Esta primera edición del manual de Álgebra Lineal que incluye demostraciones, ejemplos y ejercicios fue diseñada como herramienta o material de apoyo para ser implementada en clases de posgrado.

Universidad del Atlántico

Escanée el código QR para conocer más títulos publicados por el Sello Editorial Universidad del Atlántico

ISBN 978-958-5525-41-2

Álgebra lineal

Stiven Díaz - Jorge Rodríguez - Yesneri Zuleta

Manual de Álgebra lineal

Primera edición

Stiven Díaz
Jorge Rodríguez
Yesneri Zuleta

Sello Editorial
UNIVERSIDAD DEL ATLÁNTICO

Manual de Álgebra lineal

Primera edición

Universidad del Atlántico

Manual de Álgebra lineal

Primera edición

Stiven Díaz
Jorge Rodríguez
Yesneri Zuleta

Sello Editorial
UNIVERSIDAD DEL ATLÁNTICO

Catalogación en la publicación. Universidad del Atlántico. Departamento de Bibliotecas
Díaz, Stiven -- Rodríguez, Jorge -- Zuleta, Yesneri.
Algebra lineal / Stiven Díaz, Jorge Rodríguez, Yesneri Zuleta. – 1 edición. – Puerto Colombia, Colombia: Sello Editorial Universidad del Atlántico, 2018.
117 páginas. 21x27 centímetros.
Incluye bibliografía
ISBN 978-958-5525-41-2 (Libro descargable PDF)

1. Algebra lineal 2.Ecuaciones lineales. I. Autor. II. Título.
CDD 512.5 D542

MANUAL DE ÁLGEBRA LINEAL
PRIMERA EDICIÓN
Autoría: Stiven Díaz - Jorge Rodríguez - Yesneri Zuleta

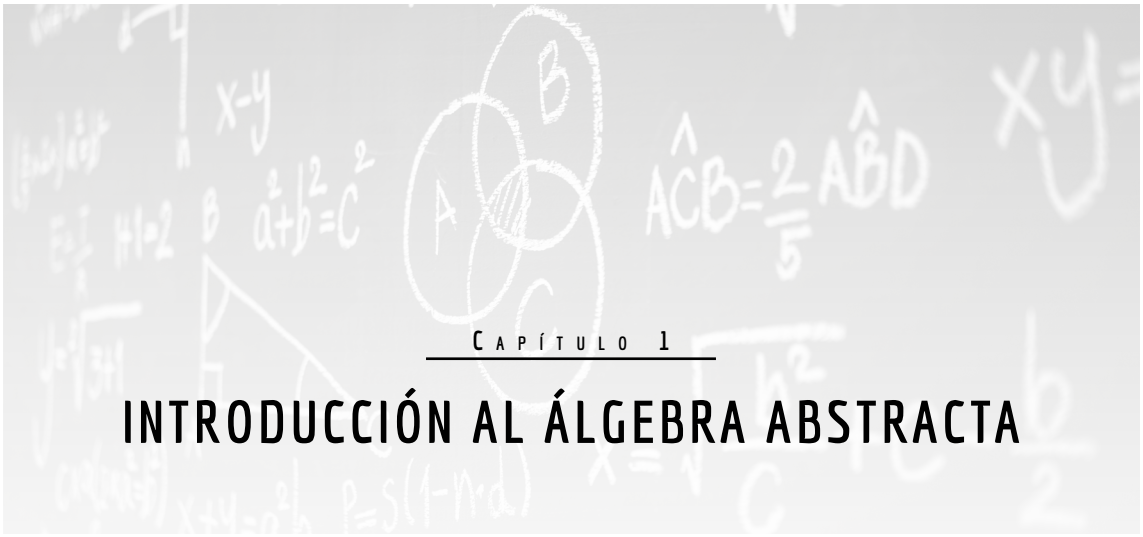
Edición:
Sello Editorial Universidad del Atlántico
Km 7 Vía Puerto Colombia (Atlántico)
www.uniatlantico.edu.co
publicaciones@mail.uniatlantico.edu.co

Producción Editorial:
Calidad Gráfica S.A.
Av. Circunvalar Calle 110 No. 6QSN-522
PBX: 336 8000
lsalcedo@calidadgrafica.com.co
Barranquilla, Colombia

Publicación Electrónica
Barranquilla (Colombia), 2018

Cómo citar este libro:
Díaz, S., Rodríguez Contreras, J & Zuleta, Y. (2018). *Manual de álgebra lineal.* Barranquilla: Sello Editorial Universidad del Atlántico.

CONTENIDO



Capítulo 1

INTRODUCCIÓN AL ÁLGEBRA ABSTRACTA

1.1 Grupos

Definición 1.

Sea $\mathbf{G}$ un conjunto no vacío. Llamaremos a $\mathbf{G}$ un grupo, si los siguientes axiomas se verifican:

$(\mathbf{G}_1)$ Cada $(x, y) \in \mathbf{G} \times \mathbf{G}$ tiene asociado un $z \in \mathbf{G}$. Escribiremos $z = x * y$ y llamaremos a $*$ la operación en $\mathbf{G}$. (Usualmente escribiremos xy en lugar de $x * y$).

$(\mathbf{G}_2)$ $\forall x, y, z \in \mathbf{G}$ se cumple que $x(yz) = (xy)z$.

$(\mathbf{G}_3)$ Existe un elemento $1 \in \mathbf{G}$ tal que $\forall x \in \mathbf{G}$, $frm[o]-- \cdot x = x$.

$(\mathbf{G}_4)$ $(\forall x \in \mathbf{G})(\exists y \in \mathbf{G})$ tal que $yx = 1$.

Definición 2.

Sea $\mathbf{G}$ un conjunto no vacío

(1) Si $\mathbf{G}$ es un grupo y se cumple que $xy = yx \quad \forall x, y \in \mathbf{G}$ diremos que $\mathbf{G}$ es un grupo abeliano o conmutativo.

(2) Si en $\mathbf{G}$ se verifican los axiomas $(\mathbf{G}_1)$ y $(\mathbf{G}_2)$, entonces $\mathbf{G}$ se llamará un semigrupo.

(3) Si $\mathbf{G}$ es un conjunto finito, entonces el número de elementos de $\mathbf{G}$, se llamará orden de $\mathbf{G}$ y lo notaremos con $|\mathbf{G}|$.

1.1.1 Ejemplos.

(1) $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ con la suma son grupos abelianos.

(2) Notemos con $\mathbb{R}^x = \{x \in \mathbb{R} : x \neq 0\}$. Entonces $\mathbb{R}^x$ con la multiplicación es un grupo.

(3) Sea $\Omega \neq \phi$. Definamos $\mathbf{G} = Sym(\Omega) = \{f : \Omega \to \Omega : f \text{ es biyección}\}$ con la composición de funciones es $\mathbf{G}$ un grupo no abeliano.

(a) Sean $f, g \in \mathbf{G}$. Demostremos que $f \circ g \in Sym(\Omega)$:

$\underline{f \circ g}$ **es inyectiva**:

Supongamos que $(f \circ g)(x_1) = (f \circ g)(x_2), \quad x_i \in \Omega$. Entonces $f(g(x_1)) = f(g(x_2)) \quad \Rightarrow \quad g(x_1) = g(x_2) \quad \Rightarrow \quad x_1 = x_2$.

$\underline{f \circ g}$ **es sobreyectiva**:

Sea $y \in \Omega$. Entonces existe $x \in \Omega$ tal que $y = f(x)$. Por otro lado, para este x, existe $w \in \Omega$ tal que $x = g(w)$. Entonces $(f \circ g)(w) = f(g(w)) = f(x) = y$.

(b) Sean $f, g, h \in \mathbf{G}$. Entonces:

$\forall x \in \Omega$ se cumple:

$$\begin{aligned} ((f \circ g) \circ h)(x) &= f(g(h(x))) \\ (f \circ (g \circ h))(x) &= f(g(h(x))) \end{aligned}$$

Entonces se verifica $(\mathbf{G}_2)$.

(c) $1 = I_\Omega$, esto es, $I_\Omega(x) = x \quad \forall x \in \Omega$. Es claro que $I_\Omega \in \mathbf{G}$. Y además $I_\Omega \cdot f = f \quad \forall f \in \mathbf{G}$.

(d) Dado $f \in \mathbf{G}$, siempre existe $f^{-1} : \Omega \to \Omega$ tal que

$$f^{-1}(f(x)) = x = I_\Omega(x) \quad \forall x \in \Omega.$$

Es conocido que también f^{-1} es una biyección, es decir, $f^{-1} \in \mathbf{G}$.

(e) En general $f \circ g \neq g \circ f$ para $f, g \in \mathbf{G}$.

Caso Especial: $\Omega = \{1, 2, \ldots, n\} \subseteq \mathbb{N}$.

Las funciones de $Sym(\Omega)$ las llamaremos permutaciones y escribiremos $Sym(\Omega) = Sym(n) = S_n$. El grupo S_n se llama grupo simétrico sobre n cifras. Note que si $f \in S_n$ se tiene que

$$\{f(1), f(2), \ldots, f(n)\} = \{1, 2, \ldots, n\}.$$

Una representación usual para f es:

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}$$

Por ejemplo: $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ representa la permutación f tal que $f(1) = 2, \quad f(2) = 3$ y $f(3) = 1$.

Observe que $|Sym(n)| = n! = n(n-1)\cdots 1$. Sea $f \in Sym(n)$, digamos

$$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}.$$

Entonces para $f(1)$ se tienen n opciones, en efecto $1, 2, \ldots, n$.
Para $f(2)$ se tienen $n-1$ opciones, los elementos de $\Omega - \{f(1)\}$ y así sucesivamente
Conclusión:

$$|S_n| = \prod_{i=1}^{n}(n-i+1) = n(n-1)\cdots 1 = n!.$$

Si el número de elementos de Ω es mayor o igual a 3, se tiene que S_n no es abeliano.
Sean $w_1, w_2, w_3 \in \Omega$ distintos dos a dos. Definamos $f, g \in Sym(n)$, de la siguiente manera:

$f(w_1) = w_2$	$g(w_1) = w_1$	
$f(w_2) = w_1$	$g(w_2) = w_3$	$f(w) = g(w) = w$
$f(w_3) = w_3$	$g(w_3) = w_2$	$\forall w \in \Omega - \{w_1, w_2, w_3\}$

Entonces tenemos:

$$(fg)(w_1) = f(g(w_1)) = f(w_1) = w_2$$

y

$$(gf)(w_1) = g(f(w_1)) = g(w_2) = w_3.$$

Es decir $f \circ g \neq g \circ f$.

(4) Definamos $\mathbf{G} := \mathbf{G}L(2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, \quad ad - bc = \lambda \right\}$.
Con la multiplicación usual de matrices se cumple que $\mathbf{G}$ es un grupo no abeliano.

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Dada $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{G}$, se verifica que $g^{-1} = \frac{1}{\lambda}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ donde $\lambda = det(g) = ad - bc$.

$$\begin{aligned} g^{-1}g &= \frac{1}{\lambda}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} \\ &= \frac{1}{\lambda}\cdot\lambda\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1. \end{aligned}$$

(5) Sean $a, b \in \mathbb{R}, \quad a \neq 0$. Definamos la función

$$\begin{aligned} T_{a,b} : \mathbb{R} &\to \mathbb{R} \\ x &\to ax + b \end{aligned}$$

Sea ahora $\mathcal{L} := \{T_{a,b} : a, b \in \mathbb{R}, \quad a \neq 0\}$. Con la composición de funciones se demuestra que $\mathcal{L}$ es un grupo no abelinano.

(a) Sean $T_{a,b}, T_{c,d} \in \mathcal{L}, \quad x \in \mathbb{R}$. Entonces

$$\begin{aligned} (T_{a,b} \circ T_{c,d})(x) &= T_{a,b}(T_{c,d}(x)) \\ &= T_{a,b}(cx + d) \\ &= a(cx + d) + b \\ &= (ac)x + (ad + b) \\ &= T_{ac,ad+b}(x). \end{aligned}$$

Es decir $T_{a,b} \circ T_{c,d} = T_{ac,ad+b}(x) \in \mathcal{L}$.

(b) La asociatividad es clara.

(c) $I_{\mathbb{R}} = T_{1,0} = 1$.

(d) Dada $T_{a,b} \in \mathcal{L} \quad , \quad T_{a,b}^{-1} = T_{a^{-1},-ba^{-1}} \in \mathcal{L}$.
Esto demuestra que $(\mathcal{L}, \circ)$ es un grupo.
Es fácil verificar que no es conmutativo.

Teorema 3.

Sea $\mathcal{G}$ un grupo, con módulo 1.

(1) $\forall x \in \mathbf{G}$ se cumple $x \cdot 1 = x$.

(2) Sean $x, y \in \mathbf{G}$. Si $yx = 1$, entonces $xy = 1$.

(3) Existe un único $1 \in \mathcal{G}$ que satisface (1)($\mathbf{G}_3$).

(4) $\forall x \in \mathbf{G}, \quad \exists! y \in \mathcal{G}$ tal que $yx = 1$. Llamaremos a y el inverso de x y los notaremos con x^{-1}. (Si $\mathbf{G}$ se escribe aditivamente, escribiremos $-x$).

(5) $\forall x \in \mathbf{G} \qquad (x^{-1})^{-1} = x$.

(6) $\forall x, y \in \mathbf{G} \qquad (xy)^{-1} = y^{-1}x^{-1}$.

DEMOSTRACIÓN.

(1) y (2) De la definición 1 ($\mathbf{G}_3$) se sigue que existen $y, z \in \mathbf{G}$ tales que

$$yx = 1 \qquad \wedge \qquad zy = 1.$$

con esto se sigue: $z \cdot 1 = z(yx) = (zy)x = 1 \cdot x = x$.
Entonces: $x = z \cdot 1 = z(1 \cdot 1) = (z \cdot 1) \cdot 1 = x \cdot 1$. Esto demuestra (1). Además se cumple:

$$x = z \cdot 1 = z \quad \Rightarrow \quad 1 = zy = xy.$$

(3) Supongamos que $e \in \mathbf{G}$ es también un módulo. Entonces $x = ex \quad \forall x \in \mathbf{G}$, en particular $1 = \underbrace{e \cdot 1 = e}_{(1)}$.

(4) Sea $x \in \mathbf{G}$ y supongamos que existen $y, z \in \mathbf{G}$ tales que

$$yx = zx = 1.$$

Entonces

$$y = 1 \cdot y = (zx)y = z(xy) = z \cdot 1 = z.$$

(5) De la definición de x^{-1} se sigue que $x^{-1}x = 1 \quad \forall x \in \mathbf{G}$. De (2) se tiene que $xx^{-1} = 1$, esto es, x es el inverso de x^{-1}, por lo tanto $x = (x^{-1})^{-1}$.

(6) Sean $x, y \in \mathbf{G}$. Entonces

$$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}y = 1.$$

De (5) se sigue que $y^{-1}x^{-1} = (xy)^{-1}$.

Teorema 4.

(Leyes de cancelación) Sea $\mathbf{G}$ un grupo, $a, x, y \in \mathbf{G}$.

(1) Si $ax = ay$, entonces $x = y$.

(2) Si $xa = ya$, entonces $x = y$.

DEMOSTRACIÓN.

(1) $x = 1 \cdot x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = 1 \cdot y = y$.

(2) Se demuestra de manera análoga al inciso (1).

Teorema 5.

Sea $\mathbf{G}$ un grupo, $a, x, b \in \mathbf{G}$. Las ecuaciones $ax = b$ y $ya = b$ tienen soluciones únicas en $\mathbf{G}$.

DEMOSTRACIÓN. En efecto

(1) Consideremos la ecuación $ax = b$.

(i) Existencia de la solución: $a^{-1}b$. En efecto, $a(a^{-1}b) = (aa^{-1})b = 1 \cdot b = b$.

(ii) Unicidad de la solución: Supongamos que existen x_1, x_2 que la satisfacen. Entonces, $ax_1 = b = ax_2 \quad \Rightarrow \quad ax_1 = ax_2$, luego por el teorema (4) $x_1 = x_2$.

(2) Se deja como ejercicio para el lector.

Definición 6.

Sea $\mathbf{G}$ un grupo, $g \in \mathbf{G}$. Definimos g^n para $n \in \mathbb{Z}$, de la siguiente manera:

$$\begin{aligned} g^0 &:= 1 \\ g^{n+1} &:= g^n \cdot g. \quad para \quad n \geq 0 \end{aligned}$$

$$g^n := (g^{-n})^{-1} \quad para \quad n < 0.$$

Teorema 7.

Sea $g \in \mathbf{G}$. $\mathbf{G}$ es un grupo. Para $n, m \in \mathbb{Z}$ se cumple:

1. $g^n \cdot g^m = g^{n+m} = g^m \cdot g^n$.
2. $(g^n)^m = g^{nm}$.

DEMOSTRACIÓN.

1.(a) Demostremos por inducción que si $n, m \geq 0$, entonces

$$g^n \cdot g^m = g^{n+m}$$

- Si $m = 0$, tenemos: $g^n \cdot g^0 = g^n \cdot 1 = g^n = g^{n+0}$.

- Supongamos ahora que para $m \geq 0$ la afirmación se cumple. Entonces se sigue:

$$g^n g^{m+1} = g^n(g^m \cdot g) = (g^n \cdot g^m)g = g^{n+m} \cdot g = g^{n+(m+1)}.$$

(b) Demostremos ahora que si $k > 0$, entonces se cumple que

$$g^{-k}g = g^{-k+1}$$

Si utilizamos (a) se tiene $g^k = gg^{k-1}$ ya que $k - 1 \geq 0$. Entonces:

$$g^{-k} = (g^k)^{-1} = (gg^{k-1})^{-1} = (g^{k-1})^{-1}g^{-1} = g^{-(k-1)}g^{-1} = g^{-k+1}g^{-1}.$$

Multiplicando a la derecha por g tenemos:

$$g^{-k}g = g^{-k+1}.$$

(c) Por la parte (b) y por la definición se cumple que

$$g^{n+m} \cdot g = g^{n+m+1} \qquad \forall n, m \in \mathbb{Z}.$$

En efecto, para $n + m \geq 0$ se tiene la definición y para $n + m < 0$ se tiene en (b).
Como en (a), se demuestra por inducción sobre m que $g^n \cdot g^m = g^{n+m}$ $\forall n \in \mathbb{Z}$ y $\forall m \geq 0$.

(d) Para completar la prueba de 1), falta demostrar que

$$g^n \cdot g^{-m} = g^{n-m} \qquad \forall n \in \mathbb{Z} \text{ y } \forall m > 0.$$

Se cumple que: $g^{n-m)}g^m = g^{n-m+m} = g^n$. Entonces

$$g^{n-m)} = g^n(g^m)^{-1} = g^n \cdot g^{-m}.$$

(Hemos multiplicado por $(g^m)^{-1}$).

2.(a) Por definición se sigue que

$$g^{-n} = (g^n)^{-1} \qquad \forall n \geq 0.$$

Sea $n < 0$. Entonces

$$(g^n)^{-1}g = ((g^{-n})^{-1})^{-1} = g^{-n}.$$

Es decir $(g^n)^{-1} = g^{-n} \quad \forall n \in \mathbb{Z}$.

(b) Demostremos ahora que $(g^n)^m = g^{nm} \quad \forall m \geq 0$ y para cualquier n. (Inducción sobre m)
- $m = 0$, entonces

$$(g^n)^0 = 1 = g^0 = g^{n\cdot 0}$$

- Supongamos que ya está demostrada la afirmación para m, entonces

$$(g^n)^{m+1} = (g^n)^m \cdot g^n = g^{nm}g^n = g^{nm+n} = g^{n(m+1)}.$$

(c) Sea $m \geq 0$, entonces

$$(g^n)^{-m} = ((g^n)^m)^{-1} = (g^{nm})^{-1} = g^{-nm}.$$

Lema 8.

Sea $\mathbf{G}$ un grupo, $g \in \mathbf{G}$. El conjunto $\mathcal{U} := \{g^n : n \in \mathbb{Z}\}$ es un grupo con la operación definida sobre $\mathbf{G}$.

DEMOSTRACIÓN. Ejercicio.

1.2 Subgrupos

Definición 9.

Sea $\mathbf{G}$ un grupo y $\phi \neq \mathcal{U} \subseteq \mathbf{G}$. Llamaremos a $\mathcal{U}$ un subgrupo de $\mathbf{G}$, si se cumple el siguiente criterio:

$$\forall x, y \in \mathcal{U} \quad : \quad xy^{-1} \in \mathcal{U}.$$

Nota: Dado que $\mathcal{U} \neq \phi$, existe por lo menos un $u \in \mathcal{U}$. Entonces por la definición de subgrupo se tiene que

$$uu^{-1} = 1 \in \mathcal{U}.$$

Se puede verificar fácilmente que si $\mathcal{U}$ es un subgrupo de $\mathbf{G}$, entonces $\mathcal{U}$ con la restricción de la operación de $\mathbf{G}$ es en sí un grupo. (Verifíquelo!)

Usaremos la notación $\mathcal{U} \leqslant \mathbf{G}$ para indicar que $\mathcal{U}$ es un subgrupo de $\mathbf{G}$. Si $\mathcal{U}$ es un subconjunto propio de $\mathbf{G}$ escribiremos $\mathcal{U} < \mathbf{G}$.

1.2.1 Ejemplos.

1. Sea $\mathbf{G}$ un grupo, entonces $\mathbf{G} \leqslant \mathbf{G}$ y $\{1\} \leqslant \mathbf{G}$. Estos subgrupos los denominaremos subgrupos triviales de $\mathbf{G}$.
2. $\mathbb{Z}$ con la suma es un grupo. Sean $n \in \mathbb{Z}$, definamos

   $$n\mathbb{Z} := \{nk : k \in \mathbb{Z}\}$$

   Se verifica que $n\mathbb{Z} \leqslant \mathbb{Z}$.

   (a) Evidentemente $n\mathbb{Z} \neq \phi$: $\quad n = n \cdot 1 \in n\mathbb{Z}$.

   (b) Sean $nk_1, \quad nk_2 \in n\mathbb{Z}$, entonces

$$nk_1 + (-nk_2) = n(k_1 - k_2) \in n\mathbb{Z}.$$

3. Sea $\Omega = \{1, 2, 3\}$ y $\mathbf{G} = S_3 = Sym(3)$. Entonces $\mathcal{U} = \{(1), (123), (132)\}$ es un subgrupo de $\mathbf{G}$.

4. Sea $\mathbf{G} = \mathbf{G}L(2, \mathbb{R})$

$$\mathcal{U} := \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a, b, c \in \mathbb{R} \quad , \quad ac \neq 0 \right\}$$

Del ejemplo (1.1.1)(4) sabemos que dado $u \in \mathcal{U}$, digamos

$$\mathcal{U} = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$$

Se cumple que

$$\mathcal{U}^{-1} = \frac{1}{det(\mathcal{U})} \begin{pmatrix} c & 0 \\ -b & a \end{pmatrix} \in \mathcal{U}$$

Es claro que la multiplicación es cerrada en $\mathcal{U}$.

5. Sea nuevamente $\mathbf{G} = \mathbf{G}L(2, \mathbb{R})$

$$\mathcal{U} := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \quad ; \quad ab - cd = 1 \right\}$$

Se demuestra que $\mathcal{U} \leqslant \mathbf{G}$.

Teorema 10.

1. Sea I un conjunto de índices, $\{\mathcal{U}_i\}_{i \in I}$ sea una familia de subgrupos de un grupo $\mathbf{G}$. Entonces $D := \bigcap_{i \in I} \mathcal{U}_i \leqslant \mathbf{G}$.

2. Sean $\mathcal{U}, \mathcal{V} \leqslant \mathbf{G}$.

$$(\mathcal{U} \cup \mathcal{V}) \leqslant \mathbf{G} \quad \Leftrightarrow \quad \mathcal{U} \subseteq \mathcal{V} \quad \vee \quad \mathcal{V} \subseteq \mathcal{U}.$$

DEMOSTRACIÓN.

1. Dado que $1 \in \mathcal{U}_i \quad \forall i \in I$, se tiene que $1 \in D$ y por lo tanto $D \neq \phi$.
Sean $x, y \in D$. entonces $x, y \in \mathcal{U}_i \quad \forall i \in I$, es decir $xy^{-1} \in \mathcal{U}_i \quad \forall i \in I$, lo cual demuestra que $xy^{-1} \in D$.

2. Note que

Si $\mathcal{U} \subseteq \mathcal{V}$, entonces $\mathcal{U} \cup \mathcal{V} = \mathcal{V} \leqslant \mathbf{G}$
Si $\mathcal{V} \subseteq \mathcal{U}$, entonces $\mathcal{U} \cup \mathcal{V} = \mathcal{U} \leqslant \mathbf{G}$.

Recíprocamente, supongamos que $(\mathcal{U} \cup \mathcal{V}) \leqslant \mathbf{G}$ pero $\mathcal{U} \nsubseteq \mathcal{V} \quad \wedge \quad \mathcal{V} \nsubseteq \mathcal{U}$. Entonces existen $u \in \mathcal{U} - \mathcal{V}$ y $v \in \mathcal{V} - \mathcal{U}$. Dado que $u, v \in \mathcal{U} \cup \mathcal{V}$ y $(\mathcal{U} \cup \mathcal{V}) \leqslant \mathbf{G}$ se tiene que $uv^{-1} \in (\mathcal{U} \cup \mathcal{V})$. Entonces $uv^{-1} \in \mathcal{U} \quad \vee \quad uv^{-1} \in \mathcal{V}$. Sin perder generalidad supongamos que $uv^{-1} \in \mathcal{U}$, entonces existe $x \in \mathcal{U}$ tal que

$$uv^{-1} = x \quad \Rightarrow \quad v = x^{-1}u \in \mathcal{U}. \quad \text{(absurdo)}$$

Entonces nuestro supuesto es falso.

1.2.2 Observación.
En general no se cumple que $\mathcal{U} \cup \mathcal{V} \leqslant \mathbf{G}$ cuando $\mathcal{U} \leqslant \mathbf{G},\ \mathcal{V} \leqslant \mathbf{G}$.

1.2.3 Ejemplo. $\mathcal{U} = 2\mathbb{Z},\ \mathcal{V} = 3\mathbb{Z}\, \mathcal{U} \cup \mathcal{V} \nleqslant \mathbb{Z}$. Luego $2 + 3 = 5 \notin (\mathcal{U} \cup \mathcal{V})$.

Definición 11.

Sea $\mathbf{G}$ un grupo y $\mathcal{M} \subseteq \mathbf{G}$. Definimos

$$\langle \mathcal{M} \rangle := \bigcap_{\mathcal{M} \subseteq \mathcal{U} \leqslant \mathbf{G}} \mathcal{U}$$

Y lo llamaremos el subgrupo generado por $\mathcal{M}$.

Lema 12.

Sea $\mathbf{G}$ un grupo, $\mathcal{U} \leqslant \mathbf{G}$. Para $g, h \in \mathbf{G}$, definamos sobre $\mathbf{G}$ la siguiente relación

$$g \backsim_{\mathcal{U}} h \quad \Leftrightarrow \quad g^{-1}h \in \mathcal{U}.$$

(O equivalentemente $g \backsim_{\mathcal{U}} h \quad \Leftrightarrow \quad h \in g\mathcal{U}$).
Entonces $\backsim_{\mathcal{U}}$ es una relación de equivalencia.

DEMOSTRACIÓN.

1. Dado que $g^{-1} \cdot g = 1 \in \mathcal{U}$, se tiene que $g \backsim_{\mathcal{U}} g$.
2. Supongamos que $g \backsim_{\mathcal{U}} h$. Entonces $g^{-1}h \in \mathcal{U}$, es decir, existe $u \in \mathcal{U}$ tal que $g^{-1}h = u$ entonces $h^{-1}g = u^{-1} \in \mathcal{U}$. Por lo tanto $h \backsim_{\mathcal{U}} g$.
3. Supongamos que $g \backsim_{\mathcal{U}} h \quad \wedge \quad h \backsim_{\mathcal{U}} k$. Entonces $g^{-1}h \in \mathcal{U} \quad \wedge \quad h^{-1}k \in \mathcal{U} \quad \Rightarrow \quad (g^{-1}h)(h^{-1}k) \in \mathcal{U} \quad \Rightarrow \quad g^{-1}k \in \mathcal{U} \quad \Rightarrow \quad g \backsim_{\mathcal{U}} k$.
   Entonces $\backsim_{\mathcal{U}}$ es una relación de equivalencia sobre $\mathbf{G}$.

Las correspondientes clases de equivalencias son:

$$\begin{aligned} [g] &= \{h \in \mathcal{U} : h \backsim_{\mathcal{U}} g\} \\ &= \{h \in \mathcal{U} : g^{-1}h \in \mathcal{U}\} \\ &= \{h \in \mathcal{U} : h \in g\mathcal{U}\} \\ &= g\mathcal{U}. \end{aligned}$$

Dado que $\backsim_{\mathcal{U}}$ induce una partición sobre $\mathbf{G}$, se tiene entonces que

$$\mathbf{G} = \bigcup_{g \in \mathbf{G}} [g] = \bigcup_{g \in \mathbf{G}} g\mathcal{U}$$

y además

$$g\mathcal{U} \cap h\mathcal{U} = \begin{cases} \phi & \text{si } h \notin g\mathcal{U} \\ g\mathcal{U} & \text{si } h \in g\mathcal{U} \end{cases}.$$

Si elegimos de cada clase lateral $g\mathcal{U}$ exactamente un elemento y formamos con estos elementos un conjunto L, se tiene entonces que

$$\mathbf{G} = \biguplus_{g\in L} g\mathcal{U} \qquad \text{(Unión disjunta).}$$

Definición 13.

1. La descomposición $\mathbf{G} = \biguplus_{g\in L} g\mathcal{U}$ se llama descomposición en clases laterales de $\mathbf{G}$ con respecto a $\mathcal{U}$. L es denominado un transversal izquierdo de $\mathcal{U}$ en $\mathbf{G}$.
2. Si L es finito, entonces llamaremos a $|L|$ el indice de $\mathcal{U}$ en $\mathbf{G}$ y lo notaremos con $|\mathbf{G} : \mathcal{U}|$.
   Evidentemente $|\mathbf{G} : \mathcal{U}|$ es el número de clases laterales izquierdas de $\mathcal{U}$ en $\mathbf{G}$.

1.2.4 Ejemplo. Sea $\mathbf{G} = S_3 = \{(1), (12), (13), (23), (123), (132)\}$.
Sea $\mathcal{U} = \{(1), (13)\}$, claramente $\mathcal{U} \leqslant \mathbf{G}$. Se puede mostrar que

$$(12)\mathcal{U} = \{(12), (132)\}$$
$$(23)\mathcal{U} = \{(23), (123)\}$$

Entonces para $\mathbf{G}$ se tiene la siguiente descomposición en clases laterales con respecto a $\mathcal{U}$:

$$\mathbf{G} = \mathcal{U} \uplus (12)\,\mathcal{U} \uplus (23)\,\mathcal{U}$$

Es decir $L = \{(1), (12), (23)\}$ es un transversal izquierdo de $\mathcal{U}$ en $\mathbf{G}$.

Teorema 14.

(Lagrange, 1736-1813). Sea $\mathbf{G}$ un grupo finito, $\mathcal{U} \leqslant \mathbf{G}$. Entonces $|\mathbf{G}| = |\mathbf{G} : \mathcal{U}||\mathcal{U}|$. En particular $|\mathcal{U}|$ y $|\mathbf{G} : \mathcal{U}|$ dividen el orden de $\mathbf{G}$.

DEMOSTRACIÓN. Sea L un transversal izquierdo de $\mathcal{U}$ en $\mathbf{G}$, entonces tenemos

$$\mathbf{G} = \biguplus_{g\in L} g\mathcal{U}.$$

Y se tiene entonces:

$$|\mathbf{G}| = \sum_{g\in L} |g\mathcal{U}|.$$

Demostremos que $|g\mathcal{U}| = |\mathcal{U}|$:

Consideremos la función $\varphi_g : \mathcal{U} \to g\mathcal{U}$ definida por $\varphi_g(u) = gu$.

φ **es uno a uno:** Si $\varphi_g(u_1) = \varphi_g(u_2)$, entonces $g(u_1) = g(u_2)$ luego $u_1 = u_2$.

φ**es sobre:** Sea $y \in g\mathcal{U}$. Entonces existe $u \in \mathcal{U}$ tal que

$$y = gu = \varphi_g(u).$$

Es decir φ_g es una biyección para todo $g \in L$. Por lo tanto $|g\mathcal{U}| = |\mathcal{U}|$.
Conclusión:

$$|\mathbf{G}| = \sum_{g\in L} |\mathcal{U}| = |L||\mathcal{U}| = |\mathbf{G} : \mathcal{U}||\mathcal{U}|.$$

1.2.5 Corolario. Sea $\mathbf{G}$ un grupo y $|\mathbf{G}| = p, \quad p$ un primo, sea $g \neq 1 \quad \wedge \quad g \in \mathbf{G}$, entonces $\mathbf{G} = \langle g \rangle$.

DEMOSTRACIÓN.
Dado que $g \neq 1$, se tiene que $1, g \in \langle g \rangle$ entonces $|\langle g \rangle| > 1$. por el teorema (14) se tiene $|\langle g \rangle|/p$ luego $|\langle g \rangle| = p = |\mathbf{G}| \quad \Rightarrow \mathbf{G} = \langle g \rangle$.
$\underline{\mathcal{U} \leqslant \mathbf{G}}$: Sean $u, v \in \mathcal{U}$, entonces

$$u = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$$
$$v = x_1^{\alpha_1} \cdots x_m^{\alpha_m}$$

$x_i \in \mathcal{M}, \quad \varepsilon_i, \alpha_i \in F, \quad n, m \in \mathbb{N}$.

Se sigue
$uv^{-1} = (x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n})(x_1^{\alpha_1} \cdots x_m^{\alpha_m})^{-1} = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} x_m^{-\alpha_m} \cdots x_1^{-\alpha_1} \in \mathcal{U}$ entonces

$u \leqslant v$.

Nota: Otra carecterización usual para $\langle \mathcal{M} \rangle$ es la siguiente:

$$\langle \mathcal{M} \rangle = \{x_1 \cdots x_n : n \in \mathbb{N}, \quad x_i \in \mathcal{M} \quad \vee \quad x_i^{-1} \in \mathcal{M}\}$$

DEMOSTRACIÓN. Ejercicio para el lector

Definición 15.

Sea $\mathbf{G}$ un grupo, $\mathcal{U} \leqslant \mathbf{G}, \quad g \in \mathbf{G}$. Definimos $g\mathcal{U} := \{gx : x \in \mathcal{U}\}$ y llamaremos a $g\mathcal{U}$ la clase lateral izquierda de g con respecto $\mathcal{U}$. Correspondientemnte se define $\mathcal{U}g := \{xg : x \in \mathcal{U}\}$ la clase lateral derecha de g con respecto $\mathcal{U}$.

Nota: $g\mathcal{U} = \mathcal{U} \quad \Leftrightarrow \quad g \in \mathcal{U}$.

DEMOSTRACIÓN. Supongamos que $g\mathcal{U} = \mathcal{U}$. Dado que $1 \in \mathcal{U}$ se tiene que $g = g \cdot 1 \in \mathcal{U}$.

Reciprocarme. Sea $g \in \mathcal{U}$, claramente $g\mathcal{U} \subseteq \mathcal{U}$.
Sea ahora $u \in \mathcal{U}$, entonces $u = (gg^{-1})u = g\underbrace{(g^{-1}u)}_{\in \mathcal{U}} \in g\mathcal{U}$, es decir $\mathcal{U} \subseteq g\mathcal{U}$.
Del teorema (10)(1) se sigue que $\mathcal{M} \subseteq \langle \mathcal{M} \rangle \leqslant \mathbf{G}$.
Sea ahora $\mathcal{V} \leqslant \mathbf{G}$ tal que $\mathcal{M} \subseteq \mathcal{V}$. Entonces por la definición de $\langle \mathcal{M} \rangle$ se cumple $\langle \mathcal{M} \rangle \subseteq \mathcal{V}$, es decir $\langle \mathcal{M} \rangle$ es el subgrupo de $\mathbf{G}$ más pequeño que contiene a $\mathcal{M}$.
Nota: Si $\mathcal{M} = \{g\}$, escribiremos $\langle g \rangle$ en lugar de $\langle \{g\} \rangle$.

Teorema 16.

Sea $\mathbf{G}$ un grupo y $\mathcal{M} \subseteq \mathbf{G}$.

1. Si $\mathcal{M} = \phi$, entonces $\langle \mathcal{M} \rangle = \{1\}$.
2. Si $\mathcal{M} = \phi$, entonces $\langle \mathcal{M} \rangle = \{x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} : n \in \mathbb{N}, \quad x_i \in \mathcal{M}, \quad \varepsilon_i \in \mathbb{Z}\}$.

DEMOSTRACIÓN.

1. Evidente.
2. Definamos $\mathcal{U} := \{x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} : n \in \mathbb{N}, \quad x_i \in \mathcal{M}, \quad \varepsilon_i \in \mathbb{Z}\}$.

   Objetivo: Demostrar que $\langle \mathcal{M} \rangle = \mathcal{U}$.

   (a) $\mathcal{U} \subseteq \langle \mathcal{M} \rangle$: Sea $u \in \mathcal{U}$, entonces $u = x_1^{\varepsilon_1} \cdots x_m^{\varepsilon_m}$ donde $m \in \mathbb{N}, \quad x_i \in \mathcal{M}, \quad \varepsilon_i \in \mathbb{Z}$. Cada $x_i^{\varepsilon_i} \in \langle \mathcal{M} \rangle$.
   Dado que $\langle \mathcal{M} \rangle$ es un subgrupo de $\mathbf{G}$ y por tanto cerrado, se tiene que $u \in \langle \mathcal{M} \rangle$.

   (b) Demostremos ahora que $\mathcal{M} \subseteq \mathcal{U} \leqslant \mathbf{G}$. Esto trae como consecuencia que $\langle \mathcal{M} \rangle \subseteq \mathcal{U}$.

   $\mathcal{M} \subseteq \mathcal{U}$: Sea $x \in \mathcal{M}$, entonces $x = x^1 \in \mathcal{U}$.

Definición 17.

Sea $\mathbf{G}$ un grupo, $\mathcal{M}, \mathcal{V} \leqslant \mathbf{G}$. Definimos

$$\begin{aligned} \mathcal{UV} :&= \{uv : u \in \mathcal{U}, \quad v \in \mathcal{V}\} \\ \mathcal{U}^{-1} :&= \{u^{-1} : u \in \mathcal{U}\} \end{aligned}$$

Teorema 18.

Sean $\mathcal{U}, \mathcal{V} \leqslant \mathbf{G}$.

1. $\mathcal{U}^{-1} = \mathcal{U}$.
2. $\mathcal{UV} \leqslant \mathbf{G} \quad \Leftrightarrow \quad \mathcal{UV} = \mathcal{VU}$.

DEMOSTRACIÓN.

1. Demostremos que $\mathcal{U} \subseteq \mathcal{U}^{-1}$ y $\mathcal{U}^{-1} \subseteq \mathcal{U}$.
   Sea $u \in \mathcal{U}$, entonces $u = (u^{-1})^{-1} \in \mathcal{U}^{-1}$. Sea $u^{-1} \in \mathcal{U}^{-1}$, entonces, dado que $u \in \mathcal{U}$ y $\mathcal{U} \leqslant \mathbf{G}$ se tiene que $u^{-1} \in \mathcal{U}$.
2. Supongamos que $\mathcal{UV} \leqslant \mathbf{G}$, entonces $(\mathcal{UV})^{-1} = \mathcal{UV}$, pero $(\mathcal{UV})^{-1} = \mathcal{V}^{-1}\mathcal{U}^{-1} = \mathcal{VU} \quad \Rightarrow \quad \mathcal{UV} = \mathcal{VU}$.
   Sea ahora $\mathcal{UV} = \mathcal{VU}$. Demostremos que $\mathcal{UV} \leqslant \mathbf{G}$.
   Sean $u_1v_1, u_2v_2 \in \mathcal{UV}$. Entonces

$$(u_1v_1)(u_2v_2)^{-1} = (u_1v_1)(v_2^{-1}u_2^{-1}) = u_1 \underbrace{(v_1v_2^{-1})u_2^{-1}}_{\in \mathcal{V}\mathcal{U}=\mathcal{U}\mathcal{V}} = u_1uv \in \mathcal{U}\mathcal{V}$$

Entonces $uv \leqslant \mathbf{G}$.

Teorema 19.

Sean $\mathcal{U}\mathcal{V} \leqslant \mathbf{G}$, entonces $\mathcal{U}, \mathcal{V}$ finitos.

$$|\mathcal{U}\mathcal{V}| = \frac{|\mathcal{U}||\mathcal{V}|}{|\mathcal{U} \cap \mathcal{V}|}$$

DEMOSTRACIÓN. Sea T un transversal izquierdo de $\mathcal{U} \cap \mathcal{V}$ en $\mathcal{U}$, esto es

$$\mathcal{U} = \biguplus_{t \in T} t(\mathcal{U} \cap \mathcal{V}). \tag{1.1}$$

Entonces

$$\mathcal{U}\mathcal{V} = \biguplus_{t \in T} t\mathcal{V}. \tag{1.2}$$

1. $\biguplus_{t \in T} t\mathcal{V} \subseteq \mathcal{U}\mathcal{V}$: se sigue del hecho de que $T \subseteq \mathcal{U}$.
2. $\mathcal{U}\mathcal{V} \subseteq \biguplus_{t \in T} t\mathcal{V}$:

Sea $uv \in \mathcal{U}\mathcal{V}$, donde $u \in \mathcal{U}, \quad v \in \mathcal{V}$. De (1.1) se sigue que existen $t \in T$ y $w \in (\mathcal{U} \cap \mathcal{V})$ tal que $u = tw$, entonces

$$uv = (tw)v = t(wv) \in t\mathcal{V} \subseteq \biguplus_{t \in T} t\mathcal{V}.$$

Hemos demostrado entonces $\mathcal{U}\mathcal{V} = \biguplus_{t \in T} t\mathcal{V}$.

Demostremos ahora que esta intersección es disyunta. Supongamos que $t_1v_1 = t_2v_2 \in t_1\mathcal{V} \cap t_2\mathcal{V}$, donde $t_i \in T, \quad v_i \in \mathcal{V}$. Entonces

$$t_2^{-1}t_1 = v_2v_1^{-1} \in (\mathcal{U} \cap \mathcal{V}) \qquad \text{(recordemos que } T \subseteq \mathcal{U})$$

Es decir

$$\begin{aligned} t_2^{-1}t_1(\mathcal{U} \cap \mathcal{V}) &= (\mathcal{U} \cap \mathcal{V}) \\ t_1(\mathcal{U} \cap \mathcal{V}) &= t_2(\mathcal{U} \cap \mathcal{V}) \end{aligned}$$

Dado que T es un transversal se tiene que $t_1 = t_2$. Esto demuestra que la Unión es disyunta.
Se sigue además

$$|t\mathcal{V}| = |\mathcal{V}|.$$

Entonces

$$|\mathcal{U}\mathcal{V}| = |T||\mathcal{V}| = |\mathcal{U} : \mathcal{U} \cap \mathcal{V}||\mathcal{V}| = \frac{|\mathcal{U}||\mathcal{V}|}{|\mathcal{U} \cap \mathcal{V}|}$$

Definición 20.

1. Un grupo $\mathbf{G}$ se llama cíclico, si existe $g \in \mathbf{G}$ tal que $\mathbf{G} = \langle g \rangle$. Del teorema (16)(2) se sigue que $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$.
2. Sea $g \in \mathbf{G}$. El número natural n más pequeño para el cual $g^n = 1$ se denomina orden g y lo notaremos con $o(g)$, si tal número existe. si no existe escribimos $o(g) = \infty$.

1.2.6 Ejemplos.

1. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle, \qquad o(1) = o(-1) = \infty.$
2. $\mathbf{G} = \{-1, 1\} \subseteq \mathbb{R}$ con multiplicación $\mathbf{G} = \langle -1 \rangle, \quad o(-1) = 2$

Teorema 21.

Sea $\mathbf{G}$ un grupo, $g \in \mathbf{G}, \quad \mathbf{G} = \langle g \rangle$ y $o(g) = n$.

1. Si $g^m = 1$, entonces $n|m \quad (m \in \mathbb{Z})$.
2. $\mathbf{G} = \{1, g, ..., g^{n-1}\}$ y $|\mathbf{G}| = o(g)$.

DEMOSTRACIÓN.

1. Por el algoritmo de la división $m = nr + s, \quad 0 \leq s < n, \quad r \in \mathbb{Z}$. Entonces

$$1 = g^m = g^{nr+s} = \underbrace{g^{nr}}_{=1} \cdot g^s = 1 \cdot g^s = g^s$$

   por la elección de n, se tiene entonces que $s = 0$ luego $n|m$.

2. Definamos $\mathcal{U} := \{1, g, ..., g^{n-1}\}$. Es claro que $\mathcal{U} \subseteq \mathbf{G}$. Sea ahora $g^k \in \langle g \rangle$ y $k = nr + s, \quad 0 \leq s < n$, entonces

$$g^k = g^{nr+s} = g^{nr} \cdot g^s = g^s \in \mathcal{U}, \quad \Rightarrow \quad \langle g \rangle \subseteq \mathbf{G}.$$

   Supongamos $g^i = g^j$ con $0 \leq i \leq j < n$. Entonces $g^{j-i} = 1$, de la parte (1) se sigue que $n|(j-i)$ entonces $j - i = 0 \quad \Rightarrow \quad j = i$. Entonces $|\mathcal{U}| = n = o(g)$.

1.3 Homomorfismos

Definición 22.

Sean $\mathbf{G}$ y $\mathbf{H}$ dos grupos.

1. Una función $\varphi : \mathbf{G} \to \mathbf{H}$ se llama un homomorfismo (de grupos) si y solo si, para todo $x, y \in \mathbf{G}$ se cumple que

$$\varphi(xy) = \varphi(x) \cdot \varphi(y)$$

   El conjunto de todos los homomorfismos de $\mathbf{G}$ en $\mathbf{H}$ lo notaremos como $Hom(\mathbf{G}, \mathbf{H})$.

2. Sea $\varphi \in Hom(\mathbf{G}, \mathbf{H})$.
   (a) Si φ es sobreyectiva, entonces llamaremos a φ un Epimorfismo.
   (b) Si φ es inyectiva, entonces llamaremos a φ un Monomorfismo.
   (c) Si φ es biyectiva, entonces llamaremos a φ un Isomorfismo.
   (d) Si $\varphi : \mathbf{G} \to \mathbf{H}$ es un isomorfismo, entonces diremos que $\mathbf{G}$ y $\mathbf{H}$ son isomorfos y escribiremos $\mathbf{G} \cong \mathbf{H}$.
   (e) Si $\varphi \in Hom(\mathbf{G}, \mathbf{G})$, entonces llamaremos a φ un Endomorfismo, escribiremos $End(\mathbf{G})$ en lugar de $Hom(\mathbf{G}, \mathbf{G})$.
   Los isomorfismos de $End(\mathbf{G})$ los llamaremos Automorfismos y el conjunto de todos estos lo notaremos con $Aut(\mathbf{G})$.

3. Sea $\varphi \in Hom(\mathbf{G}, \mathbf{H})$. Definimos

$$\begin{aligned} Im(\varphi) : &= \{\varphi(g) : g \in \mathbf{G}\} \quad (imagende\mathbf{G}) \\ \mathcal{N}(\varphi) : &= \{g \in \mathbf{G} : \varphi(g) = 1\} \quad (nucleode\mathbf{G}) \end{aligned}$$

   Es también usual la notación $kern(\varphi)$ en lugar de $\mathcal{N}(\varphi)$. (Derivada de la expresión **kernel** (núcleo))

1.3.1 Ejemplos.

1. Sea $\mathbf{G} = \mathbf{G}L(2, \mathbb{R})$ y $\mathbf{H} = \mathbb{R}^x$ (grupo multiplicativo de $\mathbb{R}$). Para $g \in \mathbf{G}$, definamos $\varphi(g) := det(g)$.
   Sabemos que $\varphi(gh) = det(gh) = det(g) \cdot det(h) = \varphi(g) \cdot \varphi(h)$. Es decir φ es un homomorfismo.

   φ **es un Epimorfismo**, en efecto, si $a \in \mathbb{R}^x$, entonces

$$\varphi(g) = a, \text{ donde } g = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}.$$

2. Sea $\mathbf{G} = \mathbb{R}$ como grupo aditivo, $\mathbf{H} = \{x \in \mathbb{R} : x > 0\} \leqslant \mathbb{R}^x$. Definamos $\varphi : \mathbf{G} \to \mathbf{H}$ así: $\varphi(x) = e^x$ para $x \in \mathbb{R}$.
   φ **es un Homomorfismo:**

$$\varphi(x + y) = e^{x+y} = e^x \cdot e^y = \varphi(x) \cdot \varphi(y).$$

   φ **es un Momorfismo:**

Recordemos que si $x < y$, entonces $\varphi(x) = e^x < e^y = \varphi(y)$.

φ **es un Epimorfismo:** Sea $0 < s \in \mathbb{R}$, entonces $\varphi(log(s)) = e^{log(s)} = s$. Entonces la función exponencial es un Isomorfismo, por lo tanto $\mathbf{G} \cong \mathbf{H}$. Es decir, el grupo aditivo de los números reales es isomorfo al grupo multiplicativo de los reales positivos.

3. Sea $\mathbf{G}$ un grupo, $g \in \mathbf{G}$. Definamos la función $\delta_g : \mathbf{G} \to \mathbf{G}$ como $\delta_g(x) = g^{-1}xg$ para $x \in \mathbf{G}$.
   Entonces para $x, y \in \mathbf{G}$ tenemos

$$\delta_g(xy) = g^{-1}(xy)g = g^{-1}x\overbrace{gg^{-1}}^{=1}yg = \delta_g(x) \cdot \delta_g(y).$$

   Entonces $\delta_g \in End(\mathbf{G})$.
   La función $\delta_{g^{-1}}$ es la inversa de δ_g. En efecto

$$\delta_{g^{-1}} = (\delta_g(x)) = \delta_{g^{-1}}(g^{-1}xg) = gg^{-1}xgg^{-1} = x.$$

   Entonces $\delta_g \in Aut(\mathbf{G})$.

El conjunto $\{\delta_g : g \in \mathbf{G}\}$ lo llamaremos conjunto de los automorfismos interiores de $\mathbf{G}$ y lo notaremos con $Inn(\mathbf{G})$.

Lema 23.

Sean $\mathbf{G}$, $\mathbf{H}$ grupos, y $\varphi \in Hom(\mathbf{G}, \mathbf{H})$.

1. $\varphi(1) = 1$.
2. $\forall g \in \mathbf{G}, \quad \varphi(g^{-1}) = (\varphi(g))^{-1}$.
3. $Im(\varphi) \leqslant \mathbf{H}$.
4. $\mathcal{N}(\varphi) \leqslant \mathbf{G}$ y además $g^{-1}\mathcal{N}(\varphi)g \leqslant \mathcal{N}(\varphi) \quad \forall g \in \mathbf{G}$.
   (Es decir, $g^{-1}xg \in \mathcal{N}(\varphi) \quad \forall g \in \mathbf{G}$ y $\forall x \in \mathcal{N}(\varphi)$).
5. φ es un Monomorfismo $\Leftrightarrow \quad \mathcal{N}(\varphi) = \{1\}$.
6. φ es un Epimorfismo $\Leftrightarrow \quad Im(\varphi) = \mathbf{H}$.

DEMOSTRACIÓN.

1. $1 \cdot \varphi(1) = \varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) \quad \Rightarrow \quad \varphi(1) = 1.$
2. Sea $g \in \mathbf{G}$, entonces

$$\varphi(g^{-1}) \cdot \varphi(g) = \varphi(g^{-1} \cdot g) = \varphi(1) = 1 \quad \Rightarrow \quad \varphi(g^{-1}) = (\varphi(g))^{-1}.$$

3. Sean $\varphi(g_1), \varphi(g_2) \in Im(\varphi)$

$$\varphi(g_1)(\varphi(g_2))^{-1} \underbrace{=}_{(2)} \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1g_2^{-1}) \in Im(\varphi).$$

4. Sean $g_1, g_2 \in \mathcal{N}(\varphi)$, entonces

$$\varphi(g_1g_2^{-1}) = \varphi(g_1)\varphi(g_2^{-1}) = \underbrace{\varphi(g_1)}_{=1}\underbrace{(\varphi(g))^{-1}}_{=1} = 1 \quad \Rightarrow \quad g_1g_2^{-1} \in \mathcal{N}(\varphi)$$

y se tiene que $\mathcal{N}(\varphi) \leqslant \mathbf{G}$.
Sea $g \in \mathbf{G}, \quad x \in \mathcal{N}(\varphi)$, entonces:

$$\varphi(g^{-1}xg) = (\varphi(g))^{-1}\underbrace{\varphi(x)}_{=1}\varphi(g) = (\varphi(g))^{-1}\varphi(g) = 1.$$

Entonces $g^{-1}xg \in \mathcal{N}(\varphi) \quad \forall g \in \mathbf{G} \quad \forall x \in \mathcal{N}(\varphi)$.

5. (a) Supongamos que φ es inyectiva, entonces existe un único $g \in \mathbf{G}$ tal que $\varphi(g) = 1$, concretamente se tiene que $g = 1$, entonces $\mathcal{N}(\varphi) = \{1\}$.
   (b) Supongamos que $\mathcal{N}(\varphi) = \{1\}$. Sea $\varphi(x) = \varphi(y)$, entonces
   $$1 = \varphi(x)\varphi(y^{-1}) = \varphi(xy^{-1}),$$
   entonces
   $$xy^{-1} \in \mathcal{N}(\varphi) = \{1\} \quad \Rightarrow \quad xy^{-1} = 1 \quad \Rightarrow \quad x = y.$$
6. Evidente, se sigue de la definicón de Epimorfismo.

Definición 24.

Sea $\mathbf{G}$ un grupo.

1. Para $g, h \in \mathbf{G}$ definimos $g^h := h^{-1}gh$ y lo llamaremos el conjugado de g respecto a h.
2. Si $\mathcal{M} \subseteq \mathbf{G}$, entonces se define $\mathcal{M}^g = \{x^g : x \in \mathcal{M}\}$.
   (Entonces $\mathcal{M}^g = \{g^{-1}xg : x \in \mathcal{M}\} = g^{-1}\mathcal{M}g$.
3. Sea $\mathbf{N} \leqslant \mathbf{G}$. Llamaremos a $\mathbf{N}$ un subgrupo normal de $\mathbf{G}$ (notado $\mathbf{N} \trianglelefteq \mathbf{G}$), si se cumple que $g^{-1}\mathbf{N}g = \mathbf{N}g \subseteq \mathbf{N}$, para todo $g \in \mathbf{G}$. Si $\mathbf{N} < \mathbf{G}$, y $\mathbf{N}$ es normal en $\mathbf{G}$, escribiremos $\mathbf{N} \triangleleft \mathbf{G}$.

Nota: Del ejemplo (1.3.1)(3) se tiene que $\mathbf{N} \trianglelefteq \mathbf{G} \Leftrightarrow \mathbf{N}$ permanece invariante bajo todo automorfismo interior de $\mathbf{G}$. Esto es, si $\delta_g \in Inn(\mathbf{G})$, entonces $\delta_g(\mathbf{G}) \subseteq \mathbf{N}$.

1.3.2 Ejemplo.

1. Sea $\varphi \in Hom(\mathbf{G}, \mathbf{H})$, entonces del lema (23)(4) se tiene que $\mathcal{N}(\varphi) \trianglelefteq \mathbf{G}$.
2. Si $\mathbf{G}$ es abeliano, entonces todo subgrupo de $\mathbf{G}$ es normal en $\mathbf{G}$.
3. Siempre se cumple que $\{1\}, \mathbf{G} \trianglelefteq \mathbf{G}$.

Teorema 25.

Sea $\mathbf{N} \leqslant \mathbf{G}$. Entonces son equivalentes:

1. $\mathbf{N} \trianglelefteq \mathbf{G}$.
2. $\forall g \in \mathbf{G}$ se cumple que $g^{-1}\mathbf{N}g = \mathbf{N}$.
3. $\forall g \in \mathbf{G}$ se cumple que $g\mathbf{N} = \mathbf{N}g$.
4. Toda clase lateral izquierda de $\mathbf{N}$ en $\mathbf{G}$ es una clase lateral derecha de $\mathbf{N}$ en $\mathbf{G}$.
5. Toda clase lateral derecha de $\mathbf{N}$ en $\mathbf{G}$ es una clase lateral de $\mathbf{N}$ en $\mathbf{G}$.
6. $\forall g, h \in \mathbf{G}$ se cumple que $(g\mathbf{N})(h\mathbf{N})$ es una clase lateral izquierda de $\mathbf{N}$.
7. $\forall g, h \in \mathbf{G}$ se verifica que $(g\mathbf{N})(h\mathbf{N}) = (gh)\mathbf{N}$

DEMOSTRACIÓN.

$(1) \Rightarrow (2)$: Por hipótesis $\mathbf{N} \trianglelefteq \mathbf{G}$, entonces $g^{-1}\mathbf{N}g \subseteq \mathbf{N}$ para todo $g \in \mathbf{G}$. También se cumple que $(g^{-1})^{-1}\mathbf{N}g^{-1} \subseteq \mathbf{N}$, entonces

$$\mathbf{N} = (g^{-1}g)\mathbf{N}(g^{-1}g) = g^{-1}(g\mathbf{N}g^{-1})g \subseteq g^{-1}\mathbf{N}g.$$

Conclusión: $g^{-1}\mathbf{N}g = \mathbf{N}$ para todo $g \in \mathbf{G}$.

$(2) \Rightarrow (3)$: $\mathbf{N}g = 1 \cdot \mathbf{N}g = (gg^{-1})\mathbf{N}g = g(g^{-1}\mathbf{N}g) = g\mathbf{N}$.

$(3) \Rightarrow (4)$: Es claro.

$(4) \Rightarrow (5)$: Por hipótesis tenemos:

$\forall g \in \mathbf{G}$, existe $h_g \in \mathbf{G}$ tal que $g\mathbf{N} = \mathbf{N}h_g$. Dado que

$$\mathbf{G} = \bigcup_{g \in \mathbf{G}} g\mathbf{N} = \bigcup_{g \in \mathbf{G}} \mathbf{N}h_g$$

uno tiene todas las clases laterales derechas de
$\mathbf{N}$ en $\mathbf{G}$ en la forma $\mathbf{N}h_g$ y cada una de estas es una clase lateral izquierda de $\mathbf{N}$, en efecto, $\mathbf{N}h_g = g\mathbf{N}$.

$(5) \Rightarrow (6)$: Por Hipótesis $\mathbf{N}g = h_g\mathbf{N}$ Para algún $h_g \in \mathbf{G}$. Entonces:

$$(g\mathbf{N})(h\mathbf{N}) = g(\mathbf{N}h)\mathbf{N} = g(k_h\mathbf{N})\mathbf{N} = (gk_h)\mathbf{N}\mathbf{N} = (gk_h)$$

$(6) \Rightarrow (7)$: Supongamos que $(g\mathbf{N})(h\mathbf{N}) = k\mathbf{N}$, entonces

$$gh = (g \cdot 1)(h \cdot 1) \in (g\mathbf{N})(h\mathbf{N}) = k\mathbf{N}.$$

Es decir: $gh \in k\mathbf{N}$, entonces existe $n \in \mathbf{N}$ tal que $gh = kn$. Con esto se tiene que $k\mathbf{N} = (kn)\mathbf{N} = (gh)\mathbf{N}$.

$(7) \Rightarrow (1)$: Por Hipótesis $\mathbf{N} \cdot g\mathbf{N} = g\mathbf{N}$, entonces

$$\overbrace{g^{-1}\mathbf{N}g}\mathbf{N} = \mathbf{N} \quad \Rightarrow \quad g^{-1}\mathbf{N}g \subseteq \mathbf{N} \quad \Rightarrow \quad \mathbf{N} \trianglelefteq \mathbf{G}.$$

Nota: El teorema (25)(7) nos permite definir sobre el conjunto de las clases laterales izquierdas de $\mathbf{N}$ en $\mathbf{G}$ una operación de tal manera que se induce una estructura de grupo.

Teorema 26.

1. Sea $\mathbf{N} \trianglelefteq \mathbf{G}$ y definamos $\mathbf{G}/\mathbf{N} := \{g\mathbf{N} : g \in \mathbf{G}\}$. Esto es, $\mathbf{G}/\mathbf{N}$ es el conjunto de las clases laterales izquierdas de $\mathbf{N}$ en $\mathbf{G}$.
   También $\mathbf{G}/\mathbf{N}$ es el conjunto de las clases laterales derechas de $\mathbf{N}$ en $\mathbf{G}$. (consecuencia del teorema (25)).
   Con la multiplicación: $(g\mathbf{N}) \cdot (h\mathbf{N}) := (gh)\mathbf{N}$, $\mathbf{G}/\mathbf{N}$ es un grupo, el cual denominaremos grupo factor de $\mathbf{G}$ con respecto a $\mathbf{N}$.
2. La función $\gamma : \mathbf{G} \to \mathbf{G}/\mathbf{N}$ definida por $\gamma(g) = g\mathbf{N}$ es un Epimorfismo y $\mathcal{N}(\gamma) = \mathbf{N}$. A γ la llamaremos Homomorfismo natural o canónico de $\mathbf{G}$ sobre $\mathbf{G}/\mathbf{N}$. (Esto demuestra que los subgrupos normales de un grupo son precisamente el nucleo de este homomorfismo natural).

DEMOSTRACIÓN.

1. Se verifica que:

   (a)
   $$\begin{aligned}(g\mathbf{N} \cdot h\mathbf{N})k\mathbf{N} &= ((gh)\mathbf{N})(k\mathbf{N}) = ((gh)k)\mathbf{N} \\ &= (g(hk))\mathbf{N} = (g\mathbf{N})((hk)\mathbf{N}) \\ &= g\mathbf{N}((h\mathbf{N})(k\mathbf{N})).\end{aligned}$$

   (b) $\mathbf{N}(g\mathbf{N}) = (1\mathbf{N})(g\mathbf{N}) = (1g)\mathbf{N} = g\mathbf{N} \quad \forall g \in \mathbf{G}$. Entonces el 1 de $\mathbf{G}/\mathbf{N}$ es $\mathbf{N}$.

   (c) Se cumple que $(g^{-1}\mathbf{N})(g\mathbf{N}) = (g^{-1}g)\mathbf{N} = 1\mathbf{N} = \mathbf{N} \quad \forall g \in \mathbf{G}$, es decir, $(g\mathbf{N})^{-1} = g^{-1}\mathbf{N}$. Esto demuestra que $\mathbf{G}/\mathbf{N}$ es un grupo.

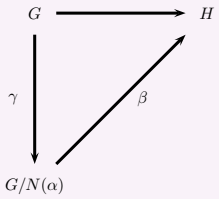
2. (a) γ es un Homomorfismo: $\gamma(gh) = (gh)\mathbf{N} = g\mathbf{N} \cdot h\mathbf{N} = \gamma(g) \cdot \gamma(h)$.

   (b) Es claro que γ es un Epimorfismo.

   (c)
   $$\begin{aligned}\mathcal{N}(\gamma) &= \{g \in \mathbf{G} : \gamma(g) = \mathbf{N}\} \\ &= \{g \in \mathbf{G} : \underbrace{g\mathbf{N} = \mathbf{N}}_{\Leftrightarrow g \in \mathbf{N}}\} \\ &= \{g \in \mathbf{G} : g \in \mathbf{N}\} \\ &= \mathbf{N}\end{aligned}$$

Teorema 27 (Primer Teorema de Isomorfía)**.**

Sean $\mathbf{G}, \mathbf{H}$ dos grupos, $\alpha \in Hom(\mathbf{G}, \mathbf{H})$. Sea γ el homomorfismo canónico de $\mathbf{G}$ en $\mathbf{G}/_{\mathcal{N}(\alpha)}$, entonces existe un homomorfismo $\beta \in Hom(\mathbf{G}/_{\mathcal{N}(\alpha)}, \mathbf{H})$ con la propiedad $\alpha = \beta\gamma$. Se cumple además que $\mathbf{G}/_{\mathcal{N}(\alpha)} \cong Im(\alpha)$.



DEMOSTRACIÓN.
Necesitamos construir la función β. Definamos,

$$\begin{aligned} \beta : \mathbf{G}/_{\mathcal{N}(\alpha)} &\to \mathbf{H} \\ \beta(g\mathcal{N}(\alpha)) &= \alpha(g). \end{aligned}$$

1. β **está bien definida:** Esto es necesario hacerlo ya que un elemento $g \in \mathbf{G}$ no queda completamente determinado por una clase lateral $g\mathcal{N}(\alpha)$. La idea es asegurarse que no importa el representante de la clase lateral que se tome, la función β arroja el mismo resultado.
   Demostremos entonces que si $g\mathcal{N}(\alpha) = h\mathcal{N}(\alpha)$, entonces $\alpha(g) = \alpha(h)$. Bien, supongamos entonces que $g\mathcal{N}(\alpha) = h\mathcal{N}(\alpha)$, entonces $h^{-1}g\mathcal{N}(\alpha) = \mathcal{N}(\alpha)$, lo cual implica que $h^{-1}g \in \mathcal{N}(\alpha)$ entonces $\alpha(h^{-1}g) = 1$, entonces

$$1 = \alpha(h^{-1}g) = \alpha(h^{-1})\alpha(g) = (\alpha(h))^{-1}\alpha(g) \quad \Rightarrow \quad \alpha(g) = \alpha(h).$$

2. β **es Homomorfismo:**

$$\begin{aligned} \beta(g\mathcal{N}(\alpha) \cdot h\mathcal{N}(\alpha)) &= \beta(gh\mathcal{N}(\alpha)) \\ &= \alpha(gh) \\ &= \alpha(g) \cdot \alpha(h) \\ &= \beta(g\mathcal{N}(\alpha))\beta(h\mathcal{N}(\alpha)). \end{aligned}$$

3. β **es Monomorfismo:**

$$\begin{aligned} \mathcal{N}(\alpha) &= \{g\mathcal{N}(\alpha) : \alpha(g) = 1\} \\ &= \{g\mathcal{N}(\alpha) : g \in \mathcal{N}(\alpha)\} \\ &= \mathcal{N}(\alpha) \end{aligned}$$

   (Este es el 1 de $\mathbf{G}/_{\mathcal{N}(\alpha)}$).

4. $\alpha = \beta\gamma$: Sea $g \in \mathbf{G}$, entonces

$$\alpha(g) = \beta(g\mathcal{N}(\alpha)) = \beta(\gamma(g)) = (\beta\gamma)(g).$$

5. Es claro que $\beta : \mathbf{G}/_{\mathcal{N}(\alpha)} \to Im(\alpha)$ es un isomorfismo, entonces $\mathbf{G}/_{\mathcal{N}(\alpha)} \cong Im(\alpha)$.

Teorema 28.

Sea $\mathbf{G}$ un grupo, $\mathbf{N} \trianglelefteq \mathbf{G}$, $\quad \mathcal{U} \leqslant \mathbf{G}$.

1. $\mathcal{U}\mathbf{N} = \mathbf{N}\mathcal{U} \leqslant \mathbf{G}$.
2. $\mathcal{U} \cap \mathbf{N} \trianglelefteq \mathcal{U}$.

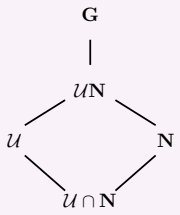
DEMOSTRACIÓN.

1. Es suficiente demostrar que $\mathcal{U}\mathbf{N} = \mathbf{N}\mathcal{U}$ (ver teorema (18)(2)).
   Dado que $\mathbf{N} \trianglelefteq \mathbf{G}$, se tiene inmediatamente la condición por teorema (25)(3).
2. Sea $u \in \mathcal{U}$, entonces $(\mathcal{U} \cap \mathbf{N})^u = \mathcal{U}^u \cap \mathbf{N}^u = \mathcal{U} \cap \mathbf{N}$, lo cual demuestra que $(\mathcal{U} \cap \mathbf{N}) \trianglelefteq \mathcal{U}$.

Teorema 29 (Segundo teorema de isomorfía)**.**

Sea $\mathbf{G}$ un grupo, $\mathbf{N} \trianglelefteq \mathbf{G}$ y $\mathcal{U} \leqslant \mathbf{G}$. Entonces,

$$\mathcal{U}\mathbf{N}/_{\mathbf{N}} \cong \mathcal{U}/_{\mathcal{U}\cap\mathbf{N}}.$$



DEMOSTRACIÓN. Por teorema (28) sabemos que $\mathcal{U}\mathbf{N} \leqslant \mathbf{G}$ y $\mathcal{U} \cap \mathbf{N} \trianglelefteq \mathcal{U}$. Definamos la función φ de la siguiente manera:

$$\begin{aligned} \varphi : \mathcal{U}\mathbf{N} &\to \mathcal{U}/_{\mathcal{U}\cap\mathbf{N}} \\ un &\xrightarrow{\varphi} \mathcal{U}(\mathcal{U} \cap \mathbf{N}) \end{aligned}$$

1. φ **está bien definida:** Supongamos que $u_1n_1 = u_2n_2$ con $u_i \in \mathcal{U}$ y $n_i \in \mathbf{N}$.
   Demostremos que $u_1(\mathcal{U} \cap \mathbf{N}) = u_2(\mathcal{U} \cap \mathbf{N})$.
   Si $u_1n_1 = u_2n_2$, entonces $\underbrace{u_2^{-1}u_1}_{\in\mathcal{U}} = \underbrace{n_2n_1^{-1}}_{\in\mathbf{N}} \in (\mathcal{U} \cap \mathbf{N})$, entonces

   $$(\mathcal{U} \cap \mathbf{N}) = u_2^{-1}u_1(\mathcal{U} \cap \mathbf{N}),$$

   luego

   $$u_1(\mathcal{U} \cap \mathbf{N}) = u_2(\mathcal{U} \cap \mathbf{N}).$$

2. φ **es un Homomorfismo:** Sea $u_1, u_2 \in \mathcal{U}, \quad n_1, n_2 \in \mathbf{N}$, entonces

$$\begin{aligned}\varphi(u_1n_1 \cdot u_2, n_2) &= \varphi(\underbrace{u_1u_2}_{\in\mathcal{U}} \overbrace{\underbrace{u_2^{-1}n_1u_2}_{\in\mathbf{N}} n_2}^{\in\mathbf{N}}) \\ &= \varphi(u_1u_2 \cdot n) \\ &= u_1u_2(\mathcal{U} \cap \mathbf{N}) \\ &= (u_1(\mathcal{U} \cap \mathbf{N}))(u_2(\mathcal{U} \cap \mathbf{N})) \\ &= \varphi(u_1n_1) \cdot \varphi(u_2n_2)\end{aligned}$$

3. Evidentemente φ es Epimorfismo.

4. φ **es inyectiva:**

$$\begin{aligned}\mathcal{N}(\varphi) &= \{un : u \in \mathcal{U}, n \in \mathbf{N}, \quad \overbrace{u(\mathcal{U} \cap \mathbf{N}) = (\mathcal{U} \cap \mathbf{N})}^{\Leftrightarrow u \in (\mathcal{U} \cap \mathbf{N})}\} \\ &= \{un : u \in (\mathcal{U} \cap \mathbf{N}), \quad n \in \mathbf{N}\} \\ &= \mathbf{N}\end{aligned}$$

5. **Conclusión**

$$\mathcal{U}\mathbf{N}/_{\mathbf{N}} = \mathcal{U}\mathbf{N}/_{\mathcal{N}(\varphi)} \cong Im(\varphi) = \mathcal{U}/_{\mathcal{U} \cap \mathbf{N}}$$

1.3.3 Ejemplo. 1. Denotemos con $\mathbb{Z}(+)$ a $\mathbb{Z}$ como grupo aditivo. Sea $n \in \mathbb{Z}$. Hemos demostrado en el ejemplo (1.2.1)(2) que $n\mathbb{Z}(+)$ es un subgrupo de $\mathbb{Z}(+)$, dado que $\mathbb{Z}(+)$ es abelinano, se tiene que $n\mathbb{Z}(+)$ es normal en $\mathbb{Z}(+)$. Note que

$$\begin{aligned}j + n\mathbb{Z}(+) = k + n\mathbb{Z}(+) &\Leftrightarrow (j-k) + n\mathbb{Z}(+) = n\mathbb{Z}(+) \\ &\Leftrightarrow (j-k) \in \mathbb{Z}(+) \\ &\Leftrightarrow n|(j-k)\end{aligned}$$

Por lo tanto: $\{0, 1, 2, ..., n-1\}$ es un transversal de $n\mathbb{Z}(+)$ en $\mathbb{Z}$, es decir

$$\mathbb{Z}(+)/_{n\mathbb{Z}(+)} = \{j + n\mathbb{Z}(+) : j \in \{0, 1, 2, ..., n-1\}\}$$

y por lo tanto

$$\left|\mathbb{Z}(+)/_{n\mathbb{Z}(+)}\right| = n$$

Por otro lado:

$$(j + n\mathbb{Z}(+)) + (k + n\mathbb{Z}(+)) = \begin{cases} (j+k) + n\mathbb{Z}(+) & \text{si } j+k < n \\ (j+k-n) + n\mathbb{Z}(+) & \text{si } j+k \geq n \end{cases}$$

Esto trae como consecuencia que $\mathbb{Z}(+)/_{n\mathbb{Z}(+)} = \langle 1 + n\mathbb{Z}(+)\rangle$, es decir un grupo cíclico de orden n.

2. Sea $\mathbf{G} = \langle g\rangle$ un grupo cíclico de orden n. (también $o(g) = n$). definamos

$$\begin{aligned}\alpha : \mathbb{Z}(+) &\to \mathbf{G} \\ \alpha(i) &= g^i \qquad \forall i \in \mathbb{Z}(+)\end{aligned}$$

(a) α **es un Homomorfismo:** $\alpha(i+j) = g^{i+j} = g^i \cdot g^j = \alpha(i)\alpha(j)$.

(b) α **es Epimorfismo:** Dado que $\mathbf{G} = \langle g \rangle = \{g^i : j \in \mathbb{Z}\}$ se tiene que α es sobre.

(c) α **es Monomorfismo:**

$$\begin{aligned} \mathcal{N}(\alpha) &= \{j \in \mathbb{Z} : g^i = 1\} \\ &= \{j \in \mathbb{Z} : n|j\} = n\mathbb{Z}(+) \end{aligned}$$

Entonces $\mathbb{Z}(+)/_{n\mathbb{Z}(+)} \cong \mathbf{G}$.

- Esto demuestra que salvo isomorfismos existe un único grupo cíclico de orden n, $\mathbb{Z}(+)/_{n\mathbb{Z}(+)} \cong \mathbf{G}$.

1.4 Permutaciones y signo

Consideremos nuevamente el grupo simétrico $Sym(n)$ o S_n. Estos

$$S_n = \{f : \Omega \to \Omega : \text{f es una biyección } \Omega = \{1, 2, ..., n\}\}$$

Definición 30.

Sea $\pi \in S_n$, llamaremos a π un k-ciclo o un ciclo de longitud k, si existen $x_1, x_2, ..., x_k \in \Omega$ (distintos dos a dos), tales que $\pi(x_i) = x_{i+1}$ para $1 \leq i \leq k-1$, $\pi(x_k) = x_1$ y $\pi(x) = x$ para todo $x \in \Omega - \{x_1, ..., x_k\}$. Esto es:

$$\begin{aligned} \pi(x_1) &= x_2 \\ \pi(x_2) &= x_3 \\ &\vdots \\ \pi(x_k) &= x_1 \\ \pi(x) &= x \end{aligned}$$

$\forall x \in \Omega - \{x_1, ..., x_k\}$.
O también

$$\pi = \begin{pmatrix} x_1 & x_2 & \cdots & x_{k-1} & x_k & x_{k+1} & \cdots & x_n \\ x_2 & x_3 & \cdots & x_k & x_1 & x_{k+1} & \cdots & x_n \end{pmatrix},$$

ó

$$\pi = (x_1, x_2, \cdots, x_k)$$

Evidentemente: $(x_1, x_2, \cdots, x_n) = (x_i, x_{i+1}, \cdots, x_m, x_1, \cdots, x_{i-1})$.

1.4.1 Ejemplo. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{pmatrix} = (1,2,3) = (2,3,1) = (3,1,2)$. Un 2-ciclo se llama una transposición. Si τ es una transpoción, entonces se cumple

$$\tau = \begin{pmatrix} j & k \\ k & j \end{pmatrix} = (j,k) \text{ donde } j \neq k \text{ y } j, k \in \{1, 2, ..., n\}$$

Definición 31.

Sea $\pi \in S_n$. Para $x, y \in \Omega$, si existe $k \in \mathbb{Z}$ tal que $\pi^k(x) = y$ denotamos $x \sim_\pi y$.

Lema 32.

$\sim_\pi$ es una relación de equivalencia sobre Ω.

DEMOSTRACIÓN.

1. $\sim_\pi$ es reflexiva:

   Sea $x \in \Omega$, se tiene que $\pi^0(x) = I_\Omega(x) = x$. Entonces, $x \sim_\pi x$

2. $\sim_\pi$ es simétrica:

   Si $x \sim_\pi y$, entonces $\pi^k(x) = y$ para algún $k \in \mathbb{Z}$. Por lo tanto,

   $$\pi^{-k}(y) = x \ \Rightarrow \ y \sim_\pi x.$$

3. $\sim_\pi$ es transitiva:

   Supongamos que $x \sim_\pi y$ y $y \sim_\pi z$ para $x, y, z \in \Omega$. Entonces, existen $k, m \in \mathbb{Z}$ tal que $\pi^k(x) = y$ y $\pi^m(y) = z$. Ahora,

   $$z = \pi^m(y) = \pi^m(\pi^k(x)) = \pi^{m+k}(x).$$

   Por lo tanto,

   $$x \sim_\pi z.$$

Sabemos que esta relación de equivalencia suministra una descomposición de Ω en conjuntos distintos, concretamente las clases de equivalencia de $\sim_\pi$.

Las clases de equivalencia de $x \in \Omega$ las llamaremos la órbita de x bajo π, entonces

$$O_\pi(x) = \{\pi^k(x) : k \in \mathbb{Z}\}.$$

Dado que Ω es un conjunto finito, los elementos $x, \pi(x), \pi^2(x), ...$ no pueden ser todos distintos, i,e. Existen $m, n \in \mathbb{N}$ tales que $m > n$ y $\pi^m(x) = \pi^n(x)$, es decir $\pi^{m-n}(x) = x$. Entonces existen k un natural con esta propiedad pero minimal. (principio de buen orden).
Tenemos entonces que la órbita de x bajo π consta exactamente de los siguientes elementos:

$$x, \pi(x), ..., \pi^{k-1}(x) \text{ y además } \pi^k(x) = x.$$

1.4.2 Ejemplo. Consideremos $\pi \in S_7$ definida por

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 6 & 5 & 4 & 7 \end{pmatrix}.$$

Entonces Ω se descompone en las siguientes órbitas:

$$\begin{aligned} 1 &= \pi^0(1), \quad 2 = \pi(1), \quad 3 = \pi^2(1) \\ O_\pi(1) &= \{1, 2, 3\} \\ 4 &= \pi^0(4), \quad 6 = \pi(4) \\ O_\pi(4) &= \{4, 6\} \\ 5 &= \pi^0(5) \quad \wedge \quad 7 = \pi^0(7) \quad \Rightarrow \quad O_\pi(5) = \{5\} \quad \wedge \quad O_\pi(7) = \{7\}. \end{aligned}$$

1.4.3 Ejemplo. Sea $\pi \in S_8$ definida por

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 7 & 4 & 1 & 8 & 3 & 5 & 2 \end{pmatrix}.$$

Halle la descomposiciín e órbitas inducida por π.

$$1 = \pi^0(1), \quad 6 = \pi^1(1), \quad 3 = \pi^2(1), \quad 4 = \pi^3(1), \quad 1 = \pi^4(1).$$

Entonces $O_\pi(1) = \{1, 3, 4, 6\}$

$$2 = \pi^0(2), \quad 7 = \pi(2), \quad 5 = \pi^2(2), \quad 8 = \pi^3(2), \quad 2 = \pi^4(2)$$

Entonces $O_\pi(2) = \{2, 5, 7, 8\}$

Teorema 33.

1. Cada permutación $\pi \in S_n$ se puede descomponer como el producto (composición) de ciclos disyuntos dos a dos y además esta descomposición es única salvo el orden en el que se escriban los ciclos. Esto es,

   $$\pi = (x_1, \pi(x_1), \ldots, \pi^{n_1-1}(x_1)) \cdots (x_k, \pi(x_k), \ldots, \pi^{n_k-1}(x_k))$$

   donde

   $$n_j \in \mathbb{N}, \quad \sum_{j=1}^{k} n_j = n \text{ y } \Omega = \biguplus_{j=1}^{n} \{(x_j, \pi(x_j), \cdots, \pi^{n_j-1}(x_j))\}.$$

2. Todo elemento de S_n es un producto de transposiciones (si $n \geq 2$).

DEMOSTRACIÓN.

1. Sean $x_1, x_2, ..., x_k$ un sistema de representantes de las órbitas de Ω inducidas por π. La órbita $O_\pi(x_j)$ tiene la forma

   $$O_\pi(x_j) = \{(x_j, \pi(x_j), \cdots, \pi^{n_k-1}(x_j))\},$$

   con $\pi^{n_k-1}(x_j) = x_j$, pero $\pi^m(x_j) \neq x_j \quad \forall m$ con $1 \leq k < n_k$.
   Definamos

   $$\sigma_j := ((x_j, \pi(x_j), \cdots, \pi^{n_j-1}(x_j))) \text{ para } j = 1, 2, ..., k.$$

   Tenemos así k ciclos disyuntos con longitud n_j. Sabemos que cada elemento de Ω aparece exactamente en una órbita ya que $\sigma_j(x) = \pi(x)$ y $\pi(x)$ aparece solamente en σ_j y bajo el resto de estos ciclos permanece invariante, esto es,

   $$(\sigma_1\sigma_2 \cdots \sigma_k)(x) = \pi(x).$$

   Entonces $\pi = \sigma_1\sigma_2 \cdots \sigma_k$.
   Sea ahora $\pi = \hat{\sigma_1} \cdots \hat{\sigma_r}$ otra descomposición de π en ciclos disyuntos.
   Sea $\hat{\sigma_j} = (y_{j1}, ..., y_{jm_j})$ un ciclo de longitud m_j, se cumple que

   $$\pi(y_{jk}) = \hat{\sigma_1} \cdots \hat{\sigma_r}(y_{jk}) = \hat{\sigma_j}(y_{jk}) = y_{j,k+1}$$

   para $1 \leq k < m_j$ y $\pi(y_{jm_j}) = y_{j1}$. Esto trae como consecuencia

$$\hat{\sigma_j} = (y_{j1}, \pi(y_{j1}), ..., \pi^{m_j-1}(y_{j1})).$$

Por otro lado existe exactamente una órbita $O_\pi(x_i)$ con la propiedad $y_{j1} \in O_\pi(x_i)$, es decir, para algún $s \in \mathbb{Z}, \quad 0 \leq s \leq n_j - 1$ se tiene

$$\pi^s(x_i) = y_{j1}.$$

Entonces,

$$\pi^{n_i}(b_{j1}) = \pi^{n_i+s}(x_i) = \pi^s(\pi^{n_i}(x_i)) = \pi^s(x_i) = y_{j1},$$

y $\pi^m(b_{j1}) \neq b_{j1}$ para todo $1 \leq m < n_j$. Entonces, $m_j = n_i$ y $\hat{\sigma_j} = \sigma_i$. En particular, se sigue que $r = k$.

2. De (1) se sigue que toda permutación se puede expresar como el producto de ciclos, entonces es suficiente demostrar que todo ciclo puede escribirse como el producto de transposiciones.

   Sea $\tau = (x_1, x_2, ..., x_m)$ un siclo.

   Caso 1: $m > 1$, entonces $\tau = (x_1, x_m)(x_1, x_{m-1}) \cdots (x_1, x_3)(x_1, x_2)$. En efecto

$$((x_1, x_m) \cdots (x_1, x_{k+1})(x_1, x_k) \cdots (x_1, x_2))(x_k)$$
$$= \begin{cases} x_1 & \text{si } k = m \\ ((x_1, x_m) \cdots (x_1, x_{k+1}))x_1 = x_{k+1} & \text{si } k < m \end{cases}$$

   Caso 2: $m = 1$ un cíclo de longitud 1 deja fijo a todo elemento de Ω, es decir, la función identidad.

Teorema 34.

1. Para $n \geq 2$ existe un Epimorfismo $sgn : S_n \to \{-1, 1\}$ (como grupo multiplicativo) tal que $sgn(\tau) = -1$ para toda transposición $\tau \in S_n$. Esta función la llamaremos signo.
2. Si $f \in Hom(S_n, \mathbb{R}^x)$, entonces se cumple que $f(\pi) = sgn(\pi)$ o $f(\pi) = 1 \; \forall \pi \in S_n$.

DEMOSTRACIÓN. Sea $\Lambda = \{\{i, j\} : i, j \in \Omega, \quad i \neq j\}$, esto es, Λ es el conjunto cuyos elementos son subconjuntos de Ω con dos elementos.

(a) Si $\sigma \in S_n$, entonces $\Lambda = \{\sigma(\mathcal{A}) : \mathcal{A} \in \Lambda\}$. Esto es claro ya que σ es una biyección.

(b) Sea $\mathcal{A} = \{i, j\} \in \Lambda$ con $i < j$ y sea $\pi \in S_n$. Definamos

$$Z_\pi(\mathcal{A}) := \begin{cases} 1 & \text{si } \pi(i) < \pi(j) \\ -1 & \text{si } \pi(i) > \pi(j) \end{cases}$$

Sea ahora $\pi, \sigma \in S_n, \quad \mathcal{A} = \{i, j\}$ con $i < j$. Consideremos la siguiente tabla.

CASOS	$z_\sigma(A)$	$z_\pi(\sigma(A))$	$z_{\pi\sigma}(A)$
$\sigma(i) < \sigma(j), \quad \pi(\sigma(i)) < \pi(\sigma(j))$	1	1	1
$\sigma(i) < \sigma(j), \quad \pi(\sigma(i)) > \pi(\sigma(j))$	1	-1	-1
$\sigma(i) > \sigma(j), \quad \pi(\sigma(i)) < \pi(\sigma(j))$	-1	-1	1
$\sigma(i) > \sigma(j), \quad \pi(\sigma(i)) > \pi(\sigma(j))$	-1	1	-1

Nota: Hemos considerado el siguiente hecho

$$(\pi\sigma)(\mathcal{A}) = \{(\pi\sigma)(i), (\pi\sigma)(j)\} = \{\pi(\sigma(i)), \pi(\sigma(i))\} = \pi(\sigma(\mathcal{A})).$$

De la tabla se sigue:

$$Z_{\pi\sigma}(\mathcal{A}) = Z_\sigma(\mathcal{A}) Z_\pi(\sigma(\mathcal{A})).$$

(c) Definamos $sgn(\pi) := \prod_{\mathcal{A}\in\Lambda} Z_\pi(\mathcal{A}) \qquad sgn : S_n \to \{-1, 1\}$, entonces tenemos

$$\begin{aligned} sgn(\pi\sigma) &= \prod_{\mathcal{A}\in\Lambda} Z_{\pi\sigma}(\mathcal{A}) \\ &= \prod_{\mathcal{A}\in\Lambda} Z_\sigma(\mathcal{A}) Z_\pi(\sigma(\mathcal{A})) \\ &= \prod_{\mathcal{A}\in\Lambda} Z_\sigma(\mathcal{A}) \prod_{\mathcal{A}\in\Lambda} Z_\pi(\sigma(\mathcal{A})) \\ &= \prod_{\mathcal{A}\in\Lambda} Z_\sigma(\mathcal{A}) \cdot \prod_{\mathcal{A}\in\Lambda} Z_\pi(\mathcal{A}) \\ &= sgn(\pi) \cdot sgn(\sigma) \end{aligned}$$

(d) Sea $\tau = (1, 2)$, entonces $Z_\tau(\mathcal{A}) = \begin{cases} -1 & \text{para } \mathcal{A} = \{1, 2\} \\ 1 & \text{en otro caso} \end{cases}$.

Entonces $sgn(\tau) = \prod_{\mathcal{A}\in\Lambda} Z_\tau(\mathcal{A}) = -1$.

(e) Sea $\tau' = (i, j)$ con $i \neq j$. Definamos $\pi = \begin{pmatrix} 1 & 2 & \cdots \\ i & j & \cdots \end{pmatrix} \in S_n$.

Entonces se cumple: $\tau' = \pi\tau\pi^{-1}$, en efecto:

$$\begin{aligned} (\pi\tau\pi^{-1})(i) &= \pi\tau(\pi^{-1}(i)) = \pi(\tau(1)) = \pi(2) = j \\ (\pi\tau\pi^{-1})(j) &= \pi\tau(\pi^{-1}(j)) = \pi(\tau(2)) = \pi(1) = i \end{aligned}$$

Sea $k \neq i, j$, entonces $\pi^{-1}(k) \neq 1, 2$. Por lo tanto

$$(\pi\tau\pi^{-1})(k) = \pi\tau(\underbrace{\pi^{-1}(k)}_{\neq 1,2}) = \pi(\pi^{-1}(k)) = k.$$

Conclusión: $\tau' = \pi\tau\pi^{-1}$, con esto se sigue:

$$sgn(\tau') = sgn(\pi) \cdot \underbrace{sgn(\tau)}_{=-1} \cdot \underbrace{sgn(\pi^{-1})}_{=(sgn(\pi))^{-1}} = -1.$$

(f) Sea $f \in Hom(S_n, \mathbb{R}^x)$ y sea τ una transposición, entonces $1 = f(\underbrace{\tau^2}_{=1}) = (f(\tau))^2$. Entonces $f(\tau) \in \{-1, 1\}$, sea ahora τ' otra transposición y sea π la permutación definida en (e) con $\tau' = \pi\tau\pi^{-1}$, entonces

$$f(\tau') = f(\pi) f(\tau) f(\pi^{-1}) = f(\tau).$$

Conclusión: Todas las transposiciones tienen la misma imagen bajo f, es decir 1 o -1.
Del teorema (33)(2) tenemos que toda permutación π tiene la forma $\pi = \tau_1\tau_2\cdots\tau_n$, τ_i son transposiciones.
Diferenciamos ahora dos casos:

Caso 1: $f(\tau_j) = -1 \quad \forall\tau_j$, entonces

$$f(\pi) = \prod_{j=1}^{m} f(\tau_j) = (-1)^m = \prod_{j=1}^{m} sgn(\tau_j) = sgn(\pi).$$

Esto se cumple $\forall\pi \in S_n$, entonces $f = sgn$.

Caso 2: $f(\tau_j) = 1 \quad \forall\tau_j$, entonces $f(\pi) = 1 \quad \forall\pi \in S_n$

1.4.4 Observación.

1. Toda permutación $\pi \in S_n$ se puede descomponer como un producto par o impar de transposiciones.
2. Si π es un k-ciclo, entonces
$$sgn(\pi) = (-1)^{k-1}$$

DEMOSTRACIÓN.

1. Sea $\pi = \tau_1\cdots\tau_k = \hat{\tau_1}\cdots\hat{\tau_k}$, donde $tau_i, \hat{\tau_i}$ son transposiciones, entonces
$$(-1)^{k-l} = sgn(\pi) = (-1)^l \Rightarrow (-1)^{k-l} = 1,$$
es decir $k - l$ es par.
2. Es claro que cada k-ciclo se puede escribir como el producto de $k-1$ transposiciones. El resto se sigue del teorema (34).

Definición 35.

Para $n \geq 2$, definamos $\mathcal{N}(sgn)$ como $\mathcal{A}_n$, esto es

$$\mathcal{A}_n = \{\pi \in S_n : sgn(\pi) = 1\}.$$

$\mathcal{A}_n$ se denomina grupo alternante de grado n. Las permutaciones que pertenecen a $\mathcal{A}_n$ las llamaremos pares y las pertenecientes a $S_n \diagdown \mathcal{A}_n$ las llamaremos impares.

Teorema 36.

Para $n \geq 2$ se tiene que $\mathcal{A}_n \lhd S_n$ y $|S_n : \mathcal{A}_n| = 2$. Para toda $\pi \in S_n$ con $sgn(\pi) = -1$ se cumple que

$$S_n = \mathcal{A}_n \quad \biguplus \quad \pi\mathcal{A}_n = \mathcal{A}_n \quad \biguplus \quad \mathcal{A}_n\pi.$$

DEMOSTRACIÓN. Dado que $\mathcal{A}_n = \mathcal{N}(sgn)$ se tiene que $\mathcal{A}_n \lhd S_n$.

$$|S_n : \mathcal{A}_n| = |S_n/_{\mathcal{A}_n}| = |Im(sgn)| = 2.$$

$\forall\pi \in S_n$, con $sgn(\pi) = -1$ se tiene que $\pi\mathcal{A}_n \neq \mathcal{A}_n \neq \mathcal{A}_n\pi$ y se tiene entonces la descomposición en clases laterales.

1.5 Cuerpos

Definición 37.

Un conjunto $\mathcal{K}$ $(\mathcal{K} \neq 0)$ sobre el cual están definidas dos operaciones binarias " $+$ " y " $\cdot$ " se llama un cuerpo (o campo), si los siguientes axiomas se verifican:

1. $\mathcal{K}$ con respecto a $+$ es un grupo abeliano con módulo 0. (A este grupo lo llamaremos grupo aditivo de $\mathcal{K}$, notado $\mathcal{K}(+)$).
2. $\mathcal{K} - \{0\}$ con respecto a la multiplicación es un grupo abeliano con módulo 1. (A este grupo lo llamaremos grupo multiplicativo de $\mathcal{K}$, este lo notaremos con $\mathcal{K}^x$).
3. $\forall x, y, z \in \mathcal{K}$ se verifica

$$x(y+z) = xy + xz$$
$$(x+y)z = xz + yz$$

1.5.1 Observación.

1. Del teorema (3) se sigue $0, \quad 1, \quad -a, \quad a^{-1}$ (para $a \neq 0$) están determinados de manera única.
2. Si $\mathcal{K}$ satisface todos los axiomas salvo $ab = ba \quad \forall a, b \in \mathcal{K}$ es decir $\mathcal{K}^x$ no es necesariamente abeliano, entonces $\mathcal{K}$ se llamará cuerpo inclinado (semi-cuerpo).
3. Si $\mathcal{K}(+)$ es un grupo abeliano y $\mathcal{K}^x$ es un semigrupo, entonces $\mathcal{K}$ se denomina anillo. Si además existe $1 \in \mathcal{K}$ tal que $1 \cdot x = x \quad \forall x \in \mathcal{K}$, entonces $\mathcal{K}$ se llama un anillo con uno.

Teorema 38.

(Leyes de cancelación). Sea $\mathcal{K}$ un cuerpo y sean $a, x, y \in \mathcal{K}$.

1. Si $a + x = a + y$, entonces $x = y$.
2. Si $a \neq 0$ y $ax = ay$, entonces $x = y$.

DEMOSTRACIÓN.

1. El teorema (3) aplicado a $\mathcal{K}(+)$.
2. Dado que $a \neq 0$, existe $b \in \mathcal{K}$ tal que $ab = 1 = ba$. Entonces

$$x = 1 \cdot x = (ba)x = b(ax) = b(ay) = (ba)y = 1 \cdot y = y.$$

Teorema 39.

Sea $\mathcal{K}$ un anillo.

1. $\forall a \in \mathcal{K}$, se cumple que $a \cdot 0 = 0 \cdot a = 0$.
2. $\forall a, b \in \mathcal{K}$, se cumple que $(-a)b = a(-b) = -(ab)$.
3. Si $\mathcal{K}$ es un cuerpo inclinado, entonces de $ab = 0$, se sigue que $a = 0 \vee b = 0$. (los cuerpos inclinados no tienen divisores de cero)

DEMOSTRACIÓN.

1. $0a+0a = (0+0)a = 0a = 0a+0 \quad \Rightarrow \quad 0a = 0$. Similarmente se demuestra $a0 = 0$.
2. $ab + (-a)b = (a + (-a))b = 0b = 0$. Entonces por la unicidad del inverso se tiene que $(-a)b = -(ab)$.
3. Supongamos que $ab = 0$ y $a \neq 0$, entonces

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

1.5.2 Ejemplos.

1. $\mathbb{Q}, \mathbb{R}$ son cuerpos con respecto a " $+$ " y " $\cdot$ ", sin embargo $\mathbb{Z}$ es solamente un anillo, por ejemplo: No existe $x \in \mathbb{Z}$ tal que $x \cdot 2 = 1$.
2. Sea $\mathcal{K} = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, con la multiplicación y la suma usual en $\mathbb{R}$, se verifica que $\mathcal{K}$ es un cuerpo.
3. Sea $n \in \mathbb{N}$ y definamos $\mathbb{F}_n := \mathbb{Z}/_{n\mathbb{Z}}$, el grupo cíclico de orden n, notado aditivamente. (ver ejemplos (1.3.3). Definamos sobre $\mathbb{F}_n$ la siguiente multiplicación

$$(a + n\mathbb{Z})(b + n\mathbb{Z}) := (ab) + n\mathbb{Z}.$$

   i Veamos que la multiplicación está bien definida:

   Supongamos que $a' = a + nk$ y $b' = b + nl$, entonces

   $$a'b' = (a + nk)(b + nl) = ab + n(al + bk + nkl) \in ab + n\mathbb{Z}.$$

   Entonces

   $$a'b' + n\mathbb{Z} = ab + n\mathbb{Z}.$$

   ii Todos los axiomas de cuerpo se verifican salvo la existencia de inversos multiplicativos. Esto es, se tiene que $\mathbb{F}_n$ es un anillo.

   iii Si $p = n$, p un número primo, entonces $\mathbb{F}_p$ es un cuerpo. (con p elementos).
   En efecto, $1 + p\mathbb{Z}$ es el módulo multiplicativo. $p\mathbb{Z}$ es el módulo aditivo. Sea ahora $a + p\mathbb{Z} \neq p\mathbb{Z}$, es decir $p \nmid a$. Se trata de encontrar $b \in \mathbb{Z}$ tal que

   $$(b + p\mathbb{Z})(a + p\mathbb{Z}) = ab + p\mathbb{Z} = 1 + p\mathbb{Z}.$$

Consideremos la función $\varphi : \mathbb{F}_p \to \mathbb{F}_p$ definida por:

$$\varphi(x + p\mathbb{Z}) = (x + p\mathbb{Z})(a + p\mathbb{Z}) = (xa) + p\mathbb{Z}.$$

- Con respecto a $+$ se verifica que φ es un homomorfismo:

$$\begin{aligned}\varphi((x + p\mathbb{Z}) + (y + p\mathbb{Z})) &= \varphi((x + y) + p\mathbb{Z}) \\ &= (x + y + p\mathbb{Z})(a + p\mathbb{Z}) \\ &= (x + y)a + p\mathbb{Z} \\ &= (ax + ya) + p\mathbb{Z} \\ &= (xa + p\mathbb{Z}) + (ya + p\mathbb{Z}) \\ &= \varphi(x + p\mathbb{Z}) + \varphi(y + p\mathbb{Z})\end{aligned}$$

- $Im(\varphi) = \mathbb{Z}/_{p\mathbb{Z}}$. Dado que $p \nmid a$, se tiene que

$$\varphi(1 + p\mathbb{Z}) = a + p\mathbb{Z} \neq p\mathbb{Z}$$

, del teorema de Lagrange se cumple que

$$2 < |Im(\varphi)| \mid |\mathbb{Z}/_{p\mathbb{Z}}| = p \quad \Rightarrow \quad |Im(\varphi)| = p,$$

por lo tanto

$$Im(\varphi) = \mathbb{Z}/_{p\mathbb{Z}}.$$

- De lo anterior se sigue que existe $b \in \mathbb{Z}$ con la condición deseada, ya que $1 + p\mathbb{Z} \in Im(\varphi)$.

Definición 40.

1. Sea $\mathcal{K}$ un cuerpo. Un subconjunto M de $\mathcal{K}$ se llama un subcuerpo de $\mathcal{K}$ si se verifica:
   (a) $0, 1 \in M$.
   (b) Si $k_1, k_2 \in M$, entonces $k_1 \pm k_2 \in M$.
   (c) Si $0 \neq k \in M$, entonces $k^{-1} \in M$.
2. Sean $\mathcal{K}$ y $\mathcal{L}$ cuerpos. Una función $\varphi : \mathcal{K} \to \mathcal{L}$ se llama homomorfismo de cuerpos si y solo si $\forall x, y \in \mathcal{K}$

$$\begin{aligned}\varphi(x + y) &= \varphi(x) + \varphi(y) \\ \varphi(xy) &= \varphi(x) \cdot \varphi(y)\end{aligned}$$

   Similar se define Monomorfismo, Epimorfismo e Isomorfismo.

1.5.3 Ejemplos.

1. Definamos $\mathbb{C} := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$.
   Definamos sobre $\mathbb{C}$ las siguientes operaciones:
   Suma

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} x & y \\ -y & x \end{pmatrix} := \begin{pmatrix} a + x & b + y \\ -(b + y) & a + x \end{pmatrix}$$

Multiplicación

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} x & y \\ -y & x \end{pmatrix} := \begin{pmatrix} ax-by & by+bx \\ -(bx+ay) & ax-by \end{pmatrix}$$

$\mathbb{C}$ es un cuerpo, $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ y $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

2. La función $\varphi : \mathbb{R} \to \mathbb{C}$ definida por

$$\varphi = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$$

Es un Isomorfismo de $\mathbb{R}$ en el subcuerpo T de $\mathbb{C}$ definido por

$$T = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R} \right\}.$$

3. Definamos $i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, entonces

$$i^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Sea $z \in \mathbb{C}$, digamos $z = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$, entonces

$$z = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} + i\begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} \qquad \text{(veriíquelo !).}$$

Entonces

$$\mathbb{C} = \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} + i\begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} : x, y \in \mathbb{R} \right\}.$$

Si utilizamos (2) y cada $x \in \mathbb{R}$ se identifica con $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ se tiene que

$$\mathbb{C} = \{x + iy : x, y \in \mathbb{R}\} \supseteq \mathbb{R}, \qquad i^2 = -1.$$

$\mathbb{C}$ se llama el cuerpo de los números complejos. Si $z = x + iy \in \mathbb{C}$, entonces x se llama la parte real de z , y se llama la parte imaginaria de z.

Notación: $x \in Re(z);\ y = im(z)$.

Si definimos $|z| := \sqrt{x^2 + y^2}$, llamaremos a $|z|$ el valor absoluto de z.

$$\overline{z} := x - iy$$

se llamará complejo conjugado con z.

Teorema 41.

Sean $z, z_1, z_2 \in \mathbb{C}$.

1. $Re(z_1 + z_2) = Re(z_1) + Re(z_2)$.
2. $Re(z) = \dfrac{z + \overline{z}}{2}$.
3. $im(z_1 + z_2) = im(z_1) + im(z_2)$.
4. $im(z) = \dfrac{z - \overline{z}}{2}$.
5. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}, \quad \overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}, \quad \overline{\overline{z}} = z$.
   Lo anterior indica que $\varphi : \mathbb{C} \to \mathbb{C}$ definida por $\varphi(z) = \overline{z}$ es un Isomorfismo tal que $\varphi^2 = I_{\mathbb{C}}$.
6. $|z|^2 = |\overline{z}|^2 = z\overline{z} = (Re(z))^2 + (im(z))^2$.
7. $|z_1 z_2| = |z_1||z_2|$.
8. $|Re(z)| \leq |z| \quad , \quad |im(z)| \leq |z|$.
9. $|z_1 + z_2| \leq |z_1| + |z_2|$ (Desigualdad del triángulo).

DEMOSTRACIÓN.

1-6. Se siguen inmediatamente de la definición.

7. $|z_1 z_2|^2 = (z_1 z_2)(\overline{z_1 z_2}) = (z_1 z_2)(\overline{z_1} \cdot \overline{z_2}) = (z_1 \overline{z_1})(z_2 \overline{z_2}) = |z_1|^2 |z_2|^2$

   Entonces
   $$|z_1 z_2| = |z_1||z_2|.$$

8. Sea $z = a + ib$, con $a, b \in \mathbb{R}$, entonces

   $$|z|^2 = a^2 + b^2 \geq a^2,$$

   luego
   $$|Re(z)| = |a| = \sqrt{a^2} \leq |z|.$$

   De manera similar se demuestra la otra parte.

9.
$$\begin{aligned} |z_1 + z_2|^2 &= (z_1 + z_2)(\overline{z_1 + z_2}) = (z_1 + z_2)(\overline{z_1} + \overline{z_2}) \\ &= z_1\overline{z_1} + z_1\overline{z_2} + z_2\overline{z_1} + z_2\overline{z_2} \\ &= |z_1|^2 + 2Re(z_1\overline{z_2}) + |z_2|^2 \\ &\leq |z_1|^2 + 2|z_1\overline{z_2}| + |z_2|^2 \\ &= |z_1|^2 + 2|z_1||z_2| + |z_2|^2 \\ &= (|z_1| + |z_2|)^2 \end{aligned}$$

   Por tanto $|z_1 + z_2| \leq |z_1| + |z_2|$.

1.5.4 Observación. Interpretación geométrica de los números complejos.
Supongamos $\mathcal{R}^2 = \mathcal{R} \times \mathcal{R}$ está definido un sistema cartesiano de coordenadas. asociemos a cada número complejo $z = x + iy$ un punto $(x, y) \in \mathcal{R}^2$ (ver Figura 1.1).

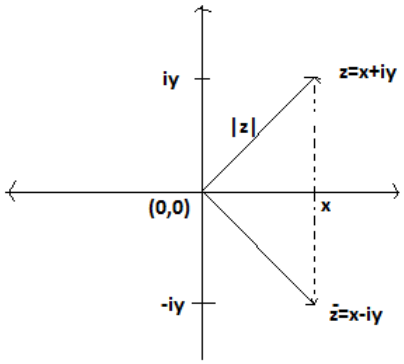


Figura 1.1: Plano complejo

Definición 42.

Sea $\mathcal{K}$ un cuerpo con módulo multiplicativo 1.
Si $n1 = \underbrace{1+1+\cdots+1}_{n\_sumandos} \neq 0$ para todo $n \in \mathbb{N}$, entonces diremos que $\mathcal{K}$ tiene característica 0. Si $n1 = 0$ y n es el número natural más pequeño con esta propiedad, entonces diremos que $\mathcal{K}$ tiene característica n.

Notación: $char(\mathcal{K}) = 0 \quad \vee \quad char(\mathcal{K}) = n.$

1.5.5 Ejemplos.

1. $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ tienen característica cero.
2. $\mathbb{F}_p$ (ver ejemplo (1.5.2)) tiene característica p.

   En efecto, Sea $m \in \mathbb{N}, \quad m \leq p$, entonces

$$\begin{aligned} m1 &= (1+p\mathbb{Z})\underbrace{+\cdots+}_{m}(1+p\mathbb{Z}) \\ &= m+p\mathbb{Z} = \begin{cases} \neq 0 & \text{para } m < p \\ = 0 & \text{para } m = p \end{cases} \end{aligned}$$

Teorema 43.

Si $\mathcal{K}$ es un cuerpo. Entonces $char(\mathcal{K}) = (0) \quad \vee \quad char(\mathcal{K}) = (p)$ donde p es un número primo.

DEMOSTRACIÓN. Supongamos que $\mathcal{K}$ es un cuerpo y $char(\mathcal{K}) \neq 0$.

1. $char(\mathcal{K}) = 1$: ya que de lo contrario se tendría $1 = 0$ (absurdo).

2. Supongamos que $char(\mathcal{K}) = m \cdot n$ con $m > 1, \quad n > 1, \quad m, n \in \mathbb{N}$. Entonces

$$0 = \underbrace{1 + \cdots + 1}_{mn-sumandos} = \underbrace{(1 + \cdots + 1)}_{m}\underbrace{(1 + \cdots + 1)}_{n}.$$

Entonces del teorema (39)(3) tendríamos que $\underbrace{(1 + \cdots + 1)}_{m} = 0 \quad \vee \quad \underbrace{(1 + \cdots + 1)}_{n} = 0$ lo cual contradice la definicón de característica, por lo tanto $char(\mathcal{K})$ es un número primo.

Capítulo 2

ESPACIOS VECTORIALES

2.1 Definiciones básicas y ejemplos.

Definición 44.

Sea $\mathcal{K}$ un cuerpo. Un subconjunto $\mathcal{V}$ se llama un espacio vectorial sobre $\mathcal{K}$ (o simplemente un $\mathcal{K}$-espacio vectorial) si los siguientes axiomas se verifican:

1. Sobre $\mathcal{V}$ está definida una operación binaria " $+$ " de tal forma que $\mathcal{V}$ es un grupo abeliano con respecto a esta.
   El módulo de $\mathcal{V}$ con respecto a $+$ se notará con 0 y generalmente es diferente del cero de $\mathcal{K}$.

2. Para cada $v \in \mathcal{V}$ y para todo $k \in \mathcal{K}$ está definido un elemento $kv \in \mathcal{V}$ (multiplicación por escalar) tal que:

   (a) Si 1 es el módulo multiplicativo de $\mathcal{K}$, entonces $1v = v$ para todo $v \in \mathcal{V}$.

   (b) $(k_1 + k_2)v = k_1v + k_2v \quad \forall k_1, k_2 \in \mathcal{K}, \quad \forall v \in \mathcal{V}$
   $(k_1k_2)v = k_1(k_2v) \quad \forall k_1, k_2 \in \mathcal{K}, \quad \forall v \in \mathcal{V}.$

   (c) $k(v_1 + v_2) = kv_1 + kv_2 \quad \forall k \in \mathcal{K}, \quad \forall v_1, v_2 \in \mathcal{V}$

2.1.1 Observación. Si en la definición (44) asumimos que $\mathcal{K}$ sea simplemente un anillo, entonces diremos que $\mathcal{V}$ es un $\mathcal{K}$-módulo izquierdo o un módulo izquierdo sobre $\mathcal{K}$

2.1.2 Ejemplos.

1. Sea $\mathcal{K}$ un cuerpo y $\mathcal{V}$ un conjunto con un solo elemento, digamos $\mathcal{V} = \{0\}$. Definamos sobre $\mathcal{V}$ una suma $0 + 0 = 0$, y definamos una multiplicación por escalar así: $k0 = 0 \quad \forall k \in \mathcal{K}$. $\mathcal{V}$ es un espacio vectorial sobre $\mathcal{K}$. (El espacio vetorial nulo).

2. Sea $\mathcal{K}$ un cuerpo. $\mathcal{V} := \mathcal{K}^n = \{(x_1, ..., x_n : x_i \in \mathcal{K}\}$. $\mathcal{V}$ es un espacio vectorial sobre $\mathcal{K}$ con las siguientes operaciones:

$$(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 + y_1, ..., x_n + y_n)$$
$$k(x_1, ..., x_n) = (kx_1, ..., kx_n).$$

$k \in \mathcal{K}, \quad (x_1, ..., x_n), (y_1, ..., y_n) \in \mathcal{V}$. El cero de $\mathcal{V}$ es $(0, ..., 0)$. Usualmente $\mathcal{V}$ es denominado el espacio vectorial de las n-tuplas sobre $\mathcal{K}$.

3. Sea $\mathcal{K}$ un cuerpo y $\mathcal{L}$ un subcuerpo $\mathcal{K}$. Entonces $\mathcal{K}$ es un espacio vectorial sobre $\mathcal{L}$. La multiplicación por escalar: $l \in \mathcal{L}, k \in \mathcal{K} \quad lk \in \mathcal{K}$.
Ejemplo, $\mathbb{C}$ es un $\mathbb{Q}$-espacio vectorial, un $\mathbb{R}$-espacio vectorial.

4. Sea M un conjunto no vacío y $\mathcal{K}$ un cuerpo, definamos

$$\mathcal{V} = \mathcal{V}(M, \mathcal{K}) = \{f : M \to \mathcal{K} : f \text{es una función}\}.$$

$\mathcal{V}$ es un espacio vectorial sobre $\mathcal{K}$ con las siguientes operaciones:

$$(f + g)(x) := f(x) + g(x) \quad \forall x \in M$$
$$(kf)(x) := kf(x) \quad \forall x \in M$$

$k \in \mathcal{K}, \quad f, g \in \mathcal{V}$.

5. $\mathcal{V} = C([0, 1], \mathbb{R}) = \{f : [0, 1] \to \mathbb{R} : f \text{es continua}\}$ con las operaciones definidas en (4) se demuestra que $\mathcal{V}$ es un espacio vectorial real (sobre $\mathbb{R}$).

Teorema 45.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$ y sean $k \in \mathcal{K}, \quad v \in \mathcal{V}$, entonces

1. $0 \cdot v = 0 \quad \forall v \in \mathcal{V} \quad (0 \in \mathcal{K})$.
2. $k \cdot 0 = 0 \quad \forall k \in \mathcal{K} \quad (0 \in \mathcal{V})$.
3. $(-k)v = k(-v) = -(kv)$.
4. Si $kv = 0$, entonces $k = 0 \quad \vee \quad v = 0$.

DEMOSTRACIÓN.

1. Se cumple que:

$$0v + 0v = (0 + 0)v = 0v = 0v + 0 \quad \Rightarrow \quad 0v = 0.$$

2. Similarmente:

$$k0 + k0 = k(0 + 0) = k0 = k0 + 0 \quad \Rightarrow \quad k0 = 0.$$

3. $kv + (-k)v = (k + (-k))v = 0v = 0 \quad \Rightarrow \quad (-k)v = -(kv)$
$kv + k(-v) = k(v + (-v)) = k0 = 0 \quad \Rightarrow \quad k(-v) = -(kv)$.

4. Supongamos que $kv = 0$ y $k \neq 0$, entonces existe

$$k^{-1} \in \mathcal{K}.$$

se tiene que:

$$0 = k^{-1}0 = k^{-1}(kv) = (k^{-1}k)v = 1v = v.$$

2.2 Subespacios

Definición 46.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$. Un subconjunto no vacío $\mathcal{U}$ de $\mathcal{V}$ se llama un subespacio de $\mathcal{V}$, notado $\mathcal{U} \ll \mathcal{V}$ si se cumple:

1. Si $u_1, u_2 \in \mathcal{U}$, entonces $u_1 \pm u_2 \in \mathcal{U}$.
2. Si $u \in \mathcal{U}$ y $k \in \mathcal{K}$, entonces $ku \in \mathcal{U}$.

Es claro que $\mathcal{U}$ con las operaciones definidas sobre $\mathcal{V}$ es en sí un espacio vectorial sobre $\mathcal{K}$.

2.2.1 Ejemplos.

1. Si $\mathcal{V}$ es un espacio vectorial sobre $\mathcal{K}$, entonces $\mathcal{V}$ y $\{0\}$ son subespacios de $\mathcal{V}$.
2. Sea $\mathcal{V} = \mathcal{V}(\mathbb{R}, \mathbb{R}) = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$ (ver ejemplo (2.1.2)(4)).

   $\mathcal{U}_1 = \{f \in \mathcal{V} : f \text{es continua}\}$ es un subespacio de $\mathcal{V}$. Usualmente se escribe

   $$\mathcal{U}_1 = C(\mathbb{R}).$$

   $\mathcal{U}_2 = \{f \in \mathcal{V} : \exists a_j \in \mathbb{R} \ \wedge \ \exists m \in \mathbb{N} \cup \{0\} | f(x) = \sum_{j=0}^{m} a_j x^j \quad \forall x \in \mathbb{R}\}$ es también un subespacio de $\mathcal{V}$.

   Notación: $\mathcal{U}_2 = P(\mathbb{R})$.
3. Sea $\mathcal{V} = \mathbb{R}^3$ y sean $a, b, c \in \mathbb{R}$, definamos

   $$\mathcal{U} = \{(x, y, z) : x, y, z \in \mathbb{R}, \quad ax + by + cz = 0\}$$

   se verifica que $\mathcal{U}$ es un subespacio de $\mathcal{V}$.

Teorema 47.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$

1. Si $\{\mathcal{U}_i\}_{i \in I}$ es una familia de subespacios de $\mathcal{V}$, entonces $D := \bigcap_{i \in I} \mathcal{U}_i$ es un subespacio de $\mathcal{V}$.
2. Sea $\mathcal{U}_1, \mathcal{U}_2$ subespacios de $\mathcal{V}$. $\mathcal{U}_1 \cup \mathcal{U}_2$ es un subespacio de $\mathcal{V}$ si y solo si $\mathcal{U}_1 \subseteq \mathcal{U}_2 \quad \vee \quad \mathcal{U}_2 \subseteq \mathcal{U}_1$.

DEMOSTRACIÓN. La demostración es similar al teorema (10).

Definición 48.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$.

1. Sea $\mathcal{M} \subseteq \mathcal{V}$, definamos

$$\langle \mathcal{M} \rangle := \bigcap_{\mathcal{M} \subseteq \mathcal{U} \ll \mathcal{V}} \mathcal{U}.$$

   Llamaremos a $\langle \mathcal{M} \rangle$ el subespacio generado por $\mathcal{M}$. Es claro que $\langle \mathcal{M} \rangle$ es el subespacio vectorial de $\mathcal{V}$ mas pequeño con la propiedad **contener a** $\mathcal{M}$.

2. Si $\mathcal{M} \subseteq \mathcal{V}$ con la propiedad $\mathcal{V} = \langle \mathcal{M} \rangle$, entonces diremos que $\mathcal{M}$ es un sistema de generadores de $\mathcal{V}$.

3. Sean $\mathcal{M}_1, \mathcal{M}_2, ..., \mathcal{M}_k$ subconjuntos de $\mathcal{V}$, definamos

$$\underbrace{\mathcal{M}_1 + \mathcal{M}_2 + \cdots + \mathcal{M}_k}_{= \sum_{j=1}^{k} \mathcal{M}_j} = \{\underbrace{m_1 + m_2 + \cdots + m_k}_{= \sum_{j=1}^{k} m_j} : m_j \in \mathcal{M}_j\}.$$

   (Esto es en notación aditiva análogo a la definición de AB para subconjuntos A, B de un grupo $\mathbf{G}$).

Teorema 49.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$.

1. Si $\mathcal{M} \subseteq \mathcal{V}$, entonces $\langle \mathcal{M} \rangle = \{\sum_{i=1}^{n} \alpha_i x_i : \alpha_i \in \mathcal{K}, x_i \in \mathcal{M}, n \in \mathbb{N}\}$.

2. Sean $\mathcal{U}_1, \mathcal{U}_2, ..., \mathcal{U}_k$ subespacios vectoriales de $\mathcal{V}$, entonces

$$\langle \mathcal{U}_1 \cup \cdots \cup \mathcal{U}_k \rangle = \sum_{j=1}^{k} \mathcal{U}_j.$$

DEMOSTRACIÓN.

1. Similar a la de grupos.

2. Demostremos inicialmente que $\sum_{j=1}^{k} \mathcal{U}_j$ es un subespacio de $\mathcal{V}$.

   Sean $x, y \in \sum_{j=1}^{k} \mathcal{U}_j$. Entonces existen $u_j, v_j \in \mathcal{U}_j$ tales que

   $x = \sum_{j=1}^{k} u_j, \quad y = \sum_{j=1}^{k} v_j$. Sea ahora $\alpha \in \mathcal{K}$, entonces

   $x + y = \sum_{j=1}^{k} (u_j + v_j) \in \sum_{j=1}^{k} \mathcal{U}_j$ (ya que cada $\mathcal{U}_j$ es subespacio de $\mathcal{V}$).

$\alpha x = \sum_{j=1}^{k} \alpha u_j \in \sum_{j=1}^{k} \mathcal{U}_j$.

Evidentemente $\bigcup_{j=1}^{k} \mathcal{U}_j \subseteq \sum_{j=1}^{k} \mathcal{U}_j$ ya que cada $\mathcal{U}_j \subseteq \sum_{j=1}^{k} \mathcal{U}_j \ \forall i \in \{1, ..., k\}$, entonces $\langle \bigcup_{j=1}^{k} \mathcal{U}_j \rangle \subseteq \sum_{j=1}^{k} \mathcal{U}_j$.

La otra inclusión se deja como ejercicio.

Definición 50.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$. Diremos que $\mathcal{V}$ es finitamente generado, si existe un subconjunto finito $\mathcal{M} = \{v_1, ..., v_m\}$ de $\mathcal{V}$ tal que $\mathcal{V} = \langle \mathcal{M} \rangle$. Esto es

$$\mathcal{V} = \{\sum_{i=1}^{k} \alpha_i v_i : \alpha_i \in \mathcal{K}\}.$$

2.2.2 Ejemplos. Sea $\mathcal{K}$ un cuerpo.

1. Sea $\mathcal{V} = \mathcal{K}^n$. Definamos $v_j = (0, ..., 0, 1, 0, ..., 0)$ para $j = 1, 2, ..., n$, entonces $\sum_{j=1}^{k} \alpha_j v_j = (\alpha_1, ..., \alpha_n)$ y se tiene que $\mathcal{V} = \langle v_1, ..., v_n \rangle$ y por lo tanto $\mathcal{V}$ es finitamente generado.

2. Sea $v = P(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} : \exists a_j \in \mathbb{R} \quad y \quad m \in \mathbb{N} \cup \{0\} | f(x) = \sum_{j=1}^{m} a_j x^j \quad \forall x \in \mathbb{R}\}$.

   Demostremos que $P(\mathbb{R})$ no es finitamente generado. Supongamos que $P(\mathbb{R}) = \langle f_1, ..., f_m \rangle$ con $f_j \in P(\mathbb{R})$.

   Sea $f_j(x) = \sum_{k=0}^{n_j} a_{jk} x^k \quad \forall x \in \mathbb{R}$ con $a_{jk} \in \mathbb{R}$.

   Sea $n := \underbrace{max}_{j \in \{1,...,m\}} \{n_j\}$

   Sea $f \in P(\mathbb{R})$, tal que $f(x) = x^{n+1} \quad \forall x \in \mathbb{R}$. Por otro lado $f = \sum_{j=1}^{m} b_j f_j$ (ya que $\mathcal{V} = \langle f_1, ..., f_m \rangle$), es decir

   $$x^{n+1} = \sum_{j=1}^{m} b_j f_j(x).$$

   Derivando $(n+1)$-veces tenemos:

   $(n+1)n \cdots 2 \cdot 1 = \sum_{j=1}^{m} b_j f_j^{n+1}(x) = 0$. (contradicción).

Teorema 51.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$ y $\mathcal{U}$ un subespacio de $\mathcal{V}$. Dado que $\mathcal{V}$ con respecto a la suma es abeliano se tiene que $\mathcal{U}$ es un subgrupo normal de $\mathcal{V}$. Podemos entonces formar el grupo cociente

$$\mathcal{V}/\mathcal{U} = \{v + \mathcal{U} : v \in \mathcal{V}\}$$

Definamos: (suma)

$$(v_1 + \mathcal{U}) + (v_2 + \mathcal{U}) := (v_1 + v_2) + \mathcal{U}, \quad v_1, v_2 \in \mathcal{V}$$

(Mult. por escalar)

$$k(v + \mathcal{U}) := (kv) + \mathcal{U} \quad k \in \mathcal{K}, v \in \mathcal{V}.$$

Entonces $\mathcal{V}/\mathcal{U}$ es un espacio vectorial sobre $\mathcal{K}$, el cual llamaremos el espacio factor de $\mathcal{V}$ con respecto a $\mathcal{U}$.

DEMOSTRACIÓN.

1. Similar como en grupos se cumple la siguiente afirmación:

$$u + \mathcal{U} = \mathcal{U} \quad \Leftrightarrow \quad u \in \mathcal{U} \quad \text{(Ejercicio)}.$$

2. Demostramos ahora:

$$v + \mathcal{U} = v' + \mathcal{U} \quad \Leftrightarrow \quad (v - v') \in \mathcal{U} \qquad v, v' \in \mathcal{V}$$

   $\Rightarrow$: Supongamos que $v + \mathcal{U} = v' + \mathcal{U}$, entonces $v = v + 0 \in v + \mathcal{U} = v' + \mathcal{U}$ entonces existe $u \in \mathcal{U}$ tal que $v = v' + u \quad \Rightarrow \quad v - v' = u \in \mathcal{U}$.
   $\Leftarrow$: Supongamos que $v - v' \in \mathcal{U}$ entonces $v - v' = u$ para algún $u \in \mathcal{U}$, entonces

$$v + \mathcal{U} = (v' + u) + \mathcal{U} = v' + (u + \mathcal{U}) = v' + \mathcal{U}.$$

3. Demostremos a continuación que las operaciones están bien definidas:
   Suma: Supongamos que $v + \mathcal{U} = v' + \mathcal{U}$ y $w + \mathcal{U} = w' + \mathcal{U}$, entonces $v - v' \in \mathcal{U} \quad \wedge \quad w - w' \in \mathcal{U}$, por lo tanto

$$(v - v') + (w + w') = (v + w) - (v' + w') \in \mathcal{U} \quad \Rightarrow \quad (v + w) + \mathcal{U} = (v' + w') + \mathcal{U}$$

   Mult. por escalar: Sea $k \in \mathcal{K}$. Entonces si $v + \mathcal{U} = v' + \mathcal{U}$ se tiene que $v - v' \in \mathcal{U}$ y por lo tanto $kv - kv' \in \mathcal{U} \quad \Rightarrow \quad kv + \mathcal{U} = kv' + \mathcal{U}$.

4. El resto de los axiomas se deja como ejercicio.

2.2.3 Ejemplo.

$$\begin{aligned} k((v + \mathcal{U}) + (v' + \mathcal{U})) &= k((v + v') + \mathcal{U}) \\ &= k(v + v') + \mathcal{U} \\ &= (kv + kv') + \mathcal{U} \\ &= (kv + \mathcal{U}) + (kv' + \mathcal{U}) \\ &= k(v + \mathcal{U}) + k(v' + \mathcal{U}) \end{aligned}$$

2.3 Dependencia e independencia lineal

Definición 52.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$ y sea $(v_i : i \in I)$ un sistema de vectores de $\mathcal{V}$, es decir

$$(v_i : i \in I) \in \underbrace{\times}_{i \in I} v_i, \quad \text{donde} \quad v_i = \mathcal{V}.$$

Diremos $(v_i : i \in I)$ es linealmente independiente, si $v_k \notin \langle v_i : i \in I \setminus \{k\}\rangle$ para todo $k \in I$.

Si $(v_i : i \in I)$ no es linealmente independiente, entonces diremos que $(v_i : i \in I)$ es linealmente dependiente.

2.3.1 Observación. Si $v \in \mathcal{V}$ y se cumple que $v \in \langle v_i : i \in I\rangle$, entonces diremos que v es una combinación lineal de los $(v_i : i \in I)$, entonces tenemos $(v_i : i \in I)$ es linealemente independiente si y solo si v_k no es combinación lineal de los elementos del sistema $(v_i : i \in I \setminus \{k\})$ para todo $k \in I$.

Notas:

1. Si $(v_i : i \in I)$ es un sistema de vectores de $\mathcal{V}$ tal que $v_j = 0$ para algún $j \in I$, entonces $(v_i : i \in I)$ es linealmente dependiente

   $$0 = v_j \in \langle v_i : i \in I \setminus \{j\}\rangle.$$

   ($\langle v_i : i \in I \setminus \{j\}\rangle$ es un subespacio de $\mathcal{V}$ y continua $\{0\}$).

2. Si existen $k, j \in I$ tal que $v_k = v_j$ y $k \neq j$, entonces $(v_i : i \in I)$ es linealmente dependiente.

   $$v_j = v_k \in \langle v_i : i \in I \setminus \{j\}\rangle.$$

Lema 53.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$ y sea $(v_i : i \in I)$ un sistema de $\mathcal{V}$, son equivalentes:

1. $(v_i : i \in I)$ es linealmente dependiente.
2. Existe un subconjunto finito J de I y un $i \in I \setminus J$ tal que

   $$v_i = \sum_{j \in J} k_j v_j \text{ con } k_j \in \mathcal{K}.$$

3. Existe un subconjunto finito L de I y $k_l \in \mathcal{K}$ para $l \in L$ no todos los $k_l = 0$ con

   $$\sum_{i \in L} k_l v_l = 0.$$

   (Esto es, cero es una combinación lineal no trivial de los elementos del sistema $(v_i : i \in I)$).

DEMOSTRACIÓN.

1⇒2 : Por hipótesis existe $i \in I$ tal que $v_i \in \langle v_j : j \in I \setminus \{i\}\rangle$, del teorema (49)(1) se tiene

$$v_i = \sum_{j\in J} k_j v_j \text{ con } k_j \in \mathcal{K} \text{ y } J \subseteq I \setminus \{i\}, J\text{finito.}$$

2⇒3. La igualdad en (2) se puede escribir de la siguiente manera:

$$1 \cdot v_i + \sum_{j\in J}(-k_j)v_j.$$

Tómese entonces $L = J \cup \{i\}$.

3⇒1. Supongamos que $\sum_{l\in L} k_l v_l = 0$ y no todos los k_l son cero, $L \subset I$, L finito. Sea $k_s \neq 0$ con $s \in L$. entonces

$$v_s = -\sum_{l\in L\setminus\{s\}} (k_s^{-1}k_l)v_l \in \langle v_l | l \in L \setminus \{s\}\rangle \subseteq \langle v_i | i \in I \setminus \{s\}\rangle.$$

Entonces $(v_i : i \in I)$ es linealmente dependiente.

Lema 54.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$ y sea $(v_i : i \in I)$ un sistema de vectores de $\mathcal{V}$. Son equivalentes

1. $(v_i : i \in I)$ es linealmente independiente.
2. Si $J \subseteq I$, J finito, $k_j \in \mathcal{K} \quad j \in J$ con $\sum_{j\in J} k_j v_j = 0$ entonces se verifica que $k_j = 0 \quad \forall j \in J$.

DEMOSTRACIÓN. Se sigue inmediatamente del lema anterior $1 \Leftrightarrow 3$.

2.3.2 Ejemplos.

1. Sea nuevamente $\mathcal{V} = \mathbb{K}^n$, v_j como en (2.2.2)(1), entonces $(v_1, ..., v_n)$ es linealmente independiente. En efecto, sea

$$(0, ..., 0) = \sum_{j=1}^{n} k_j v_j = (k_1, ..., k_n).$$

Esta igualdad se verifica si y solo si $k_i = 0 \quad \forall i = 1, 2, ..., n$, entonces $(v_j : i \in \{1, ..., n\})$ es linealmente independiente.

2. Sea nuevamente $\mathcal{V} = P(\mathbb{R})$ y sean $v_j \in P(\mathbb{R})$ definidas por $v_j(x) = x^j \quad \forall x \in \mathbb{R}, \quad j = 0, 1, 2, ...$
Entonces $(v_j : j \in \mathbb{N})$ es linealmente independiente.
Supongamos que $\sum_{j=0}^{n} k_j v_j = 0$, es decir $\sum_{j=0}^{n} k_j v_j(x) = 0 \quad \forall x \in \mathbb{R}$ (para algún $n \in \mathbb{N}$, con $k_n \neq 0$) o también $\sum_{j=0}^{n} k_j x^j = 0 \quad \forall x \in \mathbb{R}$ (para algún $n \in \mathbb{N}$, con $k_n \neq 0$), entonces derivando n-veces tenemos

$$0 = n!k_n \neq 0 \qquad \text{(contradicción).}$$

la conclusión se sigue del lema (54).

2.4 Base y dimensión.

Definición 55.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$. Un sistema $\mathfrak{B} = (v_i : i \in I)$ se llama una base para $\mathcal{V}$, si y solo si $\mathfrak{B}$ es linealmente independiente y $\mathcal{V} = \langle v_i : i \in I \rangle$.

2.4.1 Ejemplos. .

1. Sea $\mathcal{V} = \mathcal{K}^n$, entonces $\mathfrak{B} = (v_1, ..., v_2)$; $\quad v_j = (0, ..., 0, 1, 0, ..., 0)$. $j = 1, 2, ..., n$. Es una base para $\mathcal{V}$.
   (se sigue de los ejemplos (2.2.2)(1) y (2.3.2)(1)).
2. Es $(v_j : j \in \mathbb{N})$ es una base para $P(\mathbb{R})$? $v_j(x) = x^i \quad \forall x \in \mathbb{R}, j \in \mathbb{N}$

Teorema 56.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$. y $\mathfrak{B} = (v_i : i \in I)$ Un sistema de $\mathcal{V}$. Son equivalentes

1. $\mathfrak{B}$ es una base para $\mathcal{V}$.
2. $\mathfrak{B}$ un sistema linealmente independiente, pero $\forall v \in \mathcal{V}$ el sistema $(v_i, v : i \in I)$ es linealmente dependiente.
   (Esto es, $\mathfrak{B}$ es un sistema maximal linealmente independiente).
3. Se cumple que $\mathcal{V} = \langle v_i : i \in I \rangle$ pero $\langle v_i : i \in J \rangle \subset \mathcal{V}$ para todo subconjunto propio J de I.
   (Esto es, $\mathfrak{B}$ es un sistema minimal de generadores).

DEMOSTRACIÓN..

1⇒2. Por definición de base, se tiene que $\mathfrak{B}$ es linealmente independiente. Sea $v \in \mathcal{V}$, entonces se cumple:
$v \in \mathcal{V} = \langle v_i : i \in I \rangle \quad \Rightarrow \quad (v_i, v : i \in I)$ es linealmente dependiente.

2⇒3. Demostremos inicialmente que $\mathcal{V} = \langle v_i : i \in I \rangle$. Sea $v \in \mathcal{V}$, (cualquiera), por hipótesis $(v_i, v : i \in I)$ es linealmente dependiente, del lema (53) se sigue que existe un subconjunto finito J de I y además existen $k, k_j \in \mathcal{K}$ no todos ceros tales que

$$kv + \sum_{j \in J} k_j v_j = 0$$

Supongamos que $k = 0$. Dado que $J \subseteq I$, se cumple que $(v_i : i \in J)$ es también linealmente independiente y por lo tanto $k_j = 0 \quad \forall j \in J$ (absurdo). Entonces $k \neq 0$ y con esto tenemos

$$v = \sum_{j\in J}(k^{-1}k_j)v_j \in \langle v_i : i \in I\rangle.$$

Entonces $\mathcal{V} = \langle v_i : i \in I\rangle$.
Demostremos ahora que si $J \subseteq I$, entonces $\langle v_j : j \in J\rangle \subset \mathcal{V}$. Supongamos que $\mathcal{V} = \langle v_j : j \in J\rangle$. Sea $i \in I \setminus J$, entonces

$$v_i \in \mathcal{V} = \langle v_j : j \in J\rangle \subseteq \langle v_k : k \in I \setminus \{i\}\rangle \quad \text{(absurdo)}$$

ya que $(v_i : i \in I)$ es linealmente independiente.

3⇒1. Solo falta demostrar la independencia lineal del sistema $(v_i : i \in I)$.
Supongamos que no lo es, entonces existe por lema (53) un subconjunto finito $J \subseteq I$ y $k_j \in \mathcal{K}$, $j \in J$, no todos los $k_j = 0$ tales que

$$\sum_{j\in J} k_j v_j = 0.$$

Sea $j_0 \in J$ tal que $k_{j_0} \neq 0$, entonces $v_{j_0} = -\sum_{j\in J\setminus\{j_0\}} k_{j_0}^{-1}k_j v_j$. Es decir $v_{j_0} \in \langle v_i : i \in I \setminus \{j_0\}\rangle$.
Sea ahora $v \in \mathcal{V}$ (arbitrario), dado que $\mathcal{V} = \langle v_i : i \in I\rangle$ se tiene otra vez que existe un conjunto finito $\hat{J}$ con $\hat{J} \subseteq I$ y existen $a_j \in \mathcal{K}$, $\quad j \in \hat{J}$ tales que

$$v = \sum_{j\in\hat{J}} a_j v_j.$$

Diferenciamos ahora dos casos:
Caso 1: $j_0 \notin \hat{J}$. Entonces $v \in \langle v_i : i \in I \setminus \{j_0\}\rangle$.

Caso 2: $j_0 \in \hat{J}$, entonces se tiene:

$$v = a_{j_0}v_{j_0} + \sum_{j\in\hat{J}\setminus\{j_0\}} a_j v_j = a_{j_0}(-\sum_{j\in J\setminus\{j_0\}} k_{j_0}^{-1}k_j v_j) + \sum_{j\in\hat{J}\setminus\{j_0\}} a_j v_j.$$

Es decir obtenemos que $v \in \langle v_i : i \in I \setminus \{j_0\}\rangle$, por lo tanto

$$\mathcal{V} = \langle v_i : i \in I \setminus \{j_0\}\rangle = \langle v_i : i \in I\rangle.$$

Lo cual contradice la hipótesis (3).

Dado un espacio vectorial $\mathcal{V}$ sobre $\mathcal{K}$. ¿Existe siempre una base para $\mathcal{V}$? Hasta el momento nada hemos dicho sobre el particular. Demostremos ahora que para el caso en que $\mathcal{V}$ sea finitamente generado la respuesta es sí, y la demostración es inmediata. Demostremos también que en general la respuesta es afirmativa.

Teorema 57.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$, finitamente generado, digamos $\mathcal{V} = \langle\mathcal{M}\rangle$ con $|\mathcal{M}| < \infty$. Entonces existe una base $\mathfrak{B} = (v_1, ..., v_r)$ para $\mathcal{V}$ con $\{v_1, ..., v_r\} \subseteq \mathcal{M}$. En particular $r \leq |\mathcal{M}|$.

DEMOSTRACIÓN. Definamos $\chi := \{N : N \subseteq \mathcal{M}, \mathcal{V} = \langle N \rangle\}$. Dado que $\mathcal{M} \in \chi$ se tiene que χ no es vacío. Elijamos en χ un elemento v' con la condición que $|N|$ sea minimal, esto es $N' = \{v_1, ..., v_r\}$ con r minimal. Entonces,

$$\langle v_i : i \in \underbrace{\{1, ..., r\}}_{i \neq j} \rangle \neq \mathcal{V}$$

para todo $j \in \{1, 2, ..., r\}$. Es decir, N' es un sistema minimal de generadores para $\mathcal{V}$ y $\mathfrak{B} := (v_1, ..., v_r)$ es una base para $\mathcal{V}$.

Teorema 58.

Sea $(v_i : i \in I)$ una base del espacio vectorial $\mathcal{V}$ sobre un cuerpo $\mathcal{K}$.

1. $\forall v \in \mathcal{V}$ existe un subconjunto finito J de I y $k_j \in \mathcal{K}, j \in J$ tales que $v = \sum_{j \in J} k_j v_j$.
2. Si $\sum_{i \in I} k_i v_i = \sum_{i \in I} k_i' v_i$ con $k_i, k_i' \in \mathcal{K}$ y solo un número finito de estos distintos de cero, entonces se cumple que $k_i = k_i'$ para todo $i \in I$.

DEMOSTRACIÓN..

1. Es consecuencia de $\mathcal{V} = \langle v_i : i \in I \rangle$.
2. Se sigue de la independencia lineal de $(v_i : i \in I)$

Lema 59.

Sea $\mathfrak{B} = (v_1, ..., v_n)$ una base para $\mathcal{V}$ y sea $v \in \mathcal{V}$ tal que $v = \sum_{j=1}^{n} k_j v_j$ y $k_1 \neq 0$. entonces $(v, v_2, ..., v_n)$ también es una base para $\mathcal{V}$.

DEMOSTRACIÓN.
Dado que $k_1 \neq 0$, tenemos que

$$v_1 = k_1^{-1}(v - \sum_{j=2}^{n} k_j v_j) \in \langle v, v_2, ..., v_n \rangle.$$

Entonces,

$$\mathcal{V} = \langle v_1, v_2, ..., v_n \rangle = \langle v, v_2, ..., v_n \rangle.$$

Para demostrar que $(v, v_2, ..., v_n)$ es linealmente independiente, sea

$$av + \sum_{j=2}^{n} a_j v_j = 0 \text{ con } a, a_j \in \mathcal{K}$$

Entonces

$$0 = a(\sum_{j=1}^{n} k_j v_j) + \sum_{j=2}^{n} a_j v_j,$$

luego

$$0 = ak_1v_1 + \sum_{j=2}^{n}(ak_j + a_j)v_j$$

pero $(v_1, ..., v_n)$ es una base, por lo tanto es linealmente independiente, entonces $ak_1 = ak_j + a_j = 0 \quad \forall j = 2, 3, ..., n$.
Por otro lado $k_1 \neq 0$, entonces $a = 0$ y por lo tanto $a_j = 0 \quad \forall j \in \{2, ..., n\}$.

2.4.2 Observación. El resultado es el mismo si en lugar de k_1 se toma cualquier $k_j \neq 0$.

Teorema 60 (Steinnitz (1817-1928)).

Sea $\mathfrak{B} = (v_1, ..., v_n)$ una base para $\mathcal{V}$. Sea $(w_1, ..., w_m)$ un sistema linealmente independiente de $\mathcal{V}$, entonces $m \leq n$ y existen $v'_1, ..., v'_{n-m} \in \{v_1, ..., v_n\}$ tal que $(w_1, ..., w_m, v'_1, ..., v'_{n-m})$ es una base para $\mathcal{V}$.

DEMOSTRACIÓN. (Inducción sobre m).
$m = 1$**:** Dado que (w_i) es linealmente independiente, se tiene que $w_1 \neq 0$. Por lo tanto $\mathcal{V} \neq \{0\}$ y $\mathcal{V} \neq \phi$. Entonces $n \geq 1 = m$.
Dado que $\mathfrak{B}$ es una base para $\mathcal{V}$ se tiene que

$$w_1 = \sum_{j=1}^{n} k_j v_j \qquad k_j \in \mathcal{K}$$

Como $w_1 \neq 0$, entonces existe $k_j \neq 0$. Del lema (59) se sigue que
$(w_1, v_1, ..., v_{j-1}, v_{j+1}, ..., v_n)$ es una base para $\mathcal{V}$.

Sea $m > 1$ $(m - 1 \Rightarrow m)$**:** Sea $(w_1, ..., w_m)$ un sistema linealmente independiente. Por la hipótesis de inducción $m - 1 \leq n$ y existe una base para $\mathcal{V}$ que tiene la forma $(w_1, ..., w_{m-1}, v'_1, ..., v'_{n-m+1})$ con $v'_i \in \mathfrak{B}$. Demostremos que $m \leq n$. Supongamos que no es cierto. Entonces dado que $m - 1 \leq n$ se tiene que $m - 1 = n$ y $(w_1, ..., w_{m-1})$ es una base para $\mathcal{V}$. En particular se tiene que

$$w_m \in \langle w_1, ..., w_{m-1} \rangle$$

Lo cual contradice el hecho de que $(w_1, ..., w_m)$ un sistema linealmente independiente. entonces $m \leq n$ y existen $c_i, d_i \in \mathcal{K}$ tal que

$$w_m = c_1w_1 + ... + c_{m-1}w_{m-1} + d_1v'_1 + ... + d_{n-m+1}v'_{n-m+1}.$$

Si $d_1 = ... = d_{n-m+1} = 0$, entonces $(w_1, ..., w_m)$ sería linealmente independiente (absurdo). Entonces por lo menos un $d_j \neq 0$. Sin perder generalidad supongamos que $d_{n-m+1} \neq 0$, entonces $(w_1, ..., w_m v'_1, ..., v'_{n-m})$ es una base para $\mathcal{V}$.

Teorema 61.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$, finitamente generado. Entonces $\mathcal{V}$ tiene una base $(v_1, ..., v_n)$ y todas las bases de $\mathcal{V}$ tienen exactamente n elementos.

DEMOSTRACIÓN. La existencia de una base para $\mathcal{V}$ fue demostrada en el teorema (57) digamos $\mathfrak{B} = (v_1, ..., v_n)$. Sea $\mathfrak{B}' = (w_i : i \in I)$ otra base para $\mathcal{V}$. Si $|I| \geq n+1$, entonces existiría en $\mathcal{V}$ un sistema linealmente independiente $(w_1, ..., w_{n+1})$ lo cual contradice el teorema (60). Entonces $|I| \leq n$, y por tanto I es finito. Utilizando otra del teorema (60) con el cambio de los papeles entre $\mathfrak{B}$ y $\mathfrak{B}'$ se tendría que $n \leq |I|$ luego $n = |I|$.

Definición 62.

1. Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$, finitamente generado. Definamos la dimensión de $\mathcal{V}$ sobre $\mathcal{K}$ así: $dim_k\mathcal{V}$:= al número de elementos de una base para $\mathcal{V}$.
2. Si $\mathcal{V}$ no es finitamente generado, entonces definimos $dim_k\mathcal{V} = \infty$.
3. Si $\mathcal{V} = \{0\}$, se define $dim_k\mathcal{V} = 0$.

2.4.3 Ejemplos.

1. $dim_k\mathcal{K}^n = n$.
2. $dim_{\mathbb{R}}P(\mathbb{R}) = \infty$.
3. $dim_{\mathbb{R}}C^1([0,1],\mathbb{R}) = \infty$.

Teorema 63.

Sea $dim_k\mathcal{V} < \infty$ y sea $\mathcal{U} \ll \mathcal{V}$.

1. $dim_k\mathcal{U} < \infty$.
2. $dim_k\mathcal{V}/\mathcal{U} < \infty$.
3. Si $(u_1, ..., u_m)$ es una base para $\mathcal{U}$ y $(w_1 + \mathcal{U}, ..., w_k + \mathcal{U})$ es una base para $\mathcal{V}/\mathcal{U}$, entonces $(u_1, ..., u_m, w_1, ..., w_k)$ es una base para $\mathcal{V}$.
4. $dim_k\mathcal{V} = dim_k\mathcal{U} + dim_k\mathcal{V}/\mathcal{U}$.
5. $dim_k\mathcal{U} = dim_k\mathcal{V} \quad \Leftrightarrow \quad \mathcal{U} = \mathcal{V}$.

DEMOSTRACIÓN.

1. Es una consecuencia del teorema de Steinnitz.
2. si $\mathcal{V} = \langle v_1, ..., v_n\rangle$, entonces $\mathcal{V}/\mathcal{U} = \langle w_1 + \mathcal{U}, ..., w_n + \mathcal{U}\rangle$. Luego la conclusión se sigue nuevamente del teorema de Steinnitz.
3. Sean $(u_1, ..., u_m)$ una base para $\mathcal{U}$ y $(w_1 + \mathcal{U}, ..., w_k + \mathcal{U})$ una base para $\mathcal{V}/\mathcal{U}$. Demostremos que $(u_1, ..., u_m, w_1, ..., w_k)$ es una base para $\mathcal{V}$.
   (a) Sea $v \in \mathcal{V}$, entonces

$$v + \mathcal{U} = \sum_{j=1}^{k} a_j(w_j + \mathcal{U}) = \sum_{j=1}^{k} a_j w_j + \mathcal{U}, \quad a_j \in \mathcal{K}.$$

Es decir

$$v - \sum_{j=1}^{k} a_j w_j \in \mathcal{U}$$

Entonces $v - \sum_{j=1}^{k} a_j w_j = \sum_{i=1}^{n} b_i u_i$ y por lo tanto $\mathcal{V} = \langle u_1, ..., u_m, w_1, ..., w_k \rangle$.

(b) Sea $\sum_{j=1}^{m} c_j u_j + \sum_{i=1}^{k} d_i w_i = 0 \quad \forall c_j, d_i \in \mathcal{K}$. Entonces

$$\mathcal{U} = 0 + \mathcal{U} = (\underbrace{\sum_{j=1}^{m} c_j u_j}_{\in \mathcal{U}} + \sum_{i=1}^{k} d_i w_i) + \mathcal{U} = (\sum_{i=1}^{k} d_i w_i) + \mathcal{U} = \sum_{i=1}^{k} d_i (w_i + \mathcal{U}).$$

Entonces $d_1 = ... = d_k = 0$ (ya que $(w_i + \mathcal{U} : i = 1, ..., k)$ es una base para $\mathcal{V}/\mathcal{U}$, entonces $\sum_{j=1}^{m} c_j u_j = 0$ luego $c_1 = ... = c_m = 0$.

4. Se sigue de (3).

5.

$$\begin{aligned} dim_k \mathcal{U} = dim_k \mathcal{V} &\Leftrightarrow dim_k \mathcal{V}/\mathcal{U} = 0 \\ &\Leftrightarrow \mathcal{V}/\mathcal{U} = 0 \\ &\Leftrightarrow \mathcal{V} = \mathcal{U} \end{aligned}$$

Teorema 64.

Sean $\mathcal{U}_1 \mathcal{U}_2 \ll \mathcal{V}, \quad dinm_k \mathcal{U}_i < \infty$. Entonces se verifica

$$dim_k(\mathcal{U}_1 + \mathcal{U}_2) = dim_k \mathcal{U}_1 + dim_k \mathcal{U}_2 - dim_k(\mathcal{U}_1 \cap \mathcal{U}_2).$$

DEMOSTRACIÓN. Definamos $n_i := dim_k \mathcal{U}_i$ y $d := dim_k(\mathcal{U}_1 \cap \mathcal{U}_2)$. Sea $(u_1, ..., u_d)$ una base para $(\mathcal{U}_1 \cap \mathcal{U}_2)$. Usando el teorema (63)(3) podemos extender esta para obtener una base para $\mathcal{U}_1$ y otra para $\mathcal{U}_2$. Digamos

$$\begin{aligned} &(u_1, ..., u_d, u_{d+1}, ..., u_{n_1}) \quad \text{(base para } \mathcal{U}_1\text{)} \\ &(u_1, ..., u_d, u'_{d+1}, ..., u'_{n_2}) \quad \text{(base para } \mathcal{U}_2\text{)} \end{aligned}$$

1. $(u_1, ..., u_{n_1}, u'_{d+1}, ..., u'_{n_2})$ es linealmente independiente: Sea

$$a_1 u_1 + \cdots + a_{n_1} u_{n_1} + b_{d+1} u'_{d+1} + \cdots + b_{n_2} u'_{n_2} = 0 \text{ con } a_i, b_j \in \mathcal{K}.$$

Se sigue:

$$\underbrace{a_1 u_1 + \cdots + a_{n_1} u_{n_1}}_{\in \mathcal{U}_1} = -(\underbrace{b_{d+1} u'_{d+1} + \cdots + b_{n_2} u'_{n_2}}_{\in \mathcal{U}_2}) \in \mathcal{U}_1 \cap \mathcal{U}_2. \qquad (2.1)$$

Sabemos que $(u_1, ..., u_d)$ es una base para $\mathcal{U}_1 \cap \mathcal{U}_2$, entonces

$$-b_{d+1}u'_{d+1} - \cdots - b_{n_2}u'_{n_2} = \sum_{j=1}^{d} c_j u_j \text{ con } c_j \in \mathcal{K}.$$

Pero $(u_1, \cdots, u_d, u'_{d+1}, \cdots, u'_{n_2})$ es una base para $\mathcal{U}_2$ y por lo tanto tenemos $b_{d+1} = \cdots = b_{n_2} = 0$.

De (2.1) se sigue que $\sum_{i=1}^{n_1} a_i u_i = 0$ pero $(u_1, ..., u_{n_1})$ es una base para $\mathcal{U}_1$ entonces $a_i = 0 \quad \forall i = 1, 2, ..., n_1$.

2. $(u_1, \cdots, u_{n_1}, u'_{d+1}, \cdots, u'_{n_2})$ es una base para $\mathcal{U}_1 + \mathcal{U}_2$:

$$\mathcal{U}_1 + \mathcal{U}_2 = \langle \mathcal{U}_1 \cup \mathcal{U}_2 \rangle = \langle u_1, \cdots, u_{n_1}, u'_{d+1}, \cdots, u'_{n_2} \rangle.$$

El resto se sigue de (1).

3. De (2) tenemos

$$\begin{aligned} dim_k(\mathcal{U}_1 + \mathcal{U}_2) &= n_1 + (n_2 - d) \\ &= dim_k\mathcal{U}_1 + dim_k\mathcal{U}_2 - dim_k(\mathcal{U}_1 \cap \mathcal{U}_2). \end{aligned}$$

Definición 65.

Se $\mathcal{U} \ll \mathcal{V}$, $\mathcal{V}$ espacio vectorial. El subespacio $\mathcal{U}'$ de $\mathcal{V}$ se llama complemento de $\mathcal{U}$ en $\mathcal{V}$ (como espacio vectorial) si se verifica:

1. $\mathcal{U} \cap \mathcal{U}' = \{0\}$.
2. $\mathcal{U} + \mathcal{U}' = \mathcal{V}$

Notación: $\mathcal{V} = \mathcal{U} \oplus \mathcal{U}'$ (La suma directa de $\mathcal{U}$ con $\mathcal{U}'$).

2.4.4 Observación.

1. $\mathcal{U}'$ no es el complemento desde el punto de vista de la teoría de conjunto.

$$\mathcal{U} = \{(x, x) : x \in \mathbb{R}\},$$
$$\mathcal{U}' = \{(x, -x) : x \in \mathbb{R}\}.$$

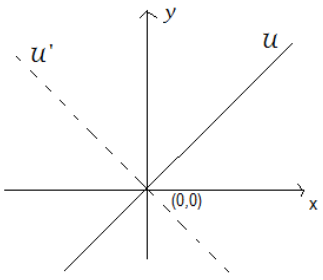


Figura 2.1: gráfica de $\mathcal{U}$ y $\mathcal{U}'$

2. Sea $\mathcal{V} = \mathbb{R}^2$

$$\mathcal{U} = \{(x,0) : x \in \mathbb{R}\}, \quad \mathcal{U}' = \{(0,x) : x \in \mathbb{R}\}, \quad \mathcal{U}'' = \{(x,x) : x \in \mathbb{R}\}$$

$$\mathcal{V} = \mathcal{U} \oplus \mathcal{U}' = \mathcal{U} \oplus \mathcal{U}'', \quad \mathcal{U}' \neq \mathcal{U}''$$

Teorema 66.

Todo subespacio vectorial de un espacio vectorial de dimensión finita admite un complemento.

DEMOSTRACIÓN. Sea $\mathcal{U} \ll \mathcal{V}$ y sea $(u_1, ..., u_m)$ una base para $\mathcal{U}$. De acuerdo al teorema (63) se puede extender esta a una base para $\mathcal{V}$, digamos $(u_1, ..., u_m, u_{m+1}, ..., u_m)$.
Definamos $\mathcal{U}' = \langle u_{m+1}, ..., u_n \rangle$. Es claro que $\mathcal{V} = \mathcal{U} + \mathcal{U}'$.
Sea $v \in \mathcal{U} \cap \mathcal{U}'$: $\quad v = \sum_{i=1}^{m} a_i u_i = \sum_{i=m+1}^{n} a_i u_i \quad a_i \in \mathcal{K}$
Entonces $\sum_{i=1}^{n} a_i u_i + \sum_{i=m+1}^{n} (-a_i) u_i = 0$ entonces $a_i = 0 \quad \forall i = 1, ..., n$ entonces $v = 0$.

2.5 Homomorfismos II (Aplicaciones lineales)

Definición 67.

1. Sea $\mathcal{K}$ un cuerpo y sean $\mathcal{V}, \mathcal{W}$ espacios vectoriales sobre $\mathcal{K}$. Una función $A : mathcalV \to \mathcal{W}$ se llama $\mathcal{K}$-lineal o $\mathcal{K}$-homomorfismo entre espacios vectoriales si se cumple:
   (a) $A(v_1 + v_2) = Av_1 + Av_2 \quad \forall v_1, v_2 \in \mathcal{V}$.
   (b) $A(kv) = kAv \quad \forall k \in \mathcal{K}, \quad v \in \mathcal{V}$.

   En particular se tiene que A es un homomorfismo del grupo aditivo abeliano $\mathcal{V}$ en $\mathcal{W}$. (se sigue de (1)).
   Por lo tanto se cumple que $A(0) = 0$ y $A(-v) = -Av \quad \forall v \in \mathcal{V}$.
2. El conjunto de todas las funciones $\mathcal{K}$-lineales de $\mathcal{V}$ en $\mathcal{W}$ lo notaremos con $Hom_k(\mathcal{V}, \mathcal{W})$.
3. Sea $A \in Hom_k(\mathcal{V}, \mathcal{W})$
   A se llama Momomorfismo $\Leftrightarrow$ A es inyectiva.
   A se llama Epimorfismo $\Leftrightarrow$ A es sobreyectiva.
   A se llama Isomorfismo $\Leftrightarrow$ A es biyectiva.
   Si existe un Isomorfismo entre $\mathcal{V}$ y $\mathcal{W}$ se dice entonces que $\mathcal{V}$ y $\mathcal{W}$ son isomorfos, escribiremos $\mathcal{V} \cong \mathcal{W}$.
4. Los elementos de $Hom_k(\mathcal{V}, \mathcal{V})$ se llaman Endomorfismos de $\mathcal{V}$.
5. Si $A \in Hom_k(\mathcal{V}, \mathcal{V})$ es un isomorfismo, entonces A se llamará un Automorfismo.
6. Sea $A \in Hom_k(\mathcal{V}, \mathcal{W})$. Definimos

$$\mathcal{N}(A) := \{v \in \mathcal{V} : Av = 0\}$$
$$Im(A) := \{Av : v \in \mathcal{V}\}$$

2.5.1 Ejemplos.

1. Sea $\mathcal{V} = P(\mathbb{R})$. Definamos $D : \mathcal{V} \to \mathcal{V}$ así:

$$(Df)(x) := f'(x) \qquad f \in P(\mathbb{R}), \quad x \in \mathbb{R}.$$

D es una función $\mathbb{R}$-lineal.
D no es un Monomorfismo: $Df = 0 \quad \forall f$ constante.
D es Epimorfismo:

$$\begin{aligned} g(x) : &= \frac{d}{dx}\left(\int_0^x g(t)dt\right) \\ &= D\left(\int_0^x g(t)dt\right) \quad \forall g \in P(\mathbb{R}) \end{aligned}$$

2. Sea $\mathcal{V} = C^1([0,1],\mathbb{R}), \quad \mathcal{W} = \mathbb{R}$

$$I : \mathcal{V} \to \mathcal{W} \text{ se define por } If := \int_0^1 f(x)dx.$$

I es una transformación lineal.

3. Sea $\mathcal{K}$ un campo. $\mathcal{V} = \mathcal{K}^n, \quad \mathcal{W} = \mathcal{K}^m$.
Sea $a_{ij} \in \mathcal{K}$ cualesquiera $i = 1, 2, ..., m \quad , \quad j = 1, 2, ..., n$.
Definamos $A : \mathcal{V} \to \mathcal{W}$ Así:
$A(x_1, ..., x_n) = \left(\sum_{j=1}^n a_{1j}x_j, ..., \sum_{j=1}^n a_{mj}x_j\right)$
Se verifica facilmente que $A \in Hom_k(\mathcal{V}, \mathcal{W})$.

4. Caso espacial de (3). Definamos $A(x_1, ..., x_n) := x_i$

$$I : \mathcal{K}^n \to \mathcal{K}$$

(Proyección sobre la i-esima componente).

5. Sea $\mathcal{V} = C^1([0,1],\mathbb{R})$. Sea $\mathcal{K} \in C^1([0,1] \times [0,1],\mathbb{R})$
Definamos $A : \mathcal{V} \to \mathcal{V}$ por $(Af)(x) = \int_0^1 \mathcal{K}(x,y)f(y)dy$.
Se demuestra que $A \in Hom_{\mathbb{R}}(\mathcal{V}, \mathcal{V})$.

6. Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$ y $\mathcal{U}$ un subespacio de $\mathcal{V}$. Definamos

$$\begin{aligned} A : \mathcal{V} &\to \mathcal{V}/\mathcal{U} \\ Av &:= v + \mathcal{U} \end{aligned}$$

A es claramente una transformación lineal, además sobreyectiva.

$$\begin{aligned} \mathcal{N}(A) &= \{v \in \mathcal{V} : Av = 0\} \\ &= \{v \in \mathcal{V} : v + \mathcal{U} = \mathcal{U}\} \\ &= \{v \in \mathcal{V} : v \in \mathcal{U}\} \\ &= \mathcal{U} \end{aligned}$$

Lema 68.

Sean $\mathcal{V}, \mathcal{W}$ espacios vectoriales sobre $\mathcal{K}$ y sea $A \in Hom_k(\mathcal{V}, \mathcal{W})$.

1. $\mathcal{N}(A)$ es un subespacio de $\mathcal{V}$ y $Im(A)$ es un subespacio de $\mathcal{W}$.
2. A es un Monomorfismo $\Leftrightarrow \mathcal{N}(A) = \{0\}$.
3. A es un Epimorfismo $\Leftrightarrow Im(A) = \mathcal{W}$.
4. A es un Isomorfismo $\Leftrightarrow \mathcal{N}(A) = \{0\} \quad \wedge \quad Im(A) = \mathcal{W}$.

DEMOSTRACIÓN. $\mathcal{N}(A) \neq 0$, ya que $0 \in \mathcal{N}(A)$.

1. (a) Sean $v_1, v_2 \in \mathcal{N}(A)$, i.e $Av_1 = Av_2 = 0$. Entonces
$A(v_1 + v_2) = Av_1 + Av_2 = 0 + 0 = 0 \quad \Rightarrow \quad (v_1 + v_2) \in \mathcal{N}(A)$.
Sea $v \in \mathcal{N}(A), \quad k \in \mathcal{K}$, entonces $A(kv) = kAv = k \cdot 0 = 0 \quad \Rightarrow$
$kv \in \mathcal{N}(A)$. Por lo tanto $\mathcal{N}(A)$ es un subespacio de $\mathcal{V}$.

   (b) $Im(A) \neq 0$, pues $0 \in Im(A)$.
Sea $w_1, w_2 \in Im(A)$, entonces existen $v_1, v_2 \in \mathcal{V}$ tales que

$$Av_1 = w_1 \quad \wedge \quad Av_2 = w_2$$
$$\Rightarrow \quad w_1 + w_2 = Av_1 + Av_2 = A(v_1 + v_2) \in Im(A)$$

Sea $k \in \mathcal{K}$, $w \in Im(A)$, entonces existe $v \in \mathcal{V}$ tal que $w = Av$

$$kw = kAv = A(kv) \in Im(A).$$

El resto se deja como ejercicio.

Teorema 69.

Sea $A \in Hom_k(\mathcal{V}, \mathcal{W})$ y sea $(v_i : i \in I)$ una base para $\mathcal{V}$.

1. A es un Epimorfismo si y solo si $\mathcal{W} = \langle Av_i : i \in I \rangle$.
2. A es un Monomorfismo si y solo si $(Av_i : i \in I)$ es linealmente independiente.
3. A es un Isomorfismo si y solo si $(Av_i : i \in I)$ es una base para $\mathcal{V}$.

DEMOSTRACIÓN..

1. (a) Sea A un epimorfismo y sea $w \in \mathcal{W}$, entonces existe $v \in \mathcal{V}$ tal que $Av = w$, pero $v = \sum_{i \in I} k_i v_i, \quad k_i \in \mathcal{K}$, y solo un número finito de estos son distintos a 0, entonces:

$$w = Av = A(\sum_{i \in I} k_i v_i) = \sum_{i \in I} k_i A v_i.$$

por tanto $\mathcal{W} = \langle Av_i : i \in I \rangle$.

   (b) Supongamos que $\mathcal{W} = \langle Av_i : i \in I \rangle$ y sea $w \in \mathcal{W}$, entonces existe $k_i \in \mathcal{K}$ con solo un número finito de estos $\neq 0$ tales que

$$w = \sum_{i \in I} k_i (Av_i) = A(\sum_{i \in I} k_i v_i) \in Im(A).$$

2. (a) Sea A un Monomorfismo y sea $\sum_{i\in I} c_i(Av_i) = 0$ con $c_i \in \mathcal{K}$.

   Debemos demostrar que $c_i = 0 \quad \forall i \in I$. Observe que

   $$0 = \sum_{i\in I} c_i(Av_i) = A(\sum_{i\in I} c_i v_i).$$

   Entonces, $\sum_{i\in I} c_i v_i \in \mathcal{N}(A)$. Por lo tanto, $\sum_{i\in I} c_i v_i = 0$. dado que $(v_i : i \in I)$ es una base para $\mathcal{V}$ se tiene que $c_i = 0 \quad \forall i \in I$.

   (b) Supongamos que $(Av_i : i \in I)$ es linealmente independiente. Demostremos que $\mathcal{N}(A) = 0$. Sea $\sum_{i\in I} \alpha_i v_i \in \mathcal{N}(A), \quad \alpha_i \in \mathcal{K}$. Entonces

   $$0 = Av = \sum_{i\in I} \alpha_i Av_i \quad \Rightarrow \quad \alpha_i = 0 \quad \forall i \in I \quad \Rightarrow \quad v = 0.$$

3. Se sigue de 1 y 2.

Teorema 70.

Sean $\mathcal{V}, \mathcal{W}$ espacios vectoriales sobre $\mathcal{K}$. Sea $(v_i : i \in I)$ una base para $\mathcal{V}$ y sea $(w_j : j \in J)$ una base para $\mathcal{W}$.

1. Dados los vectores $w'_i \in \mathcal{W} \quad i \in I$. Existe exactamente un $A \in Hom_k(\mathcal{V}, \mathcal{W})$ tal que $Av_i = w'_i \quad \forall i \in I$.
2. Dados $a_{ji} \in \mathcal{K} \quad (i \in I, j \in J)$. Para cada $i \in I$ fijo. Sean solamente un número finito de $a_{ji} \neq 0$. Entonces existe exactamente un $A \in Hom_k(\mathcal{V}, \mathcal{W})$ tal que

   $$Av_i = \sum_{j\in J} a_{ji} w_j \qquad \forall i \in I.$$

DEMOSTRACIÓN.

1. (a) **La existencia:** Sea $v \in \mathcal{V}$, entonces $v = \sum_{i\in I} k_i v_i, \quad k_i \in \mathcal{K}$, y solo un número finito de estos son $\neq 0$. Del teorema (58)(2) (principio de comparación de coeficientes) se sigue que estos k_i están determinados de manera única. Definamos $A : \mathcal{V} \to \mathcal{W}$ de la siguiente manera:

   $$Av = A(\sum_{i\in I} k_i v_i) = \sum_{i\in I} k_i w'_i.$$

   Es claro que $Av_i = w'_i$.

   A **es** $\mathcal{K}$**-lineal:** Sean
   $v_1, v_2 \in \mathcal{V} \quad \Rightarrow \quad v_1 = \sum_{i\in I} \alpha_i v_i, \quad v_2 = \sum_{i\in I} \beta_i v_i.$

   $$\begin{aligned} A(v_1 + v_2) &= A(\sum_{i\in I} \alpha_i v_i + \sum_{i\in I} \beta_i v_i) = A(\sum_{i\in I} (\alpha_i + \beta_i) v_i) \\ &= \sum_{i\in I} (\alpha_i + \beta_i) w'_i = \sum_{i\in I} (\alpha_i w'_i + \beta_i w'_i) = \sum_{i\in I} \alpha_i w'_i + \sum_{i\in I} \beta_i w'_i \\ &= Av_1 + Av_2 \end{aligned}$$

   Sea $k \in \mathcal{K}, \quad v \in \mathcal{V}$.

$$A(kv) = A(\sum_{i\in I}(k\alpha_i)v_i) = \sum_{i\in I}(k\alpha_i)w_i' = k\sum_{i\in I}\alpha_i w_i' = kAv.$$

(b) **La unicidad:** Sea $A, B \in Hom_k(\mathcal{V},\mathcal{W})$ tales que $Av_i = w_i' \quad \wedge \quad Bv_i = w_i' \quad \forall i \in I$, entonces

$$A(\sum_{i\in I}\alpha_i v_i) = \sum_{i\in I}\alpha_i Av_i = \sum_{i\in I}\alpha_i Bv_i = B(\sum_{i\in I}\alpha_i v_i)$$

Entonces $A = B$

2. Se sigue de (1) si definimos $w_i' := \sum_{i\in I} a_{ji}w_j$.

Teorema 71.

Sean $\mathcal{V},\mathcal{W}$ espacios vectoriales sobre $\mathcal{K}$.

$$\mathcal{V} \cong \mathcal{W} \Leftrightarrow dim_k\mathcal{V} = dim_k\mathcal{W}.$$

(En particular existe (salvo isomorfia) un solo espacio vectorial de dimensión n, concretamente $\mathcal{K}^n$).

DEMOSTRACIÓN.

1. Supongamos que $dim_k\mathcal{V} = dim_k\mathcal{W} = n$. Sean $\mathfrak{B}_1 = (v_1,...,v_n)$, $\mathfrak{B}_2 = (w_1,...,w_n)$ bases para $\mathcal{V}$ y $\mathcal{W}$ respectivamente. Del teorema (70) se sigue que existe un $A \in Hom_k(\mathcal{V},\mathcal{W})$ tal que $Av_i = w_i$ para $i = 1,2,...,n$ y del teorema (69)(3) se sigue que A es un isomorfismo, entonces $\mathcal{V} \cong \mathcal{W}$.

2. Sea $A : \mathcal{V} \to \mathcal{V}$ un isomorfismo ($\mathcal{V} \cong \mathcal{W}$) y sea $\mathfrak{B}_1 = (v_1,...,v_n)$ una base para $\mathcal{V}$. Del teorema (69)(3) se tiene que $(Av_i : i = 1,2,...,n)$ es una base para $\mathcal{W}$, entonces $dim_k\mathcal{V} = dim_k\mathcal{W}$.

Teorema 72 (isomorfía).

Sean $\mathcal{V},\mathcal{W}$ espacios vectoriales sobre $\mathcal{K}$. Sea $A \in Hom_k(\mathcal{V},\mathcal{W})$ y sea N el Homomorfismo natural de $\mathcal{V}$ en $\mathcal{V}/\mathcal{N}(A)$, entonces existe un Monomorfismo $B \in Hom_k(\mathcal{V}/\mathcal{N}(A),\mathcal{W})$ con $A = BN$, en particular se cumple que

$$\mathcal{V}/\mathcal{N}(A) \cong Im(A).$$

DEMOSTRACIÓN. La demostración queda como ejercicio al lector. Sugerencia, observar el primer teorema de isomorfía para grupos.

Teorema 73.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$, $dim_k\mathcal{V} < \infty$. Sea $A \in Hom_k(\mathcal{V},\mathcal{W})$, entonces $dim_k\mathcal{V} = dim_k\mathcal{N}(A) + dim_k Im(A)$.

DEMOSTRACIÓN. Del teorema (72) se sigue que $\mathcal{V}/\mathcal{N}(A) \cong Im(A)$ y por lo tanto del teorema (71) se tiene que $dim_k(\mathcal{V}/\mathcal{N}(A)) = dim_k(Im(A))$.

Teorema 74.

Sean $\mathcal{V}, \mathcal{W}$ espacios vectoriales sobre $\mathcal{K}$, $dim_k\mathcal{V} = dim_k\mathcal{W}$. Sea $A \in Hom_k(\mathcal{V}, \mathcal{W})$, entonces son equivalentes:

1. A es un isomorfismo.
2. A es un Monomorfismo.
3. A es un Epimorfismo.

DEMOSTRACIÓN.

1⇒2. Evidente.

2⇒3. Del teorema (73) tenemos que $dim_k\mathcal{V} = dim_k\mathcal{N}(A) + dim_kIm(A)$. Por lo tanto $dim_k\mathcal{V} = dim_kIm(A)$. Por hipótesis $dim_k\mathcal{V} = dim_k\mathcal{W}$, entonces $dim_k\mathcal{W} = dim_kIm(A)$, luego $Im(A) = \mathcal{W}$ entonces A es Epimorfismo.

3⇒1. Nuevamente $dim_k\mathcal{V} = dim_k\mathcal{N}(A) + dim_kIm(A)$. Entonces $dim_k\mathcal{N}(A) = 0$, luego $\mathcal{N}(A) = \{0\}$ entonces A es Monomorfismo, por tanto A es isomorfismo.

Teorema 75.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$, $\mathcal{U}$ es un subespacio de $\mathcal{V}$. Sea $A \in Hom_k(\mathcal{V}, \mathcal{V})$ tal que $Au \in \mathcal{U} \quad \forall u \in \mathcal{U}$. (Se dice en este caso que $\mathcal{U}$ es A-invariante).

1. Definamos $A_{\mathcal{U}}: \mathcal{U} \to \mathcal{U}$ así: $A_{\mathcal{U}}(u) = A_{\mathcal{U}} \forall u \in \mathcal{U}$, entonces $A_{\mathcal{U}} \in Hom_k(\mathcal{U}, \mathcal{U})$.
2. Definamos $A_{\mathcal{V}/\mathcal{U}}: \mathcal{V}/\mathcal{U} \to \mathcal{V}/\mathcal{U}$ por $A_{\mathcal{V}/\mathcal{U}}(v + \mathcal{U}) = Av + \mathcal{U} \forall v \in \mathcal{V}$, entonces $A_{\mathcal{V}/\mathcal{U}} \in Hom_k(\mathcal{V}/\mathcal{U}, \mathcal{V}/\mathcal{U})$.
3. Si $A_{\mathcal{U}}$ y $A_{\mathcal{V}/\mathcal{U}}$ son Monomorfismos (o Epimorfismos o Isomorfismos), entonces A es un Monomorfismo (o Epimorfismo ó Isomorfismo).
4. Si $dim_k\mathcal{V} < \infty$ y A es un Isomorfismo, entonces $A_{\mathcal{U}}$ y $A_{\mathcal{V}/\mathcal{U}}$ son isomorfismos.

DEMOSTRACIÓN.

1. Dado que $A \in Hom_k(\mathcal{V}, \mathcal{V})$, entonces $A_{\mathcal{U}}(u) \subseteq \mathcal{U}$.
2. (a) $A_{\mathcal{V}/\mathcal{U}}$ está bien definida: $v_1 + \mathcal{U} = v_2 + \mathcal{U}$. Entonces $(v_1 - v_2) \in \mathcal{U}$, entonces $Av_1 - Av_2 = A(v_1 - v_2) \in \mathcal{U}$, luego
$$Av_1 + \mathcal{U} = Av_2 + \mathcal{U} \quad \Rightarrow \quad A_{\mathcal{V}/\mathcal{U}}(v_1 + \mathcal{U}) = A_{\mathcal{V}/\mathcal{U}}(v_2 + \mathcal{U}).$$
(b) $A_{\mathcal{V}/\mathcal{U}}$ es $\mathcal{K}$-lineal: Sean $v_1, v_2 \in \mathcal{V}$, entonces
$$\begin{aligned} A_{\mathcal{V}/\mathcal{U}}((v_1 + \mathcal{U}) + (v_2 + \mathcal{U})) &= A_{\mathcal{V}/\mathcal{U}}((v_1 + v_2) + \mathcal{U}) \\ &= A(v_1 + v_2) + \mathcal{U} \\ &= (Av_1 + Av_2) + \mathcal{U} \\ &= (Av_1 + \mathcal{U}) + (Av_2 + \mathcal{U}) \\ &= A_{\mathcal{V}/\mathcal{U}}(v_1 + \mathcal{U}) + A_{\mathcal{V}/\mathcal{U}}(v_2 + \mathcal{U}). \end{aligned}$$

Sea $v \in \mathcal{V}, \quad k \in \mathcal{K}$, entonces

$$\begin{aligned} A_{\mathcal{V}/\mathcal{U}}(k(v+\mathcal{U})) &= A_{\mathcal{V}/\mathcal{U}}(kv+\mathcal{U}) \\ &= A(kv)+\mathcal{U} \\ &= kAv+\mathcal{U} \\ &= k(Av+\mathcal{U}) \\ &= kA_{\mathcal{V}/\mathcal{U}}(v+\mathcal{U}). \end{aligned}$$

3. (a) Supongamos que $A_{\mathcal{U}}$ y $A_{\mathcal{V}/\mathcal{U}}$ son monomorfismos. Sea $v \in \mathcal{N}(A)$, luego $Av = 0$ entonces $\mathcal{U} = 0+\mathcal{U} = Av+\mathcal{U} = A_{\mathcal{V}/\mathcal{U}}(v+\mathcal{U})$. Entonces $v+\mathcal{U} \in \mathcal{N}(A_{\mathcal{V}/\mathcal{U}}) = \mathcal{U}$.
   Entonces $v \in \mathcal{U}$. Dado que $0 = Av = A_{\mathcal{U}}(v)$, se tiene que $v \in \mathcal{N}(A_{\mathcal{U}}) = \{0\} \quad \Rightarrow \quad v = 0$ y se tiene que $\mathcal{N}(A) = \{0\}$.

   (b) Supongamos que $A_{\mathcal{U}}$ y $A_{\mathcal{V}/\mathcal{U}}$ son Epimorfismos. Sea $v \in \mathcal{V}$, dado que $A_{\mathcal{V}/\mathcal{U}}$ es un Epimorfismo se tiene que $\exists v_1 \in \mathcal{V}$ tal que $v+\mathcal{U} = A_{\mathcal{V}/\mathcal{U}}(v_1+\mathcal{U}) = Av_1+\mathcal{U}$, entonces $v - Av_1 \in \mathcal{U}$.
   Por otro lado, $A_{\mathcal{U}}$ es un Epimorfismo, entonces $\exists u \in \mathcal{U}$ tal que $v - Av_1 = A_{\mathcal{U}}(u) = A_{\mathcal{U}}$. Entonces

$$v = Av_1 + A_{\mathcal{U}} = A(v_1+\mathcal{U}) \in Im(A).$$

   (c) Se sigue de (a) y (b).

4. Sea A un isomorfismo. $\mathcal{N}(A_{\mathcal{U}}) = \mathcal{N}(A) \cap \mathcal{U} = \{0\} \cap \mathcal{U} = \{0\}$, entonces $A_{\mathcal{U}}$ es un Monomorfismo. Entonces $A_{\mathcal{U}}$ es un isomorfismo.
   Por otro lado, $Im(A_{\mathcal{V}/\mathcal{U}}) = \mathcal{V}/\mathcal{U}$, es decir $A_{\mathcal{V}/\mathcal{U}}$ es un epimorfismo, entonces $A_{\mathcal{V}/\mathcal{U}}$ es un Isomorfismo.

Teorema 76.

Sean $\mathcal{V}, \mathcal{W}$ espacios vectoriales sobre $\mathcal{K}$. $Hom_k(\mathcal{V}, \mathcal{W})$ es un espacio vectorial sobre $\mathcal{K}$ con las siguientes operaciones:

$$\begin{aligned} (A+B)v &:= Av+Bv \qquad \forall v \in \mathcal{V}, k \in \mathcal{K} \\ (kA)v &:= k(Av) \qquad A, B \in Hom_k(\mathcal{V}, \mathcal{W}) \end{aligned}$$

DEMOSTRACIÓN. El cero de $Hom_k(\mathcal{V}, \mathcal{W})$ es la función: $0v = 0$ $\forall v \in \mathcal{V}$.

1. $A+B \in Hom_k(\mathcal{V}, \mathcal{W})$:
   Evidentemente $A+B : \mathcal{V} \to \mathcal{W}$. Además sean $v_1, v_2, v \in \mathcal{V}, k \in \mathcal{K}$.

$$\begin{aligned} (A+B)(v_1+v_2) &= A(v_1+v_2)+B(v_1+v_2) \\ &= Av_1+Av_2+Bv_1+Bv_2 \\ &= Av_1+Bv_1+Av_2+Bv_2 \\ &= (A+B)v_1+(A+B)v_2 \end{aligned}$$

$$\begin{aligned} (A+B)(kv) &= A(kv)+B(kv) \\ &= kAv+kBv \\ &= k(Av+Bv) \\ &= k(A+B)v \end{aligned}$$

2. $kA \in Hom_k(\mathcal{V}, \mathcal{W})$: Es claro.
3. $Hom_k(\mathcal{V}, \mathcal{W})$ satisface los axiomas de espacio vectorial:

   Ejemplo: Sean $k_1, k_2 \in \mathcal{K}$, $A \in Hom_k(\mathcal{V}, \mathcal{W})$. $(k_1 + k_2)A = k_1A + k_2A$: Sea $v \in \mathcal{V}$, entonces

$$\begin{aligned} ((k_1 + k_2)A)v &= (k_1 + k_2)Av \\ &= k_1Av + k_2Av \\ &= (k_1A)v + (k_2A)v \\ &= (k_1A + k_2A)v. \end{aligned}$$

Teorema 77.

Sean $\mathcal{V}, \mathcal{W}$ espacios vectoriales sobre $\mathcal{K}$. $dim_k\mathcal{V} < \infty$, $dim_k\mathcal{W} < \infty$. Digamos que $(v_1, ..., v_n)$ es una base para $\mathcal{V}$ y $(w_1, ..., w_m)$ es una base para $\mathcal{W}$. Definamos

$$E_{ij}\mathcal{V}_k := \begin{cases} 0 & \text{si} \quad j \neq k \\ w_i & \text{si} \quad j = k \end{cases}$$

$k, j = 1, 2, ..., n \quad i = 1, 2, ..., m$. Del teorema (58) se tiene que E_{ij} está determinado de manera única. Entonces $(E_{ij} : i \in \{1, 2, ..., m\}, j \in \{1, 2, ..., n\})$ es una base para $Hom_k(\mathcal{V}, \mathcal{W})$, en particular se cumple que

$$dim_k Hom_k(\mathcal{V}, \mathcal{W}) = dim_k\mathcal{V} \cdot dim_k\mathcal{W}.$$

DEMOSTRACIÓN.

1. $Hom_k(\mathcal{V}, \mathcal{W}) = \langle E_{ij} : i \in \{1, 2, ..., m\}, j \in \{1, 2, ..., n\} \rangle$.
   Sea $A \in Hom_k(\mathcal{V}, \mathcal{W})$ y digamos que
   $Av_k = \sum_{i=1}^{m} a_{ik}w_i \quad k = 1, ..., n, \quad a_{ik} \in \mathcal{K}$. Entonces

$$B := \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}E_{ij} \in Hom_k(\mathcal{V}, \mathcal{W}).$$

   Se cumple para $k = 1, ..., n$ la siguiente igualdad:

$$Bv_k = (\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}E_{ij})v_k = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}\underbrace{E_{ij}v_k}_{=\delta_{kj}w_i} = \sum_{i=1}^{m} a_{ik}w_i = Av_k$$

   Entonces se tiene que $A = B \in \langle E_{ij} : \cdots \rangle$.

2. $(E_{ij} : i \in \{1, 2, ..., m\}, j \in \{1, 2, ..., n\})$ es linealmente independiente:
   Sea $0 = \sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}E_{ij}$ con $b_{ij} \in \mathcal{K}$, entonces:

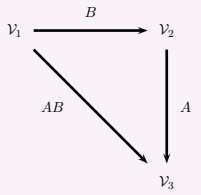
$$0 = 0v_k = (\sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}E_{ij})v_k = \sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}\underbrace{E_{ij}v_k}_{=\delta_{jk}w_i} = \sum_{i=1}^{m} b_{ik}w_i \quad \forall k$$

pero $(w_1, ..., w_m)$ es una base para $\mathcal{W}$, entonces $b_{1k} = \cdots = b_{nk} = 0 \quad \forall k$.

Teorema 78.

Sean $\mathcal{V}_1, \mathcal{V}_2, \mathcal{V}_3, \mathcal{V}_4$ espacios vectoriales sobre $\mathcal{K}$

1. Sean $A \in Hom_k(\mathcal{V}_2, \mathcal{V}_3), B \in Hom_k(\mathcal{V}_1, \mathcal{V}_2)$. Definamos $AB : \mathcal{V}_1 \to \mathcal{V}_3$ así: $(AB)v = A(Bv) \quad \forall v \in \mathcal{V}_1$. Entonces $AB \in Hom_k(\mathcal{V}_1, \mathcal{V}_3)$.

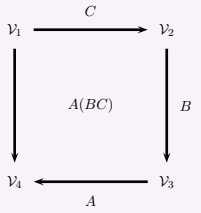


2. Sean $B, C \in Hom_k(\mathcal{V}_1, \mathcal{V}_2), A \in Hom_k(\mathcal{V}_2, \mathcal{V}_3)$, entonces $A(B + C) = AB + AC$.

3. Sea $C \in Hom_k(\mathcal{V}_1, \mathcal{V}_2)$ y sean $A, B \in Hom_k(\mathcal{V}_2, \mathcal{V}_3)$. Entonces $(A + B)C = AC + BC$.

4. Sea $A \in Hom_k(\mathcal{V}_2, \mathcal{V}_3)$; $B \in Hom_k(\mathcal{V}_1, \mathcal{V}_2)$, $k \in \mathcal{K}$, entonces $k(AB) = (kA)B = A(kB)$.

5. Sea $A \in Hom_k(\mathcal{V}_3, \mathcal{V}_4)$, $B \in Hom_k(\mathcal{V}_2, \mathcal{V}_3)$, $C \in Hom_k(\mathcal{V}_1, \mathcal{V}_2)$, entonces $A(BC) = (AB)C$.



DEMOSTRACIÓN.

1. Evidentemente la composición de funciones es otra función.
   AB **es $\mathcal{K}$-lineal:**

   (a) Sean $v_1, v_2 \in \mathcal{V}_1$, entonces

   $$(AB)(v_1 + v_2) = A(B(v_1 + v_2)) = A(Bv_1 + Bv_2) = A(Bv_1) + A(Bv_2) = (AB)v_1 + (AB)v_2.$$

   (b) Sea $v \in \mathcal{V}, \quad k \in \mathcal{K}$, entonces

   $$(AB)(kv) = A(B(kv)) = A(k(Bv)) = k(A(Bv)) = k((AB)v).$$

   Entonces $AB \in Hom_k(\mathcal{V}_1, \mathcal{V}_3)$.

2. Sea $v \in \mathcal{V}_1$, entonces

$$\begin{aligned}(A(B+C))v &= A((B+C)v) = A(Bv+Cv)\\ &= A(Bv)+A(Cv) = (AB)v+(AC)v\\ &= (AB+AC)v.\end{aligned}$$

El resto se deja como ejercicio.

Definición 79.

Un espacio vectorial sobre $\mathcal{K}$. $\mathcal{A}$ se denomina una $\mathcal{K}$-álgebra, si los siguientes axiomas se satisfacen:

1. Sobre $\mathcal{A}$, está definida una multiplicación, con respecto a la cual $\mathcal{A}$ es un anillo.
2. $\forall a, b \in \mathcal{A}, \quad \forall k \in \mathcal{K}$ se tiene $k(ab) = (ka)b = a(kb)$.

2.5.2 Ejemplo. $\mathbb{C}$ es una $\mathbb{R}$-álgebra, $\mathbb{R}$ es una $\mathbb{Q}$-álgebra.

Teorema 80.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$. Entonces $Hom_k(\mathcal{V},\mathcal{V})$ es una $\mathcal{K}$-álgebra. El módulo para la multiplicación (la composición de funciones) es la función $I : \mathcal{V} \to \mathcal{V}$ tal que $Iv = v \quad \forall v \in \mathcal{V}$. Si $dim_k\mathcal{V} = n$, entonces $dim_k Hom_k(\mathcal{V},\mathcal{V}) = n^2$.

DEMOSTRACIÓN. Del teorema (76) se tiene que $Hom_k(\mathcal{V},\mathcal{V})$ es un espacio vectorial sobre $\mathcal{K}$. El resto se sigue del teorema (78) y (77).

En general $Hom_k(\mathcal{V},\mathcal{V})$ no es un cuerpo.

2.5.3 Ejemplo. Sea $\mathcal{V} = \mathcal{K}^2, \quad \mathcal{K}$ un cuerpo. Definamos $A \in Hom_k(\mathcal{V},\mathcal{V})$ así: $A(x,y) := (x,0) \quad \forall x, y \in \mathcal{K}$.
Evidentemente $A \neq 0$. Supongamos que existe $B \in Hom_k(\mathcal{V},\mathcal{V})$ tal que $BA = I$. (I es el módulo de la multiplicación de $Hom_k(\mathcal{V},\mathcal{V})$). Entonces tendríamos:

$$(1,1) = I(1,1) = (BA)(1,1) = B(A(1,1)) = B(1,0)$$

y

$$(1,0) = I(1,0) = (BA)(1,0) = B(A(1,0)) = B(1,0) \text{ (absurdo)}$$

Entonces A no es invertible.
En general $AB \neq BA, \quad A, B \in Hom_k(\mathcal{V},\mathcal{V})$.

2.5.4 Ejemplo. $\mathcal{V} = \mathcal{K}^2$. Definamos $A(x,y) := (x,0) \quad : \quad B(x,y) := (y,x)$, entonces:

$$\begin{aligned}(AB)(x,y) &= (y,0)\\ (BA)(x,y) &= (0,x)\end{aligned}$$

$AB \neq BA$. (tomando $x \neq y$).

Teorema 81.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$, $dim_k\mathcal{V} = n$. Sea $A \in Hom_k(\mathcal{V}, \mathcal{V})$, entonces $(I, A, A^2, ..., A^{n^2})$ es linealmente independiente.

DEMOSTRACIÓN. Ejercicio.

Teorema 82.

Sean $\mathcal{V}_1, \mathcal{V}_2, \mathcal{V}_3$ espacios vectoriales sobre $\mathcal{K}$.

1. Sea $A : \mathcal{V}_1 \to \mathcal{V}_2$ un isomorfismo, entonces existe una única $B \in Hom_k(\mathcal{V}_2, \mathcal{V}_1)$ tal que $BA = Iv_1$. Además $AB = Iv_2$ y B es un isomorfismo. (Llamamos a B la inversa de A y escribiremos $B = A^{-1}$).
2. Sean $A_1 \in Hom_k(\mathcal{V}_1, \mathcal{V}_2), \quad A_2 \in Hom_k(\mathcal{V}_2, \mathcal{V}_3)$ dos Isomorfismos dados. Entonces A_2A_1 es un isomorfismo de $\mathcal{V}_1$ en $\mathcal{V}_3$ y se cumple que $(A_2A_1)^{-1} = A_1^{-1}A_2^{-1}$.

DEMOSTRACIÓN.

1. Dado que A es una biyeeción está garantizada la existencia de una función $B : \mathcal{V}_2 \to \mathcal{V}_1$ tal que $BA = Iv_1$ y $AB = Iv_2$. Queda por demostrar que $B \in Hom_k(\mathcal{V}_2, \mathcal{V}_1)$, ya que B es inyectiva y además sobreyectiva.

   B **es lineal:** Sean $v_2, v_2' \in \mathcal{V}_2$, entonces

   $$\begin{aligned} A(B(v_2 + v_2')) &= (AB)(v_2 + v_2') \\ &= Iv_2(v_2 + v_2') \\ &= v_2 + v_2' \\ &= (AB)v_2 + (AB)v_2' \\ &= A(Bv_2 + Bv_2') \end{aligned}$$

   Dado que A es un monomorfismo, se sigue que

   $$B(v_2 + v_2') = Bv_2 + Bv_2'.$$

   Sean ahora $v \in \mathcal{V}_2, \quad k \in \mathcal{K}$.

   $$A(B(kv)) = (AB)(kv) = kv = k((AB)v) = k(A(Bv)) = A(k(Bv)).$$

   Nuevamente usando que A es inyectiva se tiene que $B(kv) = kBv$.

2. $$\begin{aligned} (A_2A_1)(A_1^{-1}A_2^{-1}) &= A_2(A_1A_1^{-1})A_2^{-1} \\ &= A_2Iv_2A_2^{-1} \\ &= Iv_3 \end{aligned}$$

Además

$$\begin{aligned}(A_1^{-1}A_2^{-1})(A_2A_1) &= A_1^{-1}(A_2^{-1}A_2)A_1\\ &= A_1^{-1}Iv_3A_1\\ &= A_1^{-1}A_1\\ &= Iv_1\end{aligned}$$

Es claro que $(A_2A_1)^{-1} = (A_1^{-1}A_2^{-1})$

Definición 83.

1. Si A es un automorfismo de un espacio vectorial $\mathcal{V}$, (i.e $A \in End(\mathcal{V})$ y existe A^{-1}), entonces A se llamará regular o invertible. Si A no es regular se llamará singular.
2. Definimos $\mathbf{G}L(\mathcal{V}) := \{A \in Hom_k(\mathcal{V},\mathcal{V}) : A \text{ es regular}\}$. $\mathbf{G}L(\mathcal{V})$ es con respecto a la multiplicación definida en $Hom_k(\mathcal{V},\mathcal{V})$ un grupo. El llamado **general linear group** o también grupo de automorfismos de $\mathcal{V}$.
3. Sean $\mathcal{V}, \mathcal{W}$ espacios vectoriales sobre $\mathcal{K}$. Y sea $A \in Hom_k(\mathcal{V},\mathcal{W})$. Definimos el rango de A notado con $r(A)$ así:

$$r(A) := dim_k(Im(A)).$$

Lema 84.

Sea $A \in Hom_k(\mathcal{V},\mathcal{W})$.

1. Si $dim_k\mathcal{V} < \infty$, entonces $r(A) = dim_k\mathcal{V} - dim_k\mathcal{N}(A)$.
2. Si $dim_k\mathcal{W} < \infty$, entonces $r(A) \leq dim_k\mathcal{W}$.

DEMOSTRACIÓN.

1. Del teorema (73) se tiene que $dim_k Im(A) = dim_k\mathcal{V} - dim_k\mathcal{N}(A)$.
2. $Im(A) \subseteq \mathcal{W}$.

Teorema 85.

Sean $\mathcal{V}_1, \mathcal{V}_2, \mathcal{V}_3, \mathcal{V}_4$ espacios vectoriales sobre $\mathcal{K}$.

1. Sean $A \in Hom_k(\mathcal{V}_2,\mathcal{V}_3)$ y $B \in Hom_k(\mathcal{V}_1,\mathcal{V}_2)$. Si $r(A)$ y $r(B)$ son finitos, entonces $r(AB) \leq min\{r(A), r(B)\}$.
2. Sean $B \in Hom_k(\mathcal{V}_1,\mathcal{V}_2)$, $A \in Hom_k(\mathcal{V}_2,\mathcal{V}_3)$ y $C \in Hom_k(\mathcal{V}_3,\mathcal{V}_4)$. Sea $r(A) < \infty$. Si B es epimorfismo y C es un monomorfismo, entonces

$$r(A) = r(AB) = r(CA).$$

DEMOSTRACIÓN.

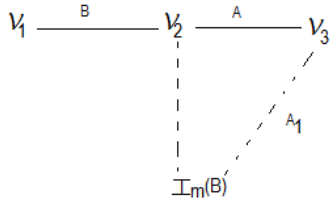
1. Definamos: $A_1 := A|_{Im(B)}$, tenemos:

$$\begin{aligned} r(AB) &= dim_k(Im(AB)) \\ &= dim_k\{(AB)v : v \in \mathcal{V}_1\} \\ &= dim_k\{ \underbrace{A(Bv) : v \in \mathcal{V}_1}_{\subseteq\{Av' : v' \in \mathcal{V}_2\} = Im(A)} \} \\ &\leq r(A) \end{aligned}$$

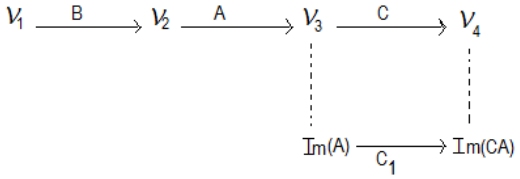
Por otro lado

$$\begin{aligned} r(AB) &= dim_k(Im(AB)) \\ &= dim_k\{A_1(w) : w = Bv \in Im(B)\} \\ &= dim_k Im(A_1) \\ &= dim_k Im(B) - dim_k \mathcal{N}(A_1) \\ &= dim_k Im(B) \\ &= r(B) \end{aligned}$$

La ilustración de la demostración se puede ver en el siguiente gráfico.



2. Tenemos ahora:



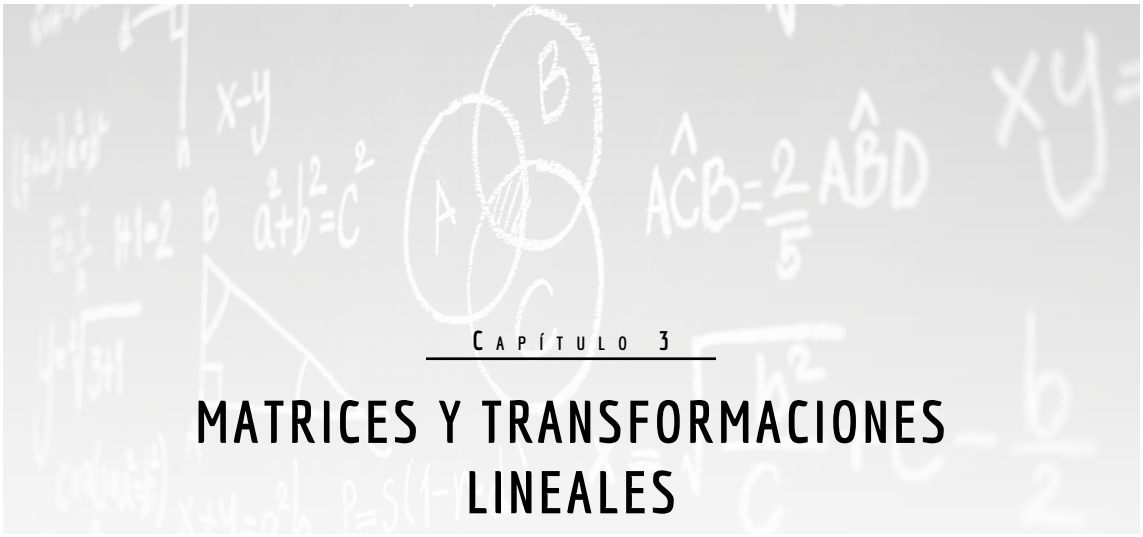
donde $C_1(w) = Cw \quad \forall w \in Im(A)$. Dado que C es un monomorfismo, se tiene que C_1 es un isomorfismo, entonces

$$\begin{aligned} r(A) &= dim_k(Im(A)) \\ &= dim_k Im(CA) \\ &= r(CA) \end{aligned}$$

Por otro lado

$$\begin{aligned} Im(B) &= \{ABv : v \in \mathcal{V}_1\} \\ &= \{Av' : v' \in \mathcal{V}_2\} \\ &= Im(A) \end{aligned}$$

Entonces $r(AB) = r(A)$.



CAPÍTULO 3

MATRICES Y TRANSFORMACIONES LINEALES

3.1 Definiciones básicas y ejemplos

Definición 86.

Sea $\mathcal{K}$ un cuerpo. Una matriz del tipo (m,n) sobre $\mathcal{K}$ es un esquema rectangular

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

de m filas $\left(a_{i1}, a_{i2}, ..., a_{in}\right)$ para $i = 1, 2, \ldots, m$ y n columnas $\begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$ para $j = 1, 2, \ldots, n$ con coeficientes $a_{ij} \in \mathcal{K}$.

Usualmente se representan matrices mediante letras mayúsculas y los elementos de estas mediante letras minúsculas.

El conjunto de todas las matrices del tipo (m,n) sobre $\mathcal{K}$ lo notaremos con $(\mathcal{K})_{mn}$. Matrices del tipo (m,m) se llaman cuadradas y se escribe $(\mathcal{K})_m$ en lugar de $(\mathcal{K})_{mm}$.

3.1.1 Observación. Sea $A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$

1. La diagonal principal de A se denota y define de las siguiente manera

$$diag(A) = (a_{11}, a_{22}, ..., a_{nn})$$

2. Decimos que A es una **matriz triangular superior** si $a_{ij} = 0$ para $i > j$, es decir, si los elementos por debajo de la diagonal principal son cero.

3. Decimos que A es una **matriz triangular inferior** si $a_{ij} = 0$ para $i < j$, es decir, si los elementos por encima de la diagonal principal son cero.

4. Llamamos a la matriz A **diagonal**, cuando A es triangular superior e inferior.

5. Diremos que la matriz A es **escalar** si la matriz es diagonal y si además los elementos de la diagonal principal son todos iguales a un mismo número k.

6. La matriz escalar cuadrada de tamaño n, donde $k = 1$ se denomina matriz de identidad y se notará con $\mathbf{1}$, I_n o simplemente I.

$$\mathbf{1} = \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$$

7. La matriz de tamaño (m, n), donde $a_{ij} = 0$ para todo $i = 1, \ldots, m$ y $j = 1, \ldots, n$ se denomina matriz nula o matriz cero, también notada por $O_{m,n}$.

$$\mathbf{0} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

Definición 87.

Sobre el conjunto de todas las matrices se definen las operaciones de suma y multiplicación por un escalar k de la siguiente manera:

$$(a_{ij}) + (b_{ij}) := (a_{ij} + b_{ij})$$
$$k(a_{ij}) := (ka_{ij})$$

Las anteriores operaciones definen a $(\mathcal{K})_{mn}$ como un espacio vectorial de dimensión $m \cdot n$.

3.1.2 Ejemplo. Sean

$$A = \begin{pmatrix} 1 & \frac{1}{2} & 0 \\ 1 & 2 & -1 \\ 0 & -1 & \sqrt{2} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & \frac{1}{2} & -1 \\ 2 & 2 & 0 \\ 1 & -2 & 2 \end{pmatrix},$$

entonces

$$\begin{aligned} A + B &= \begin{pmatrix} 1+0 & \frac{1}{2}+\frac{1}{2} & 0-1 \\ 1+2 & 2+2 & -1+0 \\ 0+1 & -1-2 & \sqrt{2}+2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & -1 \\ 3 & 4 & -1 \\ 1 & -3 & \sqrt{2}+2 \end{pmatrix} \end{aligned}$$

Definición 88.

Sean $\mathcal{V}, \mathcal{W}$ espacios vectoriales sobre $\mathcal{K}$. $\mathfrak{B}_1 = (v_1, ..., v_n)$ una base para $\mathcal{V}$ y $\mathfrak{B}_2 = (w_1, ..., w_m)$ una base para $\mathcal{W}$. Sea $A \in Hom_k(\mathcal{V}, \mathcal{W})$, entonces

$$Av_j = \sum_{i=1}^{m} a_{ij} w_i \qquad j = 1, 2, ..., n$$

y los $a_{ij} \in \mathcal{K}$ están determinados de manera única, por lo tanto del teorema (70) A queda completamente determinado por los $a_{ij} \quad i = 1, 2, ..., m \quad j = 1, 2, ..., n$. Definamos

$${}_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} = (a_{ij})$$

y llamaremos a ${}_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1}$ la matriz de A con respecto a las bases $\mathfrak{B}_1$y $\mathfrak{B}_2$.

3.1.3 Ejemplos. Sean $\mathcal{V}, \mathcal{W}$ espacios vectoriales sobre $\mathcal{K}$. $dim_k \mathcal{V} = 3$; $dim_k \mathcal{W} = 2 \quad ; \quad \mathfrak{B}_1 = (v_1, v_2, v_3) \quad ; \quad \mathfrak{B}_2 = (w_1, w_2)$.
(1)

$$\begin{aligned} Av_1 &= a_{11}w_1 + a_{21}w_2 \\ Av_2 &= a_{12}w_1 + a_{22}w_2 \\ Av_3 &= a_{13}w_1 + a_{23}w_2. \end{aligned}$$

Entonces,

$${}_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}$$

(2)

$$\begin{aligned} Av_1 &= w_1 \\ Av_2 &= 3w_1 - w_2 \\ Av_3 &= w_2. \end{aligned}$$

Entonces,

$${}_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1} = \begin{pmatrix} 1 & 3 & 0 \\ 0 & -1 & 1 \end{pmatrix}$$

3.1.4 Observación. En este punto es importante resaltar la diferencia entre sistema de vectores y conjuntos. Cambios en la enumeración de los vectores de la base origina cambios en la matriz.

Consideremos nuevamente el ejemplo (2), y elijamos

$$v_i' = v_i \quad \text{para } i = 1, 2, 3$$

y

$$w_1' = w_2 \quad , \quad w_2' = w_1.$$

Entonces

$$\begin{aligned} Av_1' &= w_2' \\ Av_2' &= -w_1' + 3w_2' \\ Av_3' &= w_1' \end{aligned}$$

Entonce, $_{\mathfrak{B}_2'}(A)_{\mathfrak{B}_1'} = \begin{pmatrix} 0 & -1 & 1 \\ 1 & 3 & 0 \end{pmatrix}$

Teorema 89.

1. Sean $\mathcal{V}, \mathcal{W}$ espacios vectoriales sobre $\mathcal{K}$. $\mathfrak{B}_1 = (v_1, ..., v_n)$ una base para $\mathcal{V}$ y $\mathfrak{B}_2 = (w_1, ..., w_m)$ una base para $\mathcal{W}$.
   La función $_{\mathfrak{B}_2}(f)_{\mathfrak{B}_1} : Hom_k(\mathcal{V}, \mathcal{W}) \to (\mathcal{K})_{m,n}$ definida por
   $_{\mathfrak{B}_2}(f)_{\mathfrak{B}_1} A = {}_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1}$ es una transformación lineal, en particular $Hom_k(\mathcal{V}, \mathcal{W}) \cong (\mathcal{K})_{m,n}$

2. Sean $\mathcal{V}_1, \mathcal{V}_2, \mathcal{V}_3$ espacios vectoriales sobre $\mathcal{K}$ con bases $\mathfrak{B}_1 = (v_1, ..., w_{n_1})$,
   $\mathfrak{B}_2 = (w_1, ..., w_{n_2}), \mathfrak{B}_2 = (u_1, ..., u_{n_3})$ respectivamente.
   Sean $B \in Hom_k(\mathcal{V}_1, \mathcal{V}_2), \quad A \in Hom_k(\mathcal{V}_2, \mathcal{V}_3)$

   $$\mathcal{V}_1 \xrightarrow{B} \mathcal{V}_2 \xrightarrow{A} \mathcal{V}_3$$

   Sea $_{\mathfrak{B}_3}(A)_{\mathfrak{B}_2} = (a_{ki})$ y $_{\mathfrak{B}_2}(B)_{\mathfrak{B}_1} = (b_{ij})$. Entonces
   $_{\mathfrak{B}_3}(AB)_{\mathfrak{B}_1} = (c_{kj}) \quad k = 1, ..., n_3, \quad j = 1, ..., n_1$ donde $c_{kj} = \sum_{i=1}^{n_2} a_{ki} b_{ij}$.

DEMOSTRACIÓN.

1. Sean $A, B \in Hom_k(\mathcal{V}, \mathcal{W})$ con $Av_j = \sum_{i=1}^{m} a_{ij} w_i, \quad Bv_j = \sum_{i=1}^{m} b_{ij} w_i$, entonces

   $$(A+B)v_j = Av_j + Bv_j = \sum_{i=1}^{m} a_{ij} w_i + \sum_{i=1}^{m} b_{ij} w_i = \sum_{i=1}^{m} (a_{ij} + b_{ij}) w_i$$

   Entonces:

   $$\begin{aligned} {}_{\mathfrak{B}_2}(f)_{\mathfrak{B}_1}(A+B) &= {}_{\mathfrak{B}_2}(A+B)_{\mathfrak{B}_1} \\ &= (a_{ij} + b_{ij}) = (a_{ij}) + (b_{ij}) \\ &= {}_{\mathfrak{B}_2}(f)_{\mathfrak{B}_1} A + {}_{\mathfrak{B}_2}(f)_{\mathfrak{B}_1} B \end{aligned}$$

   Además

   $$(kA)v_j = k(Av_j) = k \sum_{i=1}^{m} a_{ij} w_i = \sum_{i=1}^{m} (k a_{ij}) w_i$$

y con esto se tiene:

$$\begin{aligned}{}_{\mathfrak{B}_2}(f)_{\mathfrak{B}_1}(kA) &= {}_{\mathfrak{B}_2}(kA)_{\mathfrak{B}_1} = (ka_{ij}) = k(a_{ij}) \\ &= k_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1} = k_{\mathfrak{B}_2}(f)_{\mathfrak{B}_1}A.\end{aligned}$$

Entonces ${}_{\mathfrak{B}_2}(f)_{\mathfrak{B}_1}$ es lineal.
La inyectividad y la sobreyectividad se sigue del teorema (70).

2. Se tiene que:

$$\begin{aligned}Bv_j &= \sum_{i=1}^{n_2} b_{ij}w_i \qquad j = 1, 2, ..., n_1 \\ Aw_i &= \sum_{k=1}^{n_3} a_{ki}u_k \qquad i = 1, 2, ..., n_2\end{aligned}$$

Entonces:

$$\begin{aligned}(AB)v_j &= A(Bv_j) = A\left(\sum_{i=1}^{n_2} b_{ij}w_i\right) = \sum_{i=1}^{n_2} b_{ij}Aw_i \\ &= \sum_{i=1}^{n_2} b_{ij}\left(\sum_{k=1}^{n_3} a_{ki}u_k\right) \\ &= \sum_{k=1}^{n_3}(\sum_{i=1}^{n_2} \underbrace{b_{ij}a_{ki}}_{=a_{ki}b_{ij}})u_k = \sum_{k=1}^{n_3} c_{kj}u_k\end{aligned}$$

Definición 90.

Sean $(a_{ki}) \in (\mathcal{K})_{r,m}$ y $(b_{ij}) \in (\mathcal{K})_{m,n}$. Definamos

$$(a_{ki})(b_{ij}) := (c_{kj}) \in (\mathcal{K})_{r,n} \text{ donde } c_{kj} = \sum_{i=1}^{m} a_{ki}b_{ij}.$$

Con esta definición se cumple en el teorema (89)(2)

$${}_{\mathfrak{B}_3}(AB)_{\mathfrak{B}_1} = {}_{\mathfrak{B}_3}(A)_{\mathfrak{B}_2\mathfrak{B}_2}(B)_{\mathfrak{B}_1}$$

3.1.5 Ejemplos.

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

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

3. $\begin{pmatrix}1 & -3 & 5\\ -2 & 0 & 6\\ 1 & 3 & 1\end{pmatrix}\begin{pmatrix}2 & 4 & 3\\ 1 & 3 & 2\\ 2 & 0 & 1\end{pmatrix} = \begin{pmatrix}9 & -5 & 2\\ 8 & -8 & 0\\ 7 & 13 & 10\end{pmatrix}$

4. $\begin{pmatrix}7 & 1 & 4\\ 2 & -3 & 5\end{pmatrix}\begin{pmatrix}1 & 6\\ 0 & 4\\ -2 & 3\end{pmatrix} = \begin{pmatrix}-1 & 58\\ -8 & 15\end{pmatrix}$

5. $\begin{pmatrix} 1 & 4 & 0 & 2 \end{pmatrix} \begin{pmatrix} 3 & -6 \\ 2 & 4 \\ 1 & 0 \\ -2 & 3 \end{pmatrix} = \begin{pmatrix} 7 & 16 \end{pmatrix}$

Teorema 91.

1. Sean $(a_{ki}), (\tilde{a}_{ki}) \in (\mathcal{K})_{r,m}$ y $(b_{ij}), (\tilde{b}_{ij}) \in (\mathcal{K})_{m,n}$. Entonces se cumplen las siguientes propiedades:

$$((a_{ki}) + (\tilde{a}_{ki}))(b_{ij}) = (a_{ki})(b_{ij}) + (\tilde{a}_{ki})(b_{ij})$$
$$(a_{ki})((b_{ij}) + (\tilde{b}_{ij})) = (a_{ki})(b_{ij}) + (a_{ki})(\tilde{b}_{ij}).$$

2. Sean $(a_{ki}) \in (\mathcal{K})_{r,m}$, $(b_{ij}) \in (\mathcal{K})_{m,n}$, $(c_{js}) \in (\mathcal{K})_{n,t}$. entonces se cumple la propiedad asociativa:

$$((a_{ki})(b_{ij}))(c_{js}) = (a_{ki})((b_{ij})(c_{js})).$$

DEMOSTRACIÓN.

1. Sean $(\lambda_{kj}) = ((a_{ki}) + (\tilde{a}_{ki}))(b_{ij})$ y $(\alpha_{kj}) = (a_{ki})(b_{ij}) + (\tilde{a}_{ki})(b_{ij})$. Entonces:

$$\lambda_{kj} = \sum_{i=1}^{m} (a_{ki} + \tilde{a}_{ki}) b_{ij} = \sum_{i=1}^{m} a_{ki} b_{ij} + \sum_{i=1}^{m} \tilde{a}_{ki} b_{ij} = \alpha_{kj}.$$

Definición 92.

Sean $\mathcal{A}$ y $\mathcal{B}$, $\mathcal{K}$-álgebras. Una función $\varphi : \mathcal{A} \to \mathcal{B}$ se llama un homomorfismo entre $\mathcal{K}$-álgebras si se cumple:

1. φ es $\mathcal{K}$-lineal.
2. $\varphi(xy) = \varphi(x) \cdot \varphi(y) \quad \forall x, y \in \mathcal{A}$

Como es usual se define Monomorfismo, Epimorfismo, Isomorfismo.

Teorema 93.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$, $dim_k \mathcal{V} = n$, $\mathfrak{B}$ una base para $\mathcal{V}$. Entonces la función

$$f_{\mathfrak{B}} : Hom_k(\mathcal{V}, \mathcal{V}) \to (\mathcal{K})_n$$

Definida por $f_{\mathfrak{B}}(A) = (a_{ki}) = {}_{\mathfrak{B}}(A)_{\mathfrak{B}}$ es un Isomorfismo entre $\mathcal{K}$-álgebras. En particular se tiene que $Hom_k(\mathcal{V}, \mathcal{V}) \cong (\mathcal{K})_n$.

DEMOSTRACIÓN.

1. Del teorema (89)(1) se tiene que $f_{\mathfrak{B}}$ es lineal. ($\mathcal{K}$-lineal).

2. Sean $A, B \in Hom_k(\mathcal{V}, \mathcal{V})$. Entonces

$$f_{\mathfrak{B}}(AB) = \mathfrak{B}(AB)_{\mathfrak{B}} = \mathfrak{B}(A)_{\mathfrak{B}\mathfrak{B}}(B)_{\mathfrak{B}} = f_{\mathfrak{B}}(A) \cdot f_{\mathfrak{B}}(B).$$

Teorema 94.

Sean $A, B \in (\mathcal{K})_n$

1. Si $BA = I$, entonces $AB = I$ y B es la única matriz en $(\mathcal{K})_n$ con la propiedad $BA = I$, B se llamará la inversa de A y se notará con A^{-1}.
2. Si $AB = I$, entonces $BA = I$ y $B = A^{-1}$.

DEMOSTRACIÓN.

1. Sea $\mathcal{V}$ un espacio vectorial de dimensión n, $\mathfrak{B}$ una base para $\mathcal{V}$ y $f_{\mathfrak{B}} : Hom_k(\mathcal{V}, \mathcal{V}) \to (\mathcal{K})_n$ el isomorfismo del teorema (93). Es fácil verificar que $f_{\mathfrak{B}}^{-1} : (\mathcal{K})_n \to Hom_k(\mathcal{V}, \mathcal{V})$ es también un isomorfismo entre álgebras.
   Sean $A, B \in (\mathcal{K})_n$ tal que $AB = I$, entonces

$$f_{\mathfrak{B}}^{-1}(B) f_{\mathfrak{B}}^{-1}(A) = f_{\mathfrak{B}}^{-1}(BA) = f_{\mathfrak{B}}^{-1}(I) = Iv$$

   Del teorema (82) se tiene:

$$f_{\mathfrak{B}}^{-1}(A) f_{\mathfrak{B}}^{-1}(B) = Iv \quad \wedge \quad (f_{\mathfrak{B}}^{-1}(A))^{-1} = f_{\mathfrak{B}}^{-1}(B)$$

   Es decir

$$AB = f_{\mathfrak{B}} f_{\mathfrak{B}}^{-1}(AB) = f_{\mathfrak{B}}(f_{\mathfrak{B}}^{-1}(A) f_{\mathfrak{B}}^{-1}(B)) = f_{\mathfrak{B}}(Iv) = I$$

   y

$$B = f_{\mathfrak{B}} f_{\mathfrak{B}}^{-1}(B) = f_{\mathfrak{B}}(f_{\mathfrak{B}}^{-1}(A))^{-1} = f_{\mathfrak{B}} f_{\mathfrak{B}}^{-1}(A^{-1})) = A^{-1}.$$

2. Se demuestra de manera similar.

3.2 Matriz inversa

Definición 95.

Sea $A \in (\mathcal{K})_n$. A se llama regular o invertible, si A^{-1} existe.

Del teorema anterior se tiene: A es regular $\Leftrightarrow$ existe $B \in (\mathcal{K})_n$ tal que $AB = I$, $BA = I$.

Consecuencia: Si A es regular y $AC = 0$, entonces $C = 0$.

En efecto:

$$I = BA \quad \Rightarrow \quad C = IC = (BA)C = B(AC) = 0.$$

Teorema 96.

Sea $dim_k < \infty, \quad A \in Hom_k(\mathcal{V}, \mathcal{V})$, son equivalentes:

1. A es regular.
2. Para toda base $\mathfrak{B}$ de $\mathcal{V}$ si tiene que ${}_{\mathfrak{B}}(A)_{\mathfrak{B}}$ es regular.
3. Existe una base $\mathfrak{B}$ de $\mathcal{V}$ tal que ${}_{\mathfrak{B}}(A)_{\mathfrak{B}}$ es regular.

DEMOSTRACIÓN.

1⇒2. Si A es regular, entonces existe A^{-1}.

Por otro lado: $f_{\mathfrak{B}}(A^{-1}) = (f_{\mathfrak{B}}(A))^{-1} = ({}_{\mathfrak{B}}(A)_{\mathfrak{B}})^{-1}$, decir ${}_{\mathfrak{B}}(A)_{\mathfrak{B}}$ es regular.

2⇒3. Se tiene.

3⇒1. Por hipótesis existe ${}_{\mathfrak{B}}(A)^{-1}_{\mathfrak{B}}$.

$$f^{-1}_{\mathfrak{B}}(({}_{\mathfrak{B}}(A)_{\mathfrak{B}})^{-1}) = (\underbrace{f^{-1}_{\mathfrak{B}}(f_{\mathfrak{B}}(A))}_{=A})^{-1} = A^{-1}$$

3.2.1 Observación. Se define $\mathbf{G}L(n, \mathcal{K}) := \{A \in (\mathcal{K})_n : A \text{ es regular}\}$, con respecto a la multiplicación de matrices $\mathbf{G}L(n, \mathcal{K})$ es un grupo.
Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$, $dim_k\mathcal{V} = n$ y sea $\mathfrak{B}$ una base para $\mathcal{V}$, entonces

$$\begin{array}{c} f_{\mathfrak{B}} : \mathbf{G}L(\mathcal{V}) \to \mathbf{G}L(n, \mathcal{K}) \\ f_{\mathfrak{B}}(A) = {}_{\mathfrak{B}}(A)_{\mathfrak{B}} \end{array}$$

es un isomorfismo. Es decir $\mathbf{G}L(n, \mathcal{K}) \cong \mathbf{G}L(\mathcal{V}) \cong \mathbf{G}L(\mathcal{K}^n)$.

En particular $\mathbf{G}L(2, \mathbb{R}) \cong \mathbf{G}L(\mathbb{R}^2)$.

Teorema 97.

Sea $\mathfrak{B} = (v_1, ..., v_n)$ una base del espacio vectorial $\mathcal{V}$. Sean $a_{ij}, \quad i, j = 1, 2, ..., n$ dados. Definamos

$$w_j = \sum_{i=1}^{n} a_{ij} v_i \qquad j = 1, 2, ..., n$$

1. Son equivalentes:
   (a) $(w_1, ..., w_n)$ es una base para $\mathcal{V}$.
   (b) (a_{ij}) es regular.
2. Sea (a_{ij}) regular y $(b_{ij}) = (a_{ij})^{-1}$. Entonces

$$v_j = \sum_{k=1}^{n} b_{kj} w_k \qquad j = 1, 2, ..., n$$

DEMOSTRACIÓN.

1. Definamos $A \in Hom_k(\mathcal{V},\mathcal{V})$ así: $Av_j := w_j \quad (j = 1, 2, ..., n)$.
   Entonces
   $$\mathfrak{B}(A)_{\mathfrak{B}} = (a_{ij}).$$
   $(w_1, ..., w_n)$ es una base $\Leftrightarrow$ A es un isomorfismo (Automorfismo) $\Leftrightarrow$ A es regular $\Leftrightarrow \underbrace{\mathfrak{B}(A)_{\mathfrak{B}}}_{=(a_{ij})}$ es regular.

2. se tiene que $\sum_{k=1}^{n} b_{kj}w_k = \delta_{ij} \qquad \delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$. Entonces

$$\begin{aligned} v_j &= \sum_{i=1}^{n} \delta_{ij} v_i = \sum_{i=1}^{n}\sum_{k=1}^{n} a_{ik}b_{kj}v_i \\ &= \sum_{k=1}^{n} b_{kj} \underbrace{\sum_{i=1}^{n} a_{ik}v_i}_{w_k} = \sum_{k=1}^{n} b_{kj}w_k \end{aligned}$$

3.2.2 Ejemplo. Sea $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in (\mathcal{K})_2$. £ Cuándo existe A^{-1}?

Definamos $d = a_{11}a_{22} - a_{12}a_{21}$ y diferenciemos dos casos:

Caso 1:

Si $d \neq 0$, note que

$$\frac{1}{d}\begin{pmatrix} -a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix} A = I,$$

entonces A es regular.

Caso 2:

Si $d = 0$. Sea $a_{12} \neq 0$ o $a_{22} \neq 0$

$$\begin{pmatrix} a_{22} & -a_{12} \\ 0 & 0 \end{pmatrix} A = \begin{pmatrix} a_{22} & -a_{12} \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & 0 \end{pmatrix} = 0$$

Por la definición de matriz regular, se tiene que A no es regular.

Sea $a_{12} = a_{22} = 0$

$$A\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_{11} & 0 \\ a_{21} & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$$

Entonces A no es regular.

Cunclusión: A es no regular $\Leftrightarrow a_{11}a_{22} - a_{12}a_{21} \neq 0$.

Teorema 98 (Cambio de base).

1. Sean $\mathcal{V}, \mathcal{W}$ espacios vectoriales sobre $\mathcal{K}$. Sean

$$\begin{array}{ll} \mathfrak{B}_1 = (v_1, ..., v_n), & \mathfrak{B}'_1 = (v'_1, ..., v'_n) \text{ dos bases para } \mathcal{V} \\ \mathfrak{B}_2 = (w_1, ..., w_m), & \mathfrak{B}'_2 = (w'_1, ..., w'_m) \text{ dos bases para } \mathcal{W}. \end{array}$$

   Sean

$$\begin{aligned} v'_j &= \sum_{i=1}^{n} a_{ij} v_i \qquad j = 1, 2, ..., n \\ w'_l &= \sum_{k=1}^{m} b_{kl} w_k \qquad l = 1, 2, ..., m \end{aligned}$$

   Entonces todo $A \in Hom_k(\mathcal{V}, \mathcal{W})$ se tiene:

$$\begin{aligned} {}_{\mathfrak{B}'_2}(A)_{\mathfrak{B}'_1} &= (b_{kl})^{-1} {}_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1}(a_{ij}) \\ &= {}_{\mathfrak{B}'_2}(I_w)_{\mathfrak{B}_2\mathfrak{B}_2}(A)_{\mathfrak{B}_1\mathfrak{B}_2}(I_v)_{\mathfrak{B}'_1} \end{aligned}$$

   además (a_{ij}) y (b_{kl}) son regulares.

2. Caso especial: $\mathcal{V} = \mathcal{W}, \quad \mathfrak{B}_1 = \mathfrak{B}_2 = \mathfrak{B}_3, \quad \mathfrak{B}'_1 = \mathfrak{B}'_2 = \mathfrak{B}'_3$. Entonces

$$ {}_{\mathfrak{B}'}(A)_{\mathfrak{B}'} = (a_{ij})^{-1} {}_{\mathfrak{B}}(A)_{\mathfrak{B}}(a_{ij}) $$

3. Supongamos que son dadas $B \in (\mathcal{K})_{m,n}, \quad X \in (\mathcal{K})_m$ regular, $Y \in (\mathcal{K})_n$ regular. Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$ de dimensión n y sea $\mathcal{W}$ un espacio vectorial sobre $\mathcal{K}$ de dimensión m. Entonces existe $A \in Hom_k(\mathcal{V}, \mathcal{W})$ y existen bases $\mathfrak{B}_1, \mathfrak{B}'_1$ para $\mathcal{V}$ y $\mathfrak{B}_2, \mathfrak{B}'_2$ para $\mathcal{W}$ tal que

$$ {}_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1} = B \quad \wedge \quad {}_{\mathfrak{B}'_2}(A)_{\mathfrak{B}'_1} = XBY. $$

DEMOSTRACIÓN.

1. Se tiene $I_v v'_j = v'_j = \sum_{i=1}^{n} a_{ij} v_i$. Es decir ${}_{\mathfrak{B}_1}(I_v)_{\mathfrak{B}'_1} = (a_{ij})$. Del teorema (97) se tiene que (a_{ij}) es regular. Además $I_w w'_l = w'_l = \sum_{k=1}^{m} b_{kl} w_k$.
   Entonces ${}_{\mathfrak{B}_2}(I_w)_{\mathfrak{B}'_2} = (b_{kl})$.
   Del teorema (97) se tiene que (b_{kl}) es regular y $(b_{kl})^{-1} = {}_{\mathfrak{B}'_2}(I_w)_{\mathfrak{B}_2}$. Con esto tenemos:

$$\begin{aligned} {}_{\mathfrak{B}'_2}(A)_{\mathfrak{B}'_1} &= {}_{\mathfrak{B}'_2}(I_w A I_v)_{\mathfrak{B}'_1} \\ &= {}_{\mathfrak{B}'_2}(I_w)_{\mathfrak{B}_2\mathfrak{B}_2}(A)_{\mathfrak{B}_1\mathfrak{B}_1}(I_v)_{\mathfrak{B}'_1} \\ &= (b_{kl})^{-1} {}_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1}(a_{ij}). \end{aligned}$$

2. Se sigue de (1).

3. Sean $\mathfrak{B}_1 = (v_1, ..., v_n)$, $\mathfrak{B}_2 = (w_1, ..., w_m)$ bases para $\mathcal{V}$ y $\mathcal{W}$ respectivamente. Sea $B = (b_{jk})$.

   Definamos $A \in Hom_k(\mathcal{V}, \mathcal{W})$ así: $Av_i = \sum_{j=1}^{m} b_{ji} w_j$.

   Es claro que ${}_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1} = B$. Sean también $X^{-1} = (x_{ij})$, $Y = (y_{ij})$, definamos

$$v'_j = \sum_{i=1}^{n} y_{ij} v_i \qquad j = 1, 2, ..., n$$
$$w'_l = \sum_{k=1}^{m} x_{kl} w_k \qquad l = 1, 2, ..., m.$$

   Definamos $\mathfrak{B}'_1 = (v'_1, ..., v'_n)$, $\mathfrak{B}'_2 = (w'_1, ..., w'_m)$, entonces

$${}_{\mathfrak{B}'_2}(A)_{\mathfrak{B}'_1} = (x_{ij})^{-1} {}_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1} (y_{ij}) = XBY.$$

3.2.3 Observación. Sean $\mathcal{V}, \mathcal{W}$ espacios vectoriales sobre $\mathcal{K}$, ambos de dimensión finita, y sea $A \in Hom_k(\mathcal{V}, \mathcal{W})$.

Problema: ¿Cómo puede uno elegir bases $\mathfrak{B}_1, \mathfrak{B}_2$ para $\mathcal{V}$ y $\mathcal{W}$ respectivamente, de tal forma que la matriz ${}_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1}$ tenga una forma sencilla?

Iniciemos ahora el camino para responder esta pregunta.

Definición 99.

Sea

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \in (\mathcal{K})_{m,n}$$

Definimos para $j = 1, 2, ..., m$ $z_j := (a_{j1}, a_{j2}, ..., a_{jn})$ z_j se denomina el j-esimo vector fila de A. Para $i = 1, 2, ..., n$ definimos $s_i = \begin{pmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{mi} \end{pmatrix}$, s_i se denomina el i-esimo vector columna de A.

En ambos casos estos vectores pueden considerarse como elementos de $\mathcal{K}^n$ y $\mathcal{K}^m$ respectivamente.

Definamos $r(A) := dim_k \langle s_1, ..., s_n \rangle$ (El rango de A). Estos es, $r(A)$ es el maximo número de columnas linealmente independientes de A.

Teorema 100.

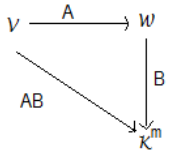
1. Sean $\mathcal{V}, \mathcal{W}$ espacios vectoriales sobre $\mathcal{K}$, ambos de dimensión finita, y sea $A \in Hom_k(\mathcal{V}, \mathcal{W})$. Sean $\mathfrak{B}_1, \mathfrak{B}_2$ bases para $\mathcal{V}$ y $\mathcal{W}$ respectivamente, entonces $r(A) = r({}_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1})$.
2. Sean $A \in (\mathcal{K})_{m,n}$, X, Y sean matrices regulares del tipo $(m,m), (n,n)$ respectivamente, entonces $r(A) = r(XAY)$.
3. Para $A \in (\mathcal{K})_{m,n}$ y $B \in (\mathcal{K})_{n,r}$, se cumple $r(AB) \leq min\{r(A), r(B)\}$.

DEMOSTRACIÓN.

1. Sean $\mathfrak{B}_1 = (v_1, ..., v_n)$ y $\mathfrak{B}_2 = (w_1, ..., w_m)$. Sea $Av_j = \sum_{i=1}^{m} a_{ij} w_i$.

   Definamos

$$B : \mathcal{W} \to \mathcal{K}^m$$
$$B(\sum_{i=1}^{m} k_i w_i) = \begin{pmatrix} k_1 \\ \vdots \\ k_m \end{pmatrix}$$



   Se demuestra facilmente que B es un isomorfismo. Del teorema (85)(2) se tiene que:

$$r(A) = r(AB) = dim_k Im(BA)$$
$$Im(BA) = \langle BAv_j : j = 1, 2, ..., n \rangle$$

   y

$$BAv_j = B(\sum_{i=1}^{m} a_{ij} w_i) = \begin{pmatrix} a_{ij} \\ \vdots \\ a_{mj} \end{pmatrix} := s_j,$$

   donde ${}_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1} = (a_{ij})$. Entonces

$$r(A) = dim_k Im(BA) = dim_k \langle s_j : j = 1, ..., n \rangle = r({}_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1})$$

2. Del teorema (98) tenemos: XAY y A son matrices para algún operador lineal Z con respecto a algunas bases, entonces

$$r(XAY) = r(Z) = r(A).$$

3. Se sigue del teorema (85)(1).

Teorema 101.

1. Sean $\mathcal{V}, \mathcal{W}$ espacios vectoriales sobre $\mathcal{K}$, ambos de dimensión finita. Sea $A \in Hom_k(\mathcal{V}, \mathcal{W})$ con $r(A) = r$. Entonces existe una base $\mathfrak{B}_1$ para $\mathcal{V}$ y una base $\mathfrak{B}_2$ para $\mathcal{W}$ tal que

$$ {}_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1} = \left(\begin{array}{c|c|c} I_r & | & 0 \\ - & - & - \\ 0 & | & 0 \end{array}\right) = \left(\begin{array}{cccc|cc} 1 & 0 & \cdots & 0 & & \\ 0 & 1 & \cdots & 0 & & \\ \vdots & & & & | & 0 \\ 0 & 0 & \cdots & 0 & & \\ \hline & & 0 & & | & 0 \end{array}\right) $$

2. Sean $A \in (\mathcal{K})_{m,n}$ con $r(A) = r$. Entonces existe una matriz regular $X \in (\mathcal{K})_n$ y una matriz regular $Y \in (\mathcal{K})_m$ tal que

$$ YAX = \left(\begin{array}{c|c|c} I_r & | & 0 \\ - & - & - \\ 0 & | & 0 \end{array}\right) $$

DEMOSTRACIÓN.

1. Sea $\mathfrak{B} = (v_1, ..., v_n)$ una base para $\mathcal{V}$ tal que $(v_{r+1}, ..., v_n)$ sea una base para $\mathcal{N}(A)$. Entonces $Im(A) = \langle Av_1, ..., Av_r \rangle$. Dado que

$$ dim_k Im(A) = dim_k \mathcal{V} - dim_k \mathcal{N}(A) = n - dim_k \mathcal{N}(A) = r, $$

se tiene que $(Av_1, ..., Av_r)$ es una base para $Im(A)$ (Verificar).

Definamos $w_i = Av_i \quad i = 1, 2, ..., r$ y entonces podemos extender estos a una base para $\mathcal{W}$, digamos $\mathfrak{B}_2$. Entonces

$$ \begin{array}{ll} Av_i = w_i & i = 1, 2, ..., r \\ Av_i = 0 & i = r+1, ..., n. \end{array} $$

Entonces ${}_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1} = \left(\begin{array}{c|c|c} I_r & | & 0 \\ - & - & - \\ 0 & | & 0 \end{array}\right)$.

2. Se sigue del teorema de cambio de base y (1).

3.2.4 Observación. Definamos sobre $(\mathcal{K})_{m,n}$ la siguiente relación:
$A \sim B \quad \Leftrightarrow \quad$ existen $X \in (\mathcal{K})_n, \quad Y \in (\mathcal{K})_m$ regulares tales que $B = YAX$.

1. $\sim$ es una relación de equivalencia:
   (a) **Reflexiva:** Tomando $X = I_n, \quad Y = I_m$ se verifica $A \sim A \quad \forall A \in (\mathcal{K})_{m,n}$.
   (b) **Simetría:** Supongamos que $A \sim B$. Entonces existen $X \in (\mathcal{K})_n$, $Y \in (\mathcal{K})_m$ regulares tales que $B = YAX$. Por lo tanto $A = Y^{-1}BX^{-1} \quad \Rightarrow \quad B \sim A$.
   (c) **Transitiva:** Supongamos que $A \sim B$ y $B \sim C$. Entonces

$$B = YAX \quad \wedge \quad C = \tilde{Y}B\tilde{X} \text{ donde } X, \tilde{X} \in (\mathcal{K})_n, \quad Y, \tilde{Y} \in (\mathcal{K})_m$$

todos regulares, entonces

$$C = \tilde{Y}(YAX)\tilde{X} = (\tilde{Y}Y)A(\tilde{X}X) \quad \Rightarrow \quad A \sim C.$$

Las clases de equivalencias:

$$\begin{aligned}
[A] &= \{B \in (\mathcal{K})_{m,n} : A \sim B\} \\
&= \{B \in (\mathcal{K})_{m,n} : \exists X, Y \cdots \text{tal que} \quad B = YAX\} \\
&= \{YAX : X \in (\mathcal{K})_n, \quad Y \in (\mathcal{K})_m \text{regulares}\} \\
&= \left\{ \begin{pmatrix} I_r & | & 0 \\ - & - & - \\ 0 & | & 0 \end{pmatrix} : r = 0, 1, ...min\{m, n\} \right\}
\end{aligned}$$

(El rango describe a $\sim$). Esta es la respuesta a la pregunta de la definición (99).

3.3 Matriz transpuesta

Definición 102.

Sea $A \in (\mathcal{K})_{m,n}$, donde

$$A = a($$

Definamos

$$A^t = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & & & \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix} \text{ La transpuesta de } A$$

$A^t = (x_{ij})$, donde $x_{ij} = a_{ji}$

Teorema 103.

1. Sean $A, B \in (\mathcal{K})_{n,m}, \quad k \in \mathcal{K}$. Entonces $(A + B)^t = A^t + B^t$ y $(kA)^t = kA^t$, entonces la función $A \to A^t$ es $\mathcal{K}$-lineal y además un Isomorfismo de $(\mathcal{K})_{n,m}$ en $(\mathcal{K})_{m,n}$.
2. Si $A \in (\mathcal{K})_{m,n}$ y $B \in (\mathcal{K})_{n,t}$, entonces $(AB)^t = B^t A^t$.
3. Si A es regular, entonces A^t también lo es.

DEMOSTRACIÓN.

1. Inmediato.
2. Sean $A = (a_{ij}) \quad B = (b_{jk}), \quad C := (AB)^t = (c_{ik})$, $D = B^t A^t = (d_{ik})$, entonces

$$c_{ik} = \sum_{j=1} a_{kj} b_{ji} \text{ y } d_{ik} = \sum_{j=1} b'_{ij} a'_{jk} = \sum_{j=1} b_{ji} a_{kj}$$

Entonces $C = D$.

3. $I = I^t = (AA^{-1})^t = (A^{-1})^t A^t \quad \Rightarrow \quad A^t$ tiene inversa.

Teorema 104.

Sea $A \in (\mathcal{K})_{n,m}$. Entonces $r(A) = dim_k\langle z_1, ..., z_m\rangle$, cada $z_i := (a_{i1}, ..., a_{in})$ (ver def (99)). En particular se cumple que

$$r(A) = r(A^t).$$

DEMOSTRACIÓN. Del teorema (101)(2) se tiene que existen matrices regulares X, Y tales que

$$YAX = \begin{pmatrix} I_r & | & 0 \\ - & - & - \\ 0 & | & 0 \end{pmatrix}, \text{ donde } r = r(A).$$

Del teorema (103) tenemos:

$$(YAX)^t = X^t A^t Y^t = \begin{pmatrix} I_r & | & 0 \\ - & - & - \\ 0 & | & 0 \end{pmatrix} \text{ con } X^t, Y^t \text{ regulares.}$$

Entonces:

$$\begin{aligned} dim_k\langle z_1, ..., z_m\rangle &= r(A^t) \\ &= r(X^t A^t Y^t) \\ &= r\begin{pmatrix} I_r & | & 0 \\ - & - & - \\ 0 & | & 0 \end{pmatrix} \\ &= r \\ &= r(A) \end{aligned}$$

Definición 105.

Sea $A \in (\mathcal{K})_{n,m}$, digamos $A = (A_{ij})$. Definimos la traza de A notada $Tr(A)$ así:

$$Tr(A) = \sum_{i=1}^{n} a_{ii}$$

Teorema 106.

1. $Tr : (\mathcal{K})_n \to (\mathcal{K})$ es $\mathcal{K}$-lineal.
2. $Tr(AB) = Tr(BA) \quad \forall A, B \in (\mathcal{K})_n$.
3. Sean $A, B \in (\mathcal{K})_n$ con B regular, entonces $Tr(B^{-1}AB) = Tr(A)$.
4. $Tr(A) = Tr(A^t)$.

DEMOSTRACIÓN.

1.

$$\begin{aligned} Tr((a_{ij})+(b_{ij})) &= Tr(a_{ij}+b_{ij}) \\ &= \sum_{i=1}^{n}(a_{ii}+b_{ii}) = \sum_{i=1}^{n}a_{ii}+\sum_{i=1}^{n}b_{ii} = Tr(a_{ij})+Tr(b_{ij}) \end{aligned}$$

$$Tr(k(a_{ij})) = Tr(ka_{ij}) = \sum_{i=1}^{n} ka_{ii} = k\sum_{i=1}^{n} a_{ii} = kTr(a_{ij}).$$

2. Sea $A=(a_{ij}) \quad B=(b_{jk}) \quad AB=(c_{ik}); \quad c_{ik}=\sum_{j=1}^{n} a_{ij}b_{ji}$

$$\begin{aligned} Tr(AB) &= \sum_{i=1}^{n} c_{ii} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}b_{ji} \\ &= \sum_{j=1}^{n}\sum_{i=1}^{n} b_{ji}a_{ij} = Tr(AB). \end{aligned}$$

3. $Tr(B^{-1}AB) = Tr(B^{-1}(AB)) = Tr(ABB^{-1}) = Tr(A).$

4. Ejercicio.

Definición 107.

Sea $A \in Hom_k(\mathcal{V},\mathcal{V}), \quad dim_k\mathcal{V} < \infty$. Sea $\mathfrak{B}$ una base cualquiera para $\mathcal{V}$. Definimos $Tr(A) = Tr({}_{\mathfrak{B}}(A)_{\mathfrak{B}})$.

Esta definición no depende de la elección de la base: Sea $\mathfrak{B}'$ otra base para $\mathcal{V}$. Usando el teorema del cambio de la base tenemos:

$${}_{\mathfrak{B}}(A)_{\mathfrak{B}} = X^{-1}{}_{\mathfrak{B}'}(A)_{\mathfrak{B}'}X, \quad X \text{ regular.}$$

Del teorema (106) se sigue:

$$Tr({}_{\mathfrak{B}}(A)_{\mathfrak{B}}) = Tr(X^{-1}{}_{\mathfrak{B}'}(A)_{\mathfrak{B}'}X) = Tr({}_{\mathfrak{B}'}(A)_{\mathfrak{B}'})$$

Sea $A=(a_{ij}) \in (\mathcal{K})_{m,n}$. Una transformación elemental de A será cualquiera de los siguientes cuatro pasos:

1. La multiplicación de una fila por una constante $k \in \mathcal{K}$, $k \neq 0$.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \rightarrow \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ ka_{i1} & ka_{i2} & \cdots & ka_{in} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

2. La adición de la fila j de A a la fila i de A: $\quad (i \neq j)$.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \to \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1}+a_{j1} & a_{i2}+a_{j2} & \cdots & a_{in}+a_{jn} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

$1'$ La multiplicación de una columna por una constante $k \in \mathcal{K}$, $k \neq 0$

$2'$ La adición de la columna j de A a la fila i de A: $\quad (i \neq j)$.

Lema 108.

Las siguientes operaciones se pueden obtener a partir de las transformaciones elementales.

3 La suma de k-veces la fila j de A a la fila i de A: $\quad (i \neq j)$.

$3'$ La suma de k-veces la columna j de A a la columna i de A: $\quad (i \neq j)$.

4 Intercambio de dos filas.

$4'$ Intercambio de dos columnas.

DEMOSTRACIÓN. Para (3) y (4). Las otras se hacen de manera análoga.

3. Sea $k \in \mathcal{K}, \quad k \neq 0$. Sean $z_i := (a_{i1}, a_{i2}, ..., a_{in}) \quad i = 1, 2, ..., m$

$$A = \begin{pmatrix} z_1 \\ \vdots \\ z_i \\ \vdots \\ z_j \\ \vdots \\ z_m \end{pmatrix} \xrightarrow{(1)} \begin{pmatrix} z_1 \\ \vdots \\ z_i \\ \vdots \\ kz_j \\ \vdots \\ z_m \end{pmatrix} \xrightarrow{(2)} \begin{pmatrix} z_1 \\ \vdots \\ z_i + kz_j \\ \vdots \\ kz_j \\ \vdots \\ z_m \end{pmatrix} \xrightarrow{(1)} \begin{pmatrix} z_1 \\ \vdots \\ z_i + kz_j \\ \vdots \\ z_j \\ \vdots \\ z_m \end{pmatrix}$$

4. $A = \begin{pmatrix} z_1 \\ \vdots \\ z_i \\ \vdots \\ z_j \\ \vdots \\ z_m \end{pmatrix} \xrightarrow{(2)} \begin{pmatrix} z_1 \\ \vdots \\ z_i + z_j \\ \vdots \\ z_j \\ \vdots \\ z_m \end{pmatrix} \xrightarrow{(1)} \begin{pmatrix} z_1 \\ \vdots \\ -z_i - z_j \\ \vdots \\ z_j \\ \vdots \\ z_m \end{pmatrix} \xrightarrow{(2)} \begin{pmatrix} z_1 \\ \vdots \\ -z_i - z_j \\ \vdots \\ -z_i \\ \vdots \\ z_m \end{pmatrix} \xrightarrow{(1)}$

$$\begin{pmatrix} z_1 \\ \vdots \\ z_i + z_j \\ \vdots \\ -z_i \\ \vdots \\ z_m \end{pmatrix} \xrightarrow{(2)} \begin{pmatrix} z_1 \\ \vdots \\ z_j \\ \vdots \\ -z_i \\ \vdots \\ z_m \end{pmatrix} \xrightarrow{(1)} \begin{pmatrix} z_1 \\ \vdots \\ z_j \\ \vdots \\ z_i \\ \vdots \\ z_m \end{pmatrix}$$

Lema 109.

Se verifica:

1. $$\begin{pmatrix} z_1 \\ \vdots \\ kz_i \\ \vdots \\ z_m \end{pmatrix} = \begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & k & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix} A$$

   Es decir la transformación elemental (1) se obtiene multiplicando a la izquierda de A por la matriz de arriba.

2. $$\begin{pmatrix} z_1 \\ \vdots \\ z_i + z_j \\ \vdots \\ z_m \end{pmatrix} = \begin{pmatrix} 1 & & & & \\ & 1 & & 0 & \\ & & \ddots & & \\ & 1 & & \ddots & \\ & & & & 1 \end{pmatrix} A$$

   Es decir la transformación elemental (2) se obtiene multiplicando a la izquierda de A por la matriz referenciada arriba.

Nota: La multiplicación a la derecha produce el mismo efecto pero sobre las columnas de A.

3.4 Matrices elementales.

Definición 110.

Las matrices

$$\begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & k & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & & & & \\ & 1 & & 0 & \\ & & \ddots & & \\ & 1 & & \ddots & \\ & & & & 1 \end{pmatrix}$$

con $k \in \mathcal{K} \quad k \neq 0, i \neq j (I + I_{ij})$

$$I_{ij} = (\lambda_{rs}): \quad \lambda_{rs} = \begin{cases} 1 & \text{si } r = i, s = j \\ 0 & \text{en otro caso} \end{cases}$$

Se denominan matrices elementales.

Nota: Las matrices elementales son regulares. En efecto

$$\begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & k & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix} \begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & k^{-1} & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix} = I$$

$(I + I_{ij})(I - I_{ij}) = I^2 - I_{ij} + I_{ij} - I_{ij}^2 = I - I_{ij}I_{ij}$. Pero $I_{ij}I_{ij} = 0$ si $i \neq j$, entonces $(I + I_{ij})(I - I_{ij}) = I$. Del teorema (100)(2) se sigue que las transformaciones elementales dejan fijo el rango de una matriz fila.

Otra observación importante es que la inversa de una matriz elemental es el producto de matrices elementales. En efecto

Caso 1:

$$A = \begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & k & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix} \quad \Rightarrow \quad A^{-1} = \begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & k^{-1} & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix}$$

Caso 2: $A = I + I_{ij} \quad \Rightarrow \quad A^{-1} = (I - I_{ij})$ (ver arriba).
Denotemos con $X \to A^{-1}X$: sumamos a la i-esima fila de X (-1)-veces la j-esima fila de X. Del lema (108) se sigue que A^{-1} es el producto de matrices elementales.

$$A^{-1} = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & -1 & & \ddots & \\ & & & & 1 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & -1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & 1 & & \ddots & \\ & & & & 1 \end{pmatrix} \begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & -1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix}$$

Teorema 111.

Sea $A = (a_{ij}) \in (\mathcal{K})_{m,n}$. Entonces matrices elementales $X_1, ..., X_s \in (\mathcal{K})_m$ y $Y_1, ..., Y_s \in (\mathcal{K})_n$ tal que

$$X_1, ..., X_s A Y_1, ..., Y_s = \begin{pmatrix} I_r & | & 0 \\ - & - & - \\ 0 & | & 0 \end{pmatrix}, \text{ donde } r = r(A).$$

DEMOSTRACIÓN.[Constructiva]

Si $A = 0$, entonces el resultado es evidente.
Supongamos entonces que $A \neq 0$. entonces existe $a_{ij} \neq 0$.

Paso 1:

$$A \to \begin{pmatrix} 1 & \tilde{a}_{12} & \cdots & \tilde{a}_{1n} \\ \tilde{a}_{21} & & & \\ \vdots & & * & \\ \tilde{a}_{m1} & & & \end{pmatrix}$$

Paso 2:

$$A \to \begin{pmatrix} 1 & \tilde{a}_{12} & \cdots & \tilde{a}_{1n} \\ 0 & & & \\ \vdots & & * & \\ 0 & & & \end{pmatrix}$$

Paso 3:

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

Si $A^* = 0$, entonces listo!

Si $A^* \neq 0$, entonces repite el proceso para A^*. El resto se sigue del lema (109)

3.4.1 Ejemplo. Sea

$$A = \begin{pmatrix} 0 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \\ 4 & 5 & 6 \end{pmatrix}$$

Aplicando operaciones elementales se obtiene:

$$A \to \begin{pmatrix} 2 & 0 & 3 \\ 3 & 2 & 4 \\ 4 & 3 & 5 \\ 5 & 4 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 3/2 \\ 3 & 2 & 4 \\ 4 & 3 & 5 \\ 5 & 4 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 3/2 \\ 0 & 2 & -1/2 \\ 0 & 3 & -1 \\ 0 & 4 & -3/2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -1/2 \\ 0 & 3 & -1 \\ 0 & 4 & -3/2 \end{pmatrix} \to$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1/4 \\ 0 & 3 & -1 \\ 0 & 4 & -3/2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1/4 \\ 0 & 0 & -1/4 \\ 0 & 0 & -1/2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1/4 \\ 0 & 0 & -1/2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -1/2 \end{pmatrix} \to$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Note entonces que $r(A) = 3$.

Teorema 112.

Sea $A \in (\mathcal{K})_n$ regular. Entonces A es el producto de matrices elementales.

DEMOSTRACIÓN. Del teorema (111) se sigue que existen matrices elementales X_i, Y_j tal que

$$X_1 \cdots X_s A Y_1 \cdots Y_r = I$$

Entonces $A = X_s^{-1} \cdots X_1^{-1} Y_r^{-1} \cdots Y_1^{-1}$. Además se demostró que la inversa de una matriz elemental es el producto de matrices elementales.

Teorema 113.

Sea $A \in (\mathcal{K})_n$ regular. Entonces existen matrices elementales $X_1 \cdots X_s$ tal que $X_1 \cdots X_s A = I$.
(Es decir, es posible utilizar solo transformaciones elementales sobre las filas. Correspondientemente vale para columnas).

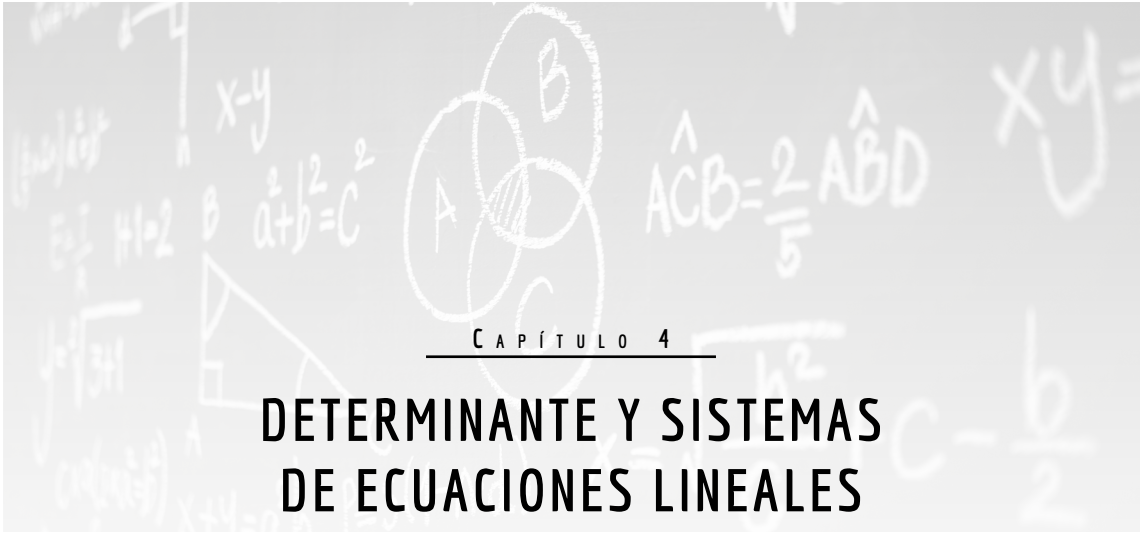
DEMOSTRACIÓN. Dado que A es no singular, existe A^{-1} tal que $A^{-1}A = I$. Del teorema (112) se tiene que A^{-1} es el producto de matrices elementales.

3.4.2 Corolario. Sea A una matriz regular del tipo (n, n). Entonces se puede obtener A^{-1} efectuando sobre I las mismas transformaciones elementales (en el mismo orden) que transforman a A en I.

DEMOSTRACIÓN.

Del teorema (113) $X_1 \cdots X_s A = I$, donde cada X_i es elemental. Multiplicando a la derecha por A^{-1} se tiene:

$$X_1 \cdots X_s I = A^{-1}.$$



Capítulo 4

DETERMINANTE Y SISTEMAS DE ECUACIONES LINEALES

4.1 La función determinante

A lo largo de este capítulo, $(\mathcal{R})_n$ denotará el anillo de las matrices del tipo (n, n) sobre $\mathcal{R}$.

Definición 114.

Sea $A = (a_{ij}) \in (\mathcal{R})_n$. Definamos el determinante de A, denotado $det(A)$ o $\mid A \mid$, como

$$\begin{aligned} det(A) : (\mathcal{R})_n &\longrightarrow \mathcal{R} \\ A &\longrightarrow \sum_{\pi \in S_n} Sgn\pi a_{1\pi(1)} a_{2\pi(2)} \cdots a_{n\pi(n)}. \end{aligned}$$

También podemos ver a det como una función definida sobre las filas o sobre las columnas de A. Esto es,

$$det(A) = f(\underbrace{z_1}_{filas}, ..., z_n) \text{ donde } f : \mathcal{R}^n \times \cdots \times \mathcal{R}^n \to \mathcal{R}$$

o

$$det(A) = f(\underbrace{s_1}_{columnas}, ..., s_n) \text{ donde } f : \mathcal{R}^n \times \cdots \times \mathcal{R}^n \to \mathcal{R}$$

4.1.1 Ejemplos.

1. Sean $n = 1, A = (a_{11})$ y $S_1 = \{I\}$. Entonces,

$$det(A) = \sum_{\pi \in S_1} Sgn\pi a_{1\pi(1)} = a_{11}.$$

2. Sean $n = 2, A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ y $S_2 = \{(1), (12)\}$. Observe que $Sgn(1) = 1$ y $Sgn(12) = -1$. Entonces,

$$det(A) = Sgn(1)a_{11}a_{12} + Sgn(12)a_{21}a_{21} = a_{11}a_{22} - a_{12}a_{21}.$$

3. Sean $n = 3$,

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \text{ y } S_3 = \{(1), (12), (13), (23), (123), (132)\}.$$

Sabemos que $Sgn(ij) = -1, \quad Sgn(123) = Sgn(132) = +1$. Entonces,

$$det(A) = a_{11}a_{22}a_{33} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32}.$$

4. Sea $A = (a_{ij})$ una matriz triangular inferior, i.e $a_{ij} = 0$ para $i < j$.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & 0 \\ a_{12} & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

5. Consideramos $\pi \in S_n, \pi \neq I_\Omega$ y $\Omega = \{1, 2, ..., n\}$. Entonces, existe $i_0 \in \Omega$ tal que $\pi(i_0) > i_0$ (este i_0 depende de π). Probemos por inducción matemática que: Si $\pi(i) \leq i$ para $i \in \{1, 2, ..., r\}$, entonces $\pi(i) = i$ para $i \in \{1, 2, ..., r\}$.

Sea $r = 1$. Si $\pi(1) \leq 1$, evidentemente $\pi(1) = 1$. Supongamos que:

Si $\pi(i) \leq i$ para todo $i \in \{1, 2, ..., r-1\}$, entonces $\pi(i) = i$.

Ahora por hipótesis $\pi(r) \leq r$. Entonces $\pi(r) = r$. Como consecuencia se tiene: Si $\pi \neq I_\Omega$, entonces existe $i_0 \in \Omega$ tal que $\pi(i_0) > i_0$, entonces $a_{i_0}\pi(i_0) = 0$ (por hipótesis A es triangular inferior).

$$det(A) = a_{11}a_{22}\cdots a_{nn} + \underbrace{\sum_{\substack{\pi \in S_n \\ \pi \neq I_\Omega}} Sgn\pi a_{1\pi(1)}a_{2\pi(2)}\cdots a_{n\pi(n)}}_{=0}.$$

Entonces, $det(A) = a_{11}a_{22}\cdots a_{nn}$. Como caso particular: Si A es una matriz diagonal

$$A = \begin{pmatrix} a_{11} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_{nn} \end{pmatrix} \quad ; \quad det(A) = a_{11}\cdots a_{nn}.$$

Además $det(I) = 1$.

Lema 115.

Sea $A = (a_{ij}) \in (\mathcal{R})_n$. Entonces, $det(A) = det(A^t)$.

DEMOSTRACIÓN. Sea $A^t = (b_{ij})$. Entonces, $b_{ij} = a_{ji} \quad \forall i, j$

$$\begin{aligned} det(A^t) &= \sum_{\pi \in S_n} Sgn\pi b_{1\pi(1)}\cdots a_{n\pi(n)} \\ &= \sum_{\pi \in S_n} Sgn\pi a_{\pi(1)1}\cdots a_{\pi(n)n}. \end{aligned}$$

Para cada $j \in \{1, 2, ..., n\}$ existe exactamente un $k \in \{1, 2, ..., n\}$ tal que $\pi(k) = j$. Por lo tanto, $a_{\pi(k)k} = a_{j\pi^{-1}(j)}$ y

$$\begin{aligned} det(A^t) &= \sum_{\pi \in S_n} Sgn\pi a_{1\pi^{-1}(1)} a_{2\pi^{-1}(2)} \cdots a_{n\pi^{-1}(n)} \\ Sgn\pi = Sgn\pi^{-1} &= \sum_{\pi \in S_n} Sgn\pi^{-1} a_{1\pi^{-1}(1)} \cdots a_{n\pi^{-1}(n)} \\ &= \sum_{\pi \in S_n} Sgn\pi a_{1\pi(1)} \cdots a_{n\pi(n)} = det(A) \end{aligned}$$

Lema 116.

Sea $A \in (\mathcal{R})_n$ donde $A = (a_{ij})$.

1. Si existen dos vectores filas de A, z_i, z_j con $i \neq j$ tal que $z_i = z_j$, entonces el $det(A) = 0$.
2. Análogo para columnas.

DEMOSTRACIÓN.

1. Sea $\tau = (ij) \in S_n$. Del teorema (36) se sigue que $S_n = A_n \cup A_n\tau$ y $A_n \cap A_n\tau = \phi$. Entonces,

$$\begin{aligned} det(A) &= \sum_{\pi \in S_n} Sgn\pi a_{1\pi(1)} \cdots a_{n\pi(n)} \\ &= \sum_{\beta \in A_n} (Sgn\beta a_{1\beta(1)} \cdots a_{n\beta(n)} + Sgn\beta\tau a_{1\beta\tau(1)} \cdots a_{n\beta\tau(n)}). \end{aligned}$$

Sabemos que $Sgn\beta = 1$ y $Sgn(\beta\tau) = Sgn\beta \cdot Sgn\tau = -Sgn\beta = -1$. Ahora,

$$det(A) = \sum_{\beta \in A_n} (a_{1\beta(1)} \cdots a_{n\beta(n)} - a_{1\beta\tau(1)} \cdots a_{n\beta\tau(n)})$$

$$= \sum_{\beta \in A_n} (a_{1\beta(1)} \cdots a_{i\beta(i)} \cdots a_{j\beta(j)} \cdots a_{n\beta(n)} - a_{1\beta\tau(1)} \cdots a_{i\beta(j)} \cdots a_{n\beta\tau(n)}).$$

Sin embargo, $a_{i\beta(i)} = a_{j\beta(i)}$ y $a_{i\beta(j)} = a_{j\beta(j)}$ $(z_i = z_j)$. Por lo tanto, $det(A) = 0$.

2. Se sigue del lema (115) y de (1).

Teorema 117.

Consideremos como en la definición (114) $det : (\mathcal{R})_n \to \mathcal{R}$ como la función $f : \underbrace{\mathcal{R}^n \times \cdots \times \mathcal{R}^n}_{n} \to \mathcal{R}$. Sean $\alpha, \beta \in \mathcal{R}$ y $z_i, \tilde{z}_i \in \mathcal{R}^n$, entonces

$$f(z_1, ..., z_{i-1}, \alpha z_i + \beta \tilde{z}_i, z_{i+1}, ..., z_n) = \alpha f(z_1, ..., z_{i-1}, z_i, z_{i+1}, ..., z_n) + \beta f(z_1, ..., z_{i-1}, \tilde{z}_i, z_{i+1}, ..., z_n).$$

DEMOSTRACIÓN. Sean $A = (a_{ij})$, $z_1, z_2, ..., z_n$ las filas de A y $\tilde{z}_i = (\tilde{a}_{i1}, ..., \tilde{a}_{in})$. Entonces,

$$f(z_1, ..., \alpha z_i + \beta \tilde{z}_i, ..., z_n) =$$
$$\sum_{\pi \in S_n} Sgn\pi a_{1\pi(1)} \cdots a_{i-1\pi(i-1)} \cdot (\alpha a_{i\pi(i)} + \beta \tilde{a}_{i\pi(i)}) \cdot a_{i+1\pi(i+1)} \cdots a_{n\pi(n)}$$

$$\begin{aligned} &= \alpha(\sum_{\pi \in S_n} Sgn\pi a_{1\pi(1)} \cdots a_{n\pi(n)} + \beta(\sum_{\pi \in S_n} Sgn\pi a_{1\pi(1)} \cdots \tilde{a}_{i\pi(i)}) \cdot a_{n\pi(n)}) \\ &= \alpha f(z_1, ..., z_n) + \beta f(z_1, ..., z_{i-1}, \tilde{z}_i, z_{i+1}, ..., z_n). \end{aligned}$$

Definición 118.

Una función $h : \mathcal{R}^n \times \cdots \times \mathcal{R}^n \to \mathcal{R}$ se llama una función de volumen sobre $\mathcal{R}^n \times \cdots \times \mathcal{R}^n$ si se cumple:

1. Para cada i y para todo $\alpha, \beta \in \mathcal{R}$:

$$h(z_1, ..., \alpha z_i + \beta \tilde{z}_i, ..., z_n) = \alpha h(z_1, ..., z_n) + \beta h(z_1, ..., \tilde{z}_i, ..., z_n).$$

2. Si $z_i = \tilde{z}_i$ para $i \neq j$, entonces $f(z_1, ..., z_n) = 0$.

4.1.2 Observación. Por el Lema 116 y el Teorema 117 se tiene que la función f como está definida en 114 es una función de volumen.

Teorema 119.

Sea h una función de volumen $\mathcal{R}^n \times \cdots \times \mathcal{R}^n$.

1. $\forall i \neq j$ y para todo $\alpha \in \mathcal{R}$ se cumple

$$h(z_1, ..., z_i + az_j, ..., z_n) = h(z_1, ..., z_n).$$

2. $\forall \pi \in S_n \quad : \quad h(z_{\pi(1)}, ..., z_{\pi(n)}) = Sgn\pi h(z_1, ..., z_n).$

3. Sea $z_i = (a_{i1}, ..., a_{in})$ y $e_j = (\sigma_{j1}, ..., \sigma_{jn})$. Entonces $h(z_1, ..., z_n) = det(a_{ij})h(e_1, ..., e_n)$.

DEMOSTRACIÓN.

1.

$$\begin{aligned} h(z_1, ..., z_i + az_j, ..., z_n) &= h(z_1, ..., z_n) + a \underbrace{h(z_1, ..., z_j, ..., z_n)}_{=0} \\ &= h(z_1, ..., z_n). \end{aligned}$$

2. Consideremos inicialmente $\pi = (ij)$ (una transposición), sin perder generali-

dad $i < j$, entonces

$$\begin{aligned} h(z_1, ..., z_n) &= h(z_1, ..., z_i + z_j, ..., z_j, ..., z_n) \\ &= h(z_1, ..., z_i + z_j, ..., z_j - (z_i + z_j), ..., z_n) \\ &= h(z_1, ..., z_i + z_j, ..., -z_i, ..., z_n) \\ &= h(z_1, ..., (z_i + z_j) - z_i, ..., -z_i, ..., z_n) \\ &= h(z_1, ..., z_j, ..., -z_i, ..., z_n) \\ &= -h(z_1, ..., z_j, ..., z_i, ..., z_n) \\ &= Sgn\pi h(z_1, ..., z_j, ..., z_i, ..., z_n) \end{aligned}$$

Sea $\pi \in S_n$ cualquiera. Sabemos que $\pi = \tau_1 \cdot \cdot \cdot \tau_k$ donde cada τ_j es una transposición. Definamos $\pi' = \tau_2 \cdot \cdot \cdot \tau_k$. Demostremos la afirmación por inducción sobre k.

Paso 1: $k = 1$, demostrado arriba.
Hipótesis de inducción: $h(z_{\pi'(1)}, ..., z_{\pi'(n)}) = Sgn\pi' h(z_1, ..., z_n)$.

Paso 2:

$$\begin{aligned} h(z_{\pi(1)}, ..., z_{\pi(n)}) &= h(z_{\tau_1\pi'(1)}, ..., z_{\tau_n\pi'(n)}) \\ &= Sgn\tau_1 h(z_{\pi'(1)}, ..., z_{\pi'(n)}) \\ &= Sgn\tau_1 Sgn\pi' h(z_1, ..., z_n) \\ &= Sgn\pi h(z_1, ..., z_n). \end{aligned}$$

3. Se verifica que $z_i = \sum_{j=1}^{n} a_{ij} e_j \quad (i = 1, 2, ..., n)$. De la definición (118)(1) se tiene:

$$\begin{aligned} h(z_1, ..., z_n) &= h(\sum_{j=1}^{n} a_{1j_1} e_{j_1}, ..., \sum_{j_n=1}^{n} a_{nj_n} e_{j_n}) \\ h(z_1, ..., z_n) &= \sum_{j_1=1}^{n} \sum_{j_2=1}^{n} \cdots \sum_{j_n=1}^{n} a_{1j_1} \cdot a_{2j_2} \cdots a_{nj_n} h(e_{j_1}, ..., e_{j_n}). \end{aligned}$$

Si en una n-tupla $(j_1, ..., j_n)$ aparece más de una vez un elemento de $\{1, 2, ..., n\}$, entonces de la definición (118)(2) se tiene que $h(e_{j_1}, ..., e_{j_n}) = 0$. Es decir, permanecen libres solo los sumandos con $\{j_1, ..., j_n\} = \{1, 2, ..., n\}$, es decir $j_i = \pi(i)$ para algún $\pi \in S_n$.
Entonces,

$$h(z_1, ..., z_n) = \sum_{\pi \in S_n} a_{1\pi(1)} \cdots a_{n\pi(n)} h(e_{\pi(1)}, \cdots e_{\pi(n)}).$$

Por lo tanto,

$$\begin{aligned} h(z_1, ..., z_n) &= \sum_{\pi \in S_n} Sgn\pi a_{1\pi(1)} \cdots a_{n\pi(n)} h(e_1, \cdots e_n) \\ &= det(A) h(e_1, \cdots e_n) \end{aligned}$$

Teorema 120.

Las funciones de volumen sobre $\mathcal{R}^n \times \cdots \times \mathcal{R}^n$ son las funciones h que tienen exactamente la forma

$$h(z_1, ..., z_n) = C \cdot det \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}, \quad C \in \mathcal{R}.$$

DEMOSTRACIÓN. Es consecuencia del Teorema 119.

Teorema 121.

Sean $A, B \in (\mathcal{R})_n$, entonces $det(AB) = det(A) \cdot det(B)$.

DEMOSTRACIÓN. Sea $A = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$ $B = (\tilde{S}_1, ..., \tilde{S}_n)$. Consideremos

$$h_B : \mathcal{R}^n \times \cdots \times \mathcal{R}^n \to \mathcal{R}$$
$$h_B(z_1, ..., z_n) = det(AB).$$

Demostremos que h_B es una función de volumen: Supongamos que $z_i = z_j$ para $i \neq j$, se tiene:

$$AB = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} (\tilde{S}_1, ..., \tilde{S}_n)$$
$$= \begin{pmatrix} z_1 \\ \vdots \\ z_i \\ \vdots \\ z_j \\ \vdots \\ z_n \end{pmatrix} (\tilde{S}_1, ..., \tilde{S}_n)$$

(la i-esima y j-esima fila de $\sim AB$ son iguales). Por el Lema 116 se sigue que $et(AB) = 0$, por lo tanto $h_B(z_1, ..., z_n) = