$ espacios vectoriales finitamente generados y $f\colon V \to V'$ una aplicación lineal. Entonces:*

1. $\mathrm{an}(\mathrm{Im}(f)) = \ker(f^t)$.

2. $\mathrm{an}(\ker(f)) = \mathrm{Im}(f^t)$.

3. $\mathrm{rango}(f) = \mathrm{rango}(f^t)$.

En consecuencia, para cualquier matriz $A \in M_{m\times n}(\mathbb{K})$ *se tiene* $\mathrm{rango}(A) = \mathrm{rango}(A^t)$.

Demostración. Veamos el primer apartado por doble inclusión.
$\boxed{\mathrm{an}(\mathrm{Im}(f)) \subseteq \ker(f^t).}$ Dada $\varphi' \in \mathrm{an}(\mathrm{Im}(f))$, veamos que $f^t(\varphi') = \varphi_0$ (forma lineal nula sobre V): Dado $x \in V$, $[f^t(\varphi')](x) = (\varphi' \circ f)(x) = \varphi'(f(x))$, que se anula porque $\varphi' \in \mathrm{an}(\mathrm{Im}(f))$ y $f(x) \in \mathrm{Im}(f))$. Por tanto, $f^t(\varphi') = \varphi_0$ luego $\varphi' \in \ker(f^t)$.
$\boxed{\mathrm{an}(\mathrm{Im}(f)) \supseteq \ker(f^t).}$ Dada $\varphi' \in \ker(f^t)$, veamos que φ' anula a cualquier $y \in \mathrm{Im}(f)$. Dado $y \in \mathrm{Im}(f)$, existe $x \in V$ tal que $y = f(x)$. Así que $\varphi'(y) = \varphi'(f(x)) = (\varphi' \circ f)(x) = [f^t(\varphi')](x) = \varphi_0(x) = 0$.
Para el apartado 2 veremos sólo la inclusión $\boxed{\supseteq}$ y que las dimensiones coinciden.
$\boxed{\mathrm{an}(\ker(f)) \supseteq \mathrm{Im}(f^t)}$. Dada $\varphi \in \mathrm{Im}(f^t)$, existe $\varphi' \in V^*$ tal que $f^t(\varphi') = \varphi$. Veamos que φ anula a todos los vectores del núcleo de f: Dado $x \in \ker(f)$, $\varphi(x) = [f^t(\varphi')](x) = (\varphi' \circ f)(x) = \varphi'(f(x)) = \varphi'(0) = 0$.
Finalmente,

$$\dim_{\mathbb{K}} \mathrm{an}(\ker(f)) \overset{(*)}{=} n - \dim_{\mathbb{K}} \ker(f) = \mathrm{rango}(f), \tag{4.18}$$

donde en $(\star)$ hemos usado el apartado 1 del Teorema 4.4.1, y en la última igualdad hemos usado la Fórmula de la Nulidad y el Rango. Esto termina de probar el apartado 2.

Para el apartado 3, usamos el apartado 2 para igualar el miembro de la izquierda de (4.18) a $\dim_{\mathbb{K}} \mathrm{Im}(f^t)$, que es por definición el rango de f^t.

Finalmente, si $A \in M_{m\times n}(\mathbb{K})$, entonces tomemos $V, V'(\mathbb{K})$ con dimensiones n, m y bases ordenadas B, B' respectivas. Así, $\exists! f \in \mathrm{Hom}_{\mathbb{K}}(V, V')$ tal que $M(f, B, B') = A$. Por el Corolario 3.5.3, $\mathrm{rango} A) = \mathrm{rango}(f)$. Por el apartado 3 de este teorema, $\mathrm{rango}(f) = \mathrm{rango}(f^t)$, y de nuevo por el Corolario 3.5.3, $\mathrm{rango}(f^t) = \mathrm{rango} M(f^t, B'^*, B^*)$, que es A^t por la fórmula (4.17) □

Nota 4.6.2 1. Una vez probado el Teorema del Rango para matrices, podemos eliminar "rango por columnas" o "rango por filas" y sustituirlo simplemente por "rango" cada una de las veces que lo hemos usado durante el curso.

2. Toda la teoría de aplicaciones lineales se puede desarrollar independientemente de la de matrices, lo que permite deducir las propiedades de las matrices a partir de las aplicaciones lineales.

3. La inclusión $\mathrm{an}(\ker(f)) \subseteq \mathrm{Im}(f^t)$ se puede probar directamente, aunque no nos ha hecho falta (Ejercicio 19).

4.7. Determinantes de endomorfismos y matrices

Nos quedaba por demostrar el apartado 10 de la Proposición 1.4.2, que había sido pospuesto porque íbamos a deducirlo de la correspondiente propiedad para el determinante de un endomorfismo. También teníamos pendiente deducir que el determinante de un endomorfismo $f \in \mathrm{End}_{\mathbb{K}} V$ es el determinante de cualquiera de las matrices semejantes que se obtienen como $M(f, B)$, siendo B una base ordenada de V (pie de página 5 justo antes de la Definición 3.6.2). Haremos todo esto en esta sección.

Como es habitual, $V(\mathbb{K})$ denotará un espacio vectorial de dimensión $n \in \mathbb{N}$ sobre un cuerpo conmutativo $\mathbb{K}$ de característica distinta de 2.

4.7.1. Tensores antisimétricos

Definición 4.7.1 Sea $r \in \mathbb{N}$. Diremos que una aplicación

$$T \colon V \times \overset{r)}{\cdots} \times V \to \mathbb{K} \tag{4.19}$$

es un *tensor antisimétrico de orden m* si cumple:

1. *(Multilinealidad).* Para cada $i = 1, \ldots m$,

$$\begin{aligned} T(w_1, \ldots, w_i + w_i', \ldots, w_n) &= T(w_1, \ldots, w_i, \ldots, w_n) + T(w_1, \ldots, w_i', \ldots, w_n), \\ T(w_1, \ldots, a\, w_i, \ldots, w_m) &= a\, T(w_1, \ldots, w_i, \ldots, w_n), \end{aligned}$$

   $\forall w_1, \ldots, w_i, w_i', \ldots, w_n \in V$, $\forall a \in \mathbb{K}$.

2. *(Antisimetría).* Para cada par de variables $i, j \in \{1, \ldots, r\}$, $i < j$,

$$T(w_1, \ldots, w_i, \ldots, w_j, \ldots, w_n) = -D(w_1, \ldots, w_j, \ldots, w_i, \ldots, w_n). \tag{4.20}$$

Nota 4.7.1

1. Si no imponemos la condición 2, a T se le llama *tensor r-covariante*. Hay una generalización a aplicaciones multilineales de $V \times \overset{r)}{\cdots} \times V \times V^* \times \overset{s)}{\cdots} \times V^* \to \mathbb{K}$, llamados *tensores r-covariantes y s-contravariantes,* o *de tipo* (r, s).

2. Como la característica de $\mathbb{K}$ es distinta de 2, la propiedad 2 de antisimetría es equivalente a la de ser *alternado*, esto es, dados $i, j \in 1, \ldots, r$ con $i < j$,

$$\text{Si } w_i = w_j \;\Rightarrow\; T(w_1, \ldots, w_i, \ldots, w_j, \ldots, w_r) = 0. \tag{4.21}$$

3. La multilinealidad de T nos dice que si T es antisimétrico (o alternado) y lo evaluamos sobre una lista $(w_1, \ldots, w_r) \in V \times \overset{r)}{\cdots} \times V$ donde los vectores son linealmente dependientes, entonces $T(w_1, \ldots, w_r) = 0$.

Ejemplo 4.7.1 1. La aplicación $T\colon \mathbb{K}^n \times \overset{n)}{\cdots} \times \mathbb{K}^n \to \mathbb{K}$ dada por $T(A) = \det(A)$, donde vemos A como una lista de n elementos de $\mathbb{K}^n$ por sus columnas, es un tensor antisimétrico de orden n (apartados 1, 2, 3 de la Proposición 1.4.2).

2. Sea $V(\mathbb{K})$ un espacio vectorial sobre $\mathbb{K}$ con $\dim_{\mathbb{K}} V = n$, y $B = (v_1, \ldots, v_n)$ una base ordenada de V. La aplicación $\det_B\colon V \times \overset{n)}{\cdots} \times V \to \mathbb{K}$ dada por
(4.22)
$$\det_B(w_1, \ldots, w_n) = \begin{cases} 0 & \text{si } w_1, \ldots, w_n \text{ son linealmente dependientes,} \\ \det M(1_V, B', B) & \text{si } B' := (w_1, \ldots, w_n) \text{ es base de } V. \end{cases}$$
es un tensor antisimétrico de orden n. Además, $\det_B(v_1, \ldots, v_n) = 1$. A $\det_B$ se le llama el *tensor determinante en la base ordenada B.*

Es fácil comprobar que el conjunto $\mathcal{A}_r(V)$ de todos los tensores antisimétricos de orden r sobre V tiene una estructura de espacio de espacio vectorial con la suma y el producto por escalares habitual. El apartado 4 de la Nota 4.7.1 y el Corolario 2.6.1 nos dicen que si $r > n$, entonces $\mathcal{A}_r(V) = \{0\}$. En lo que sigue nos centraremos en estudiar el caso $r = n$, que es el que aparece al estudiar determinantes (apartado 2 de la Nota 4.7.1). Del apartado 2 del Ejemplo 4.7.1 deducimos que si B es una base ordenada de un espacio vectorial $V^n(\mathbb{K})$, entonces $\det_B \in \mathcal{A}_n(V) \setminus \{0\}$.

Proposición 4.7.1 *Sea $V(\mathbb{K})$ un espacio vectorial con* $\dim_{\mathbb{K}} V = n$, *y $T \in \mathcal{A}_n(V)$.*

1. Para cualquier permutación $\sigma \in S_n$,

$$T(w_{\sigma(1)}, \ldots, w_{\sigma(n)}) = \mathrm{sig}(\sigma) \cdot T(w_1, \ldots, w_n), \qquad \forall w_1, \ldots, w_n \in V,$$

donde sig *es la signatura de σ.*

2. T queda determinado por su valor sobre una base ordenada $B = (v_1, \ldots, v_n)$ de V. Esto es, si $T, T' \in \mathcal{A}_n(V)$ tales que $T(v_1, \ldots, v_n) = T'(v_1, \ldots, v_n)$, entonces $T = T'$.

3. $\dim_{\mathbb{K}} \mathcal{A}_n(V) = 1$.

Demostración. El apartado 1 es consecuencia directa de la propiedad de antisimetría de T, de que toda permutación se escribe como producto de trasposiciones (Lema 1.3.3), y del valor de la signatura (apartado (B) de la Definición 1.3.4).

Veamos el apartado 2: sean $w_1, \ldots, w_n \in V$. Si $\{w_1, \ldots, w_n\}$ es linealmente dependiente, entonces $T(w_1, \ldots, w_n) = T'(w_1, \ldots, w_n) = 0$ por el apartado 4 de la Nota 4.7.1. Así que podemos suponer que $\{w_1, \ldots, w_n\}$ es linealmente independiente. Por ser $\dim_{\mathbb{K}} V = n$, $B' := (w_1, \ldots, w_n)$ es una base ordenada de V.

Ahora escribimos el cambio de base de B a B'. Pongamos

$$w_j = \sum_{i=1}^{n} a_{ij} v_i, \qquad \forall j = 1, \ldots, n.$$

$$\begin{aligned} T(w_1, \ldots, w_n) &= T\left(\sum_{i_1=1}^{n} a_{i_1 1} v_{i_1}, \ldots, \sum_{i_n=1}^{n} a_{i_n n} v_{i_n} \right) \\ &= \sum_{i_1, \ldots, i_n=1}^{n} a_{i_1 1} \ldots a_{i_n n} \, T(v_{i_1}, \ldots, v_{i_n}). \end{aligned} \tag{4.23}$$

En la última esta expresión, cada sumando que tenga repetidos alguno de los índices $i_1, \ldots, i_n$ se anula porque $T(v_{i_1}, \ldots, v_{i_n})$ se anula en ese caso por (4.21). Sólo nos quedan los sumandos de (4.23) en que $i_1, \ldots, i_n$ no hay repeticiones, es decir $(i_1, \ldots, i_n)$ es una permutación de $(1, \ldots, n)$. Por tanto, (4.23) se escribe

$$\begin{aligned} T(w_1, \ldots, w_n) &= \sum_{\sigma \in S_n} a_{\sigma(1)1} \ldots a_{\sigma(n)n} \, T(v_{\sigma(1)}, \ldots, v_{\sigma(n)}) \\ &\overset{(\star)}{=} \sum_{\sigma \in S_n} a_{\sigma(1)1} \ldots a_{\sigma(n)n} \, \mathrm{sig}(\sigma) \cdot T(v_1, \ldots, v_n) \\ &= \left(\sum_{\sigma \in S_n} \mathrm{sig}(\sigma) \, a_{\sigma(1)1} \ldots a_{\sigma(n)n} \right) T(v_1, \ldots, v_n) \\ &= \det(A) \, T(v_1, \ldots, v_n), \end{aligned} \tag{4.24}$$

donde en $(\star)$ hemos usado el apartado 2 de esta proposición y $A = (a_{ij})_{i,j} = M(1_V, B', B) \in Gl(n, \mathbb{K})$.

Si seguimos los pasos anteriores para T' en lugar de T llegaremos a $T'(w_1, \ldots, w_n) = \det(A) \, T'(v_1, \ldots, v_n)$. Como $T(v_1, \ldots, v_n) = T'(v_1, \ldots, v_n)$ por hipótesis, deducimos que $T(w_1, \ldots, w_n) = T'(w_1, \ldots, w_n)$, lo que termina de probar el apartado 2.

Finalmente, veamos el apartado 3: Fijamos una base ordenada $B = (v_1, \ldots, v_n)$ de V y consideremos el tensor determinante $\det_B \in \mathcal{A}_n(V)$. Como $\det_B(v_1, \ldots, v_n) = 1$, deducimos que dado $T \in \mathcal{A}_n(V)$ llamando $T' := T(v_1, \ldots, v_n) \det_B$, se tiene $T(v_1, \ldots, v_n) = T'(v_1, \ldots, v_n)$. Por el apartado 2, $T = T'$, es decir

$$T = T(v_1, \ldots, v_n) \det_B . \tag{4.25}$$

$T \in \mathcal{A}_n(V)$ es arbitrario, tenemos que $\dim_{\mathbb{K}} \mathcal{A}_n(V) \leq 1$. Como $\det_B \in \mathcal{A}_n(V) \setminus \{0\}$, concluimos que $\dim_{\mathbb{K}} \mathcal{A}_n(V) \leq 1$. Como $\det_B \in \mathcal{A}_n(V) \setminus \{0\}$, tenemos $\dim_{\mathbb{K}} \mathcal{A}_n(V) = 1$. $\square$

La demostración del apartado 3 de la Proposición 4.7.1 nos dice que si $B = (v_1, \dots, v_n)$ es una base ordenada de V, entonces $\{\det_B\}$ es base de $\mathcal{A}_n(V)$, y que dado $T \in \mathcal{A}_n(V)$, la (única) coordenada de T en esa base es

$$T_{\det_B} = T(B) := T(v_1, \dots, v_n) \in \mathbb{K}. \tag{4.26}$$

En particular, $\det_B$ es el único tensor $T \in \mathcal{A}_n(V)$ tal que $T(v_1, \dots, v_n) = 1$.

El tensor determinante $\det_B$ se definió por casos en (4.22). Esto es así porque formalmente, $M(1_V, B', B)$ no tiene sentido como matriz de cambio de base cuando $\{w_1, \dots, w_n\}$ sea un conjunto linealmente dependiente. Esto puede solventarse escribiendo

$$w_j = \sum_{i=1}^{n} a_{ij} v_i, \quad \forall j = 1, \dots, n,$$

(que serían las ecuaciones de cambio de base si $\{w_1, \dots, w_n\}$ fuera base, y producen las coordenadas de $w_1, \dots, w_n$ respecto a B en el caso general), y ahora

$$\det_B(w_1, \dots, w_n) = \sum_{\sigma \in S_n} \mathrm{sig}(\sigma)\; a_{\sigma(1)1} \dots a_{\sigma(n)n} = \det(A), \tag{4.27}$$

donde $A = (a_{ij})_{i,j} \in \mathcal{M}_n(\mathbb{K})$ (en el caso de ser $B' = (w_1, \dots, w_n)$ una base ordenada, $A = M(1_V, B', B) \in Gl(n, \mathbb{K})$, mientras que en el caso $\{w_1, \dots, w_n\}$ linealmente dependiente, A tiene determinante cero). En resumen:

Corolario 4.7.1 *Sea $V(\mathbb{K})$ un espacio vectorial con $\dim_{\mathbb{K}} V = n$, y $B = (v_1, \dots, v_n)$ una base ordenada de V. Dados $w_1, \dots, w_n \in V$, se tiene que $\{w_1, \dots, w_n\}$ es base de V si y sólo si $\det_B(w_1, \dots, w_n) \neq 0$.*

Nota 4.7.2 La ecuación (4.27) relaciona el tensor antisimétrico $\det_B$ con el determinante de una matriz cuadrada, tal y como se definió en (1.4.1). Vale la pena tener esta relación como resultado para usarlo más adelante.

Corolario 4.7.2 *Sea B una base ordenada de un espacio vectorial $V(\mathbb{K})$ con $\dim_{\mathbb{K}} V = n$. Dados $w_1, \dots, w_n \in V$, sea $A \in \mathcal{M}_n(\mathbb{K})$ la matriz que se obtiene escribiendo por columnas $(w_1)_B, \dots, (w_n)_B$. Entonces,*

$$\det(A) = \det_B(w_1, \dots, w_n).$$

En particular, si B y B' son dos bases ordenadas de V,

$$\det M(1_V, B', B) = \det_B(B') \qquad y \qquad \det_{B'} = \det M(1_V, B, B') \det_B .$$

Demostración. La primera igualdad es (4.27); la segunda es un caso particular de ésta cuando $B' = (w_1, \ldots, w_n)$, y la tercera es consecuencia de (4.25) tomando $T = \det_{B'}$ (luego $\det_{B'}(v_1, \ldots, v_n) = \det M(1_V, B, B')$ a partir de (4.27) intercambiando los papeles de B y B'). □

Corolario 4.7.3 *Sea $V(\mathbb{K})$ un espacio vectorial con $\dim_{\mathbb{K}} V = n$, y $B = (v_1, \ldots, v_n)$ una base ordenada de V. Entonces, la aplicación*

$$\mathcal{A}_n(\mathbb{K}) \to \mathbb{K}, \qquad T \mapsto T(v_1, \ldots, v_n)$$

es un isomorfismo de espacios vectoriales.

Demostración. La aplicación es trivialmente lineal. Como su dominio y codominio son espacios vectoriales de dimensión 1, que sea un isomorfismo equivale a que no sea constante cero. Pero la imagen de $\det_B$ por la aplicación vale 1. □

Corolario 4.7.4 *Sea $V(\mathbb{K})$ un espacio vectorial con $\dim_{\mathbb{K}} V = n$ y $T \in \mathcal{A}_n(V) \setminus \{0\}$. Entonces, existe una base ordenada B' de V tal que $T = \det_{B'}$.*

Demostración. Tomemos una base ordenada auxiliar $B = (v_1, \ldots, v_n)$. Por el Corolario 4.7.3, tenemos $a := T(v_1, \ldots, v_n) \in \mathbb{K} \setminus \{0\}$. Definimos una nueva base como

$$B' = (v'_1 = a^{-1}\, v_1, v'_2 = v_2, \ldots, v'_n = v_n).$$

Entonces, $T(v'_1, \ldots, v'_n) = a^{-1}\, T(v_1, \ldots, v_n) = a^{-1}\, a = 1$. Por tanto, $T = \det_{B'}$. □

Nota 4.7.3 La base ordenada B' del Corolario 4.7.4 no es única: si B'' es otra base ordenada tal que $M(1_V, B'', B') = 1$, entonces $T = \det_{B''}$. Esto se deduce de aplicar (4.22) a B', B''.

4.7.2. Elementos de volumen

En geometría elemental, una base de $\mathbb{R}^2$ produce un paralelogramo y una de $\mathbb{R}^3$ un paralelepípedo. En general, en un espacio vectorial real $V(\mathbb{R})$ con $\dim_{\mathbb{R}} V = n$ diremos que una base ordenada $B = (u_1, \ldots, u_n)$ produce un *n-paralelelípedo* (o simplemente paralelepípedo) P_B, definido por

$$P_B := \{a_1 u_1 + \cdots + a_n u_n \mid a_1, \ldots, a_n \in [0, 1]\} \subset \mathbb{R}^n. \tag{4.28}$$

Definición 4.7.2 Sea $V(\mathbb{R})$ un espacio vectorial real con $\dim_{\mathbb{R}} V = n$. A los elementos de $\mathcal{A}_n(V) \setminus \{0\}$ se les llama *elementos de volumen* en V.

Fijado un elemento de volumen $T_1 \in \mathcal{A}_n(V) \setminus \{0\}$, el Corolario 4.7.4 asegura que para cada $T \in \mathcal{A}_n(V) \setminus \{0\}$ existe una base ordenada $B = (w_1, \ldots, w_n)$ de V (no única) tal que $T = \det_B$. B produce un paralelepípedo P_B como en (4.28).

En la situación anterior, llamaremos *volumen de P_B con respecto a T_1*

$$\mathrm{vol}_{T_1}(P_B) := |T_1(w_1, ..., w_n)| = |T_1(B)|,$$

donde $|\cdot|$ denota valor absoluto en $\mathbb{K} = \mathbb{R}$.

Nota 4.7.4 La expresión (4.28) de P_B y de su volumen $\mathrm{vol}_{T_1}(P_B)$ tienen sentido incluso si permitimos que los vectores de B sean linealmente dependientes: en este caso, P_B estará incluido en un subespacio vectorial de V con dimensión $< n$ (se podría considerar como un paralelepípedo degenerado), y su volumen es $\mathrm{vol}_{T_1}(P_B) = 0$.

Para justificar intuitivamente el nombre de volumen, notemos que

1. Sabemos que $T_1 = \det_{B_1}$ para alguna base ordenada $B_1 = (v_1, \ldots, v_n)$ de V que cumple $D_0(B_0) = 1$ (B_1 no es única). En particular, P_{B_1} tiene volumen 1 con respecto a T_1. Es decir, B_1 produce un paralelepípedo P_{B_1} de $V(\mathbb{R})$ que a su vez fija la "unidad de volumen", o "elemento de volumen unitario".

2. Si construimos a partir de B_1 una nueva base ordenada $B_2 = (m_1 v_1, \ldots, m_n v_n)$ con $m_1, \ldots, m_n > 0$, la multilinealidad de T_1) hace que

$$\mathrm{vol}_{T_1}(P_{B_2}) = |T_1(B_2)| = |m_1 \cdots m_n T_1(B_1)| = m_1 \cdots m_n.$$

   En el caso de que $m_1, \ldots, m_n \in \mathbb{N}$ sean enteros, esto es consistente con la intuición de que el paralelepípedo P_{B_2} ocuparía un volumen que sería cubierto por exactamente $m_1 \cdot m_2 \cdots m_n$ copias de P_{B_1}.

4.7.3. Determinante de un endomorfismo

Todo endomorfismo $f \in \mathrm{End}_{\mathbb{K}} V^n$ va a producir un endomorfismo del espacio vectorial $\mathcal{A}_n(V)$, que por tener dimensión 1, será un múltiplo de la identidad. Este múltiplo nos dará el determinante de f.

Lema 4.7.1 *Sea $V(\mathbb{K})$ un espacio vectorial con $\dim_{\mathbb{K}} V = n$ y $f \in \mathrm{End}_{\mathbb{K}} V$. Entonces,*

1. *Para cada $T \in \mathcal{A}_n(V)$, la aplicación*

$$\begin{array}{rccl} f^*T: & V \times \overset{(n)}{\cdots} \times V & \to & \mathbb{K} \\ & (w_1, \ldots, w_n) & \mapsto & T((f(w_1), \ldots, f(w_n)) \end{array}$$

   está en $\mathcal{A}_n(V)$.

2. *La aplicación:*
$$\begin{array}{rccc} f^*: & \mathcal{A}_n(V) & \to & \mathcal{A}_n(V) \\ & T & \mapsto & f^*T \end{array}$$
es lineal, es decir, $f^* \in \mathrm{End}_{\mathbb{K}}\mathcal{A}_n(V)$.

3. $(1_V)^* = 1_{\mathcal{A}_n(V)}$.

4. *Si* $h \in \mathrm{End}_{\mathbb{K}}V$*, entonces* $(f \circ h)^* = h^* \circ f^*$.

Demostración. Veamos el apartado 1.
$\boxed{\text{Multilinealidad.}}$
$$\begin{aligned} (f^*T)(w_1,\ldots,aw_i+bw_i',\ldots,w_n) &= T((f(w_1),\ldots,f(aw_i+bw_i'),\ldots,f(w_n)) \\ &= T((f(w_1),\ldots,af(w_i)+bf(w_i'),\ldots,f(w_n)) \\ &= a\,T(f(w_1),\ldots,f(w_i),\ldots,f(w_n)) \\ &\quad +b\,T(f(w_1),\ldots,f(w_i'),\ldots,f(w_n)) \\ &= a\,(f^*T)(w_1,\ldots,w_i,\ldots,w_n) \\ &\quad +b\,(f^*T)(w_1,\ldots,w_i,\ldots,w_n). \end{aligned}$$

$\boxed{\text{Antisimetría.}}$
$$\begin{aligned} (f^*T)(w_1,\ldots,w_i,\ldots,w_j,\ldots,w_n) &= T(f(w_1),\ldots,f(w_i),\ldots,f(w_j),\ldots,f(w_n)) \\ &= -T(f(w_1),\ldots,f(w_j),\ldots,f(w_i),\ldots,f(w_n)) \\ &= -(f^*T)(w_1,\ldots,w_j,\ldots,w_i,\ldots,w_n). \end{aligned}$$

Para el apartado 2, queremos ver que $f^*(aT+bT') = af^*T + bf^*T'$, siendo $a,b \in \mathbb{K}$ y $T,T' \in \mathcal{A}_n(V)$. Como ambos miembros son tensores en $\mathcal{A}_n(V)$, los aplicamos a la misma lista de n vectores de V:
$$\begin{aligned} [f^*(aT+bT')](w_1,\ldots,w_n) &= (aT+bT')((f(w_1),\ldots,f(w_n)) \\ &= a\,T(f(w_1),\ldots,f(w_n)) + b\,T'(f(w_1),\ldots,f(w_n)). \\ &= a\,f^*T(w_1,\ldots,w_n) + b\,f^*T'(w_1,\ldots,w_n) \\ &= (a\,f^*T + b\,f^*T')(w_1,\ldots,w_n). \end{aligned}$$

Para el apartado 3, tomemos $T \in \mathcal{A}_n(V)$. Dados $w_1,\ldots,w_n \in V$, $[(1_V)^*T](w_1,\ldots,w_n) = T(1_V(w_1),\ldots,1_V(w_n)) = T(w_1,\ldots,w_n)$, luego $(1_V)^*T = T$.

Por último, veamos el apartado 4. Tomemos $T \in \mathcal{A}_n(V)$ y $w_1,\ldots,w_n \in V$.
$$\begin{aligned} [(f\circ h)^*T](w_1,\ldots,w_n) &= T((f\circ h)(w_1),\ldots,(f\circ h)(w_n)) = T(f(h(w_1)),\ldots,f(h(w_n))) \\ &= (f^*T)(h(w_1),\ldots,h(w_n)) = [h^*(f^*T)](w_1,\ldots,w_n) \\ &= [(h^*\circ f^*)(T)]\,(w_1,\ldots,w_n). \end{aligned}$$

Por tanto, $(f\circ h)^*T = (h^*\circ f^*)(T)$ para todo $T \in \mathcal{A}_n(V)$. □

Como $\dim_{\mathbb{K}} \mathcal{A}_n(V) = 1$ (apartado 3 de la Proposición 4.7.1 y $f^*\colon \mathcal{A}_n(V) \to \mathcal{A}_n(V)$ es un endomorfismo, f^* es de la forma $f^* = d\,1_{\mathcal{A}_n(V)}$, para un único $d \in \mathbb{K}$.

Definición 4.7.3 Sea $V(\mathbb{K})$ un espacio vectorial con $\dim_{\mathbb{K}} V = n$ y $f \in \mathrm{End}_{\mathbb{K}} V$. Llamaremos *determinante de* f al escalar $\det f \in \mathbb{K}$ tal que $f^* = \det f \cdot 1_{\mathcal{A}_n(V)}$.

Veamos que $\det f$ coincide con $\det M(f,B)$ como habíamos anunciado.

Proposición 4.7.2 *Sea* $V(\mathbb{K})$ *un espacio vectorial finitamente generado y* $f \in \mathrm{End}_{\mathbb{K}} V$. *Dada una base ordenada* B *de* V, *se tiene* $\det f = \det M(f,B)$.

Demostración. Consideremos el tensor $\det_B \in \mathcal{A}_n(V)$. Como $f^* = \det(f)\cdot 1_{\mathcal{A}_n(V)}$, tenemos $f^* \det_B = \det f \cdot \det_B$. Aplicando esto a $B = (v_1, \ldots, v_n)$,

$$\begin{aligned} \det f &= \det f \, \det_B(v_1, \ldots, v_n) = (f^* \det_B)(v_1, \ldots, v_n) \\ &= \det_B(f(v_1), \ldots, f(v_n)) = \det M(f,B), \end{aligned}$$

donde la última igualdad es por el Corolario 4.7.2 tomando $w_i = f(v_i)$. □

Corolario 4.7.5 *Sea* $V(\mathbb{K})$ *un espacio vectorial con* $\dim_{\mathbb{K}} V = n$. *Entonces:*

1. $\det 1_V = 1$.
2. *Dados* $f, h \in \mathrm{End}_{\mathbb{K}} V$, $\det(f \circ h) = \det f \cdot \det h$.
3. $f \in \mathrm{End}_{\mathbb{K}} V$ *es biyectivo si y sólo si* $\det f \neq 0$. *En este caso,* $\det(f^{-1}) = (\det f)^{-1}$.
4. *Dado* $f \in \mathrm{End}_{\mathbb{K}} V$, $\det f = \det(f^t)$.

Demostración. El primer apartado es consecuencia directa del apartado 3 del Lema 4.7.1 y de la definición de $\det 1_V$.

Veamos el apartado 2: usando la definición de determinante de un endomorfismo y el apartado 4 del Lema 4.7.1,

$$\det(f \circ h)\cdot 1_{\mathcal{A}_n(V)} = (f \circ h)^* = h^* \circ f^* = (\det h \cdot 1_{\mathcal{A}_n(V)}) \circ (\det f \cdot 1_{\mathcal{A}_n(V)}) = (\det h \cdot \det f)\cdot 1_{\mathcal{A}_n(V)}.$$

Para el apartado 3, si f es biyectivo podemos tomar $h = f^{-1}$ en el apartado 2, con lo que $\det f \cdot \det(f^{-1}) = \det 1_V$, que vale 1 por el apartado 1. Así que $\det f \neq 0$ y $\det(f^{-1}) = (\det f)^{-1}$. Recíprocamente, si $\det f \neq 0$ entonces tomamos una base ordenada B de V y tenemos $\det f = \det M(f,B)$ por la Proposición 4.7.2. Así, $M(f,B)$ tiene determinante no nulo luego es regular (Corolario 1.4.1). Esto implica que f es biyectiva (apartado (B) de la Proposición 3.4.4).

El apartado 4 es cierto porque

$$\det f = \det M(f,B) \overset{\text{(Proposición 1.4.1)}}{=} \det(M(f,B)^t) \overset{\text{(Proposición 4.6.2)}}{=} \det M(f^t,B) = \det(f^t).$$

□

Traducimos el Corolario 4.7.5 a matrices, obteniendo algunas propiedades ya conocidas y otras que habíamos anunciado.

Corolario 4.7.6 *1.* $\det I_n = 1$.

2. Dadas $A, C \in \mathcal{M}_n(\mathbb{K})$*,* $\det(A \cdot C) = \det A \cdot \det C$.

3. $A \in Gl(n, \mathbb{K})$ *es regular si y sólo si* $\det A \neq 0$*. En este caso,* $\det(A^{-1}) = (\det A)^{-1}$.

4. Dada $A \in \mathcal{M}_n(\mathbb{K})$*,* $\det A = \det(A^t)$.

Demostración. Los apartados 1, 3 y 4 estaban ya probados (apartado 9 de la Proposición 1.4.2, Corolario 1.4.1 y Proposición 1.4.1). Queda probar el apartado 2 (es el apartado 10 de la Proposición 1.4.2, cuya demostración estaba por hacerse): Fijemos un espacio vectorial $V(\mathbb{K})$ de dimensión n y una base ordenada de V. Sean $f, h \in \mathrm{End}_{\mathbb{K}} V$ los únicos endomorfismos de V determinados por $A = M(f, B), C = M(h, B)$ (aquí estamos usando el apartado (A) de la Proposición 3.4.4). Entonces,

$$\begin{aligned} \det(A \cdot C) &= \det[M(f, B) \cdot M(h, B)] \overset{(3.9)}{=} \det M(f \circ h, B) = \det(f \circ h) \\ &\overset{(\star)}{=} \det f \cdot \det h = \det A \cdot \det C, \end{aligned}$$

donde en $(\star)$ hemos usado el apartado 2 del Corolario 4.7.5. □

Nota 4.7.5 1. No tiene sentido definir el determinante de una aplicación lineal entre dos espacios vectoriales distintos, aunque tengan la misma dimensión. Esto es así porque dos matrices de una aplicación lineal $f : V \to V'$ en pares de bases ordenadas distintas de V y V' son equivalentes, pero no necesariamente semejantes. Y si $C = P^{-1} \cdot A \cdot Q$ aunque P, Q sean matrices regulares del mismo orden, no tiene porqué set $\det C = \det A$ ya que los determinantes de P y Q no tienen porqué cancelarse.

2. Una consecuencia inmediata de la Proposición 4.7.2 (o también del apartado 2 del Corolario 4.7.6) es que si dos matrices $A, C \in \mathcal{M}_n(\mathbb{K})$ son semejantes, entonces $\det A = \det C$.

4.7.4. Orientación en un espacio vectorial real

Podemos completar la interpretación del tensor determinante en el caso de un espacio vectorial real dando una interpretación relacionada con el signo de (4.26).

Fijemos un espacio vectorial real $V(\mathbb{R})$ con $\dim_{\mathbb{R}} V = n \geq 1$. En el conjunto X formado por todas las bases ordenadas de V, definimos una relación binaria $\sim$:

$$B \sim B' \Leftrightarrow \det M(1_V, B', B) \ (= \det_B(B')) \ > 0, \qquad \forall B, B' \in X.$$

Lema 4.7.2 *La relación* $\sim$ *es de equivalencia en* X *y existen exactamente dos clases de equivalencia.*

Demostración. La propiedad reflexiva se da porque $M(1_V, B, B) = M(1_V, B) = I_n$, que tiene determinante positivo (igual a 1). La simétrica es porque el determinante de $M(1_V, B', B)$ es el inverso del determinante de $M(1_V, B, B')$, luego ambos tienen el mismo signo. La transitiva es porque $M(1_V, B'', B) = M(1_V, B', B) \cdot M(1_V, B'', B')\ \forall B, B', B'' \in X$, y tomando determinantes y aplicando el apartado 2 del Corolario 4.7.6,

$$\det M(1_V, B'', B) = \det M(1_V, B', B) \cdot \det M(1_V, B'', B'); \tag{4.29}$$

finalmente usamos que el producto de dos números positivos es positivo.

Para ver que hay al menos dos clases de equivalencia en X, primero notemos que si $B = (v_1, \ldots, v_n) \in X$ y definimos $B' := (-v_1, v_2, \ldots, v_n)$, entonces $B' \in X$ y $\det M(1_V, B', B) = -1 < 0$. Por tanto, la clase de B es distinta de la clase de B'. Y dada cualquier $B'' \in X$, (4.29) se traduce en que $\det M(1_V, B'', B) = -\det M(1_V, B'', B')$, luego uno de los dos números $\det M(1_V, B'', B)$ o $\det M(1_V, B'', B')$ es positivo, es decir, B'' está en la clase de B o en la de B'. Es decir, sólo hay dos clases de equivalencia en X. □

Definición 4.7.4 Dado un espacio vectorial real $V(\mathbb{R})$ con $\dim_{\mathbb{R}} V = n \geq 1$, a cada una de las dos clases de equivalencia en X obtenidas en el Lema 4.7.2 se le llama una *orientación en* $V(\mathbb{R})$.

En $\mathbb{R}^n(\mathbb{R})$, la base usual produce la *orientación usual.* Para $n \leq 3$, esta orientación se puede interpretar de la siguiente forma:

- $n = 1$. Las bases son escalares distintos de cero; la orientación usual se corresponde con la recta real positiva $\mathbb{R}^+$ y la otra orientación con $\mathbb{R}^-$. Así que una orientación es una eleccción de "derecha" o "izquierda".

- $n = 2$. La orientación usual se corresponde con las bases ordenadas $B = (v_1, v_2)$ que definen un giro en el sentido positivo (opuesto a las agujas del reloj), mientras que las bases ordenadas de la otra orientación definen el "giro en sentido negativo" (el de las agujas del reloj).

- $n = 3$. La orientación usual se corresponde con las bases ordenadas $B = (v_1, v_2, v_3)$ que definen la "regla de la mano derecha" (el sentido de giro de un sacacorchos al abrir una botella), mientras que las bases ordenadas de la otra orientación definen la "regla de la mano izquierda".

4.8. Ejercicios.

1. Demostrar que toda forma lineal $\varphi \in (K^n)^*(\mathbb{K})$ se escribe como $\varphi(x_1, \ldots, x_n) = \sum_{i=1}^n b_i x_i$ para ciertos $b_1, \ldots, b_n \in \mathbb{K}$.

2. Sea $V(\mathbb{R})$ el espacio vectorial de los polinomios de grado ≤ 2. Se consideran las bases ordenadas de V siguientes:

$$B = (1, x, x^2), \qquad B' = (1, 1+x, 1+x+x^2).$$

   Encontrar la matriz de cambio de base de B^* a B'^*. Si $\varphi \in V^*$ está dada por $\varphi(p(x)) = p(-1)\ \forall p(x) \in V$, encontrar las coordenadas de φ en la base ordenada B'^*.

3. Sea traza: $\mathcal{M}_2(\mathbb{R}) \to \mathbb{R}$ la aplicación lineal que le hace corresponder a cada matriz su traza. Encontrar una base $\mathcal{B}'$ de $\mathcal{M}_2(\mathbb{R})^*$ en la que esté esta forma lineal. Encontrar una base $\mathcal{B}$ de $\mathcal{M}_2(\mathbb{R})$ tal que $\mathcal{B}^* = \mathcal{B}'$.

4. En $\mathcal{M}_{2\times 1}(\mathbb{R})$ se considera la base $\{\binom{1}{1}, \binom{2}{3}\}$. Obtener la correspondiente base dual en $\mathcal{M}_{1\times 2}(\mathbb{R})$, identificando con $\mathcal{M}_{1\times 2}(\mathbb{R})$ con $\mathcal{M}_{2\times 1}(\mathbb{R})^*$ de la forma usual.

5. (1) Si $\varphi, \psi \in V^*$, demostrar: $\psi = a\varphi$ para algún $a \in \mathbb{K}$ si y sólo si $\ker(\varphi) \subset \ker(\psi)$.

   (2) Demostrar que las aplicaciones $\varphi, \psi : \mathbb{R}^2 \to \mathbb{R}, \varphi(x, y) = 2x + y, \psi(x, y) = x - 2y$ son formas lineales independientes. Representar gráficamente los núcleos de $\varphi, \psi, 2\varphi$ y $\varphi + \psi$ así como las preimágenes de $1 \in \mathbb{R}$ para cada una de esas formas lineales.

6. Se consideran en $\mathbb{R}^3$ la base ordenada usual B_u y la base ordenada

$$B' = ((0, 1, 1), (1, 0, 1), (-1, -1, 0)).$$

   Hallar las coordenadas de la forma lineal $\varphi(x, y, z) = x + 2z$ en B_u^* y B'^*, y la matriz de cambio de base $M(1_{V^*}, B'^*, B_u^*)$.

7. Se considera en $\mathbb{R}^4(\mathbb{R})$ el subespacio vectorial

$$U = \{(a_1, a_2, a_3, a_4) \in \mathbb{R}^4 \mid a_1 + a_2 - a_3 = 0\}.$$

   Calcular el anulador de U en $\mathbb{R}^4(\mathbb{R})^*$.

8. Se consideran los siguientes subespacios vectoriales de $\mathbb{R}^3$:

$$U = \{(x, y, z) \in \mathbb{R}^3 : x - y + z = 0\}, \qquad W = L(\{(1, 1, 1), (3, 2, 0)\}.$$

   Calcular bases de an(U), an(W), an$(U + W)$ y an$(U \cap W)$.

9. Sean U y W dos subespacios vectoriales de un espacio vectorial $V(\mathbb{K})$. Demostrar que
$$\mathrm{an}(U+W) = \mathrm{an}(U) \cap \mathrm{an}(W), \qquad \mathrm{an}(U \cap W) = \mathrm{an}(U) + \mathrm{an}(W).$$
Deducir que si $V = U \oplus W$, entonces $V^* = \mathrm{an}(U) \oplus \mathrm{an}(W)$.

10. Sea $A \in \mathcal{M}_n(\mathbb{K})$. Demostrar que traza$(A) =$ traza(A^t). Concluir que para cada espacio vectorial $V(\mathbb{K})$ de dimensión finita y cada $f \in \mathrm{End}_{\mathbb{K}}V$, se tiene que traza$(f) =$ traza(f^t).

11. Sean $A, B \in \mathcal{M}_n(\mathbb{K})$. Probar que A y B son semejantes si y sólo si A^t y B^t son semejantes.

12. Para cada matriz $A \in \mathcal{M}_n(\mathbb{K})$ definimos una aplicación $\varphi_A \colon \mathcal{M}_n(\mathbb{K}) \to \mathbb{K}$ mediante $\varphi_A(X) =$ traza(AX), $\forall X \in \mathcal{M}_n(\mathbb{K})$. Demostrar que $\varphi_A \in \mathcal{M}_n(\mathbb{K})^*$. Recíprocamente, probar que para cada forma lineal φ sobre $\mathcal{M}_n(\mathbb{K})$ existe $A \in \mathcal{M}_n(\mathbb{K})$ tal que $\varphi_A = \varphi$.

13. Sean $\varphi, \psi \colon \mathbb{R}^3 \to \mathbb{R}$ dadas por $\varphi(a,b,c) = 2a+b-c$, $\psi(a,b,c) = a+b+c$. Demostrar que φ y ψ son formas lineales sobre $\mathbb{R}^3(\mathbb{R})$ y que $\{\varphi, \psi\}$ es linealmente independiente en $\mathbb{R}^3(\mathbb{R})^*$. Encontrar $\alpha \in \mathbb{R}^3(\mathbb{R})^*$ de modo que $\{\varphi, \psi, \alpha\}$ sea una base de $\mathbb{R}^3(\mathbb{R})^*$. Encontrar también una base de $\mathbb{R}^3(\mathbb{R})$ cuya base dual sea $\{\varphi, \psi, \alpha\}$.

14. Sea $f \in \mathrm{End}_{\mathbb{K}}V$ tal que $f \circ f = f$. Demostrar que su aplicación traspuesta verifica $f^t \circ f^t = f^t$ y que $V^* = \mathrm{an}(\ker(f)) \oplus \mathrm{an}(\mathrm{Im}(f))$.

15. Sea $V(\mathbb{K})$ un espacio vectorial sobre un cuerpo $\mathbb{K}$, V^* su espacio dual y $\mathrm{Aut}_{\mathbb{K}}V$, $\mathrm{Aut}_{\mathbb{K}}V^*$ los grupos de automorfismos de V y V^* respectivamente. Demostrar que la aplicación
$$\mathrm{Aut}_{\mathbb{K}}V \to \mathrm{Aut}_{\mathbb{K}}V^*, \quad f \mapsto (f^t)^{-1},$$
es un isomorfismo de grupos. Como consecuencia, probar que la aplicación
$$Gl(n,\mathbb{K}) \to Gl(n,\mathbb{K}), \quad A \mapsto (A^t)^{-1},$$
es un automorfismo del grupo $Gl(n,\mathbb{K})$.

16. Probar que toda forma lineal $\varphi \in (\mathbb{R}^3)^*$ es de la forma $\varphi(a_1,a_2,a_3) = r_1a_1+r_2a_2+r_3a_3$ donde $r_i = \varphi(e_i) \in \mathbb{R}$, $i = 1,2,3$, y $B_u = (e_1,e_2,e_3)$ es la base ordenada usual. Demostrar también que (r_1,r_2,r_3) son las coordenadas de φ en la base de $(\mathbb{R}^3)^*$ dual de B_u.

17. Sea $B = (\varphi_1,\varphi_2,\varphi_3)$ la base de $(\mathbb{R}^3)^*$ dual de la base usual de $(\mathbb{R}^3)$ y sea f el endomorfismo de $(\mathbb{R}^3)^*$ definido por $f(\varphi_1) = \varphi_1+\varphi_2-\varphi_3$, $f(\varphi_2) = \varphi_1+2\varphi_3$, $f(\varphi_3) = \varphi_1+\varphi_2+\varphi_3$. Calcular el único endomorfismo h de $\mathbb{R}^3$ que cumple $h^t = f$.

18. Sea U un subespacio de un espacio vectorial $V(\mathbb{K})$ con $\dim_{\mathbb{K}} V = n$. Demostrar que si H es una base de an(U), entonces $U = \mathrm{an}(H)$.

19. Sean V, V' espacios vectoriales sobre $\mathbb{K}$, $f\colon V \to V'$ una aplicación lineal y $\varphi \in V^*$. Probar que son equivalentes:

    (A) Existe $\varphi' \in (V')^*$ tal que $\varphi' \circ f = \varphi$.

    (B) $\ker(f) \subset \ker(\varphi)$.

20. Sea V un espacio vectorial complejo. Considerando a V como espacio vectorial real, dotar a Hom$_{\mathbb{R}}(V, \mathbb{C})$ de estructura de espacio vectorial complejo. Probar que

$$\mathrm{Hom}_{\mathbb{R}}(V, \mathbb{C}) = V^* \oplus V',$$

siendo V^* el espacio dual de $V(\mathbb{C})$ y $V' = \{f \in \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{C}) \mid f(ix) = -if(x)\ \forall x \in V\}$.

21. (Examen de Algebra Lineal y Geometría, septiembre de 1994). Sea V un espacio vectorial finitamente generado sobre un cuerpo conmutativo $\mathbb{K}$ y $x \in V \setminus \{0\}$. Encontrar $f \in$ End$_{\mathbb{K}}V$ tal que $f \circ f = f$ y $\ker(f^t) = \mathrm{an}(\{x\})$.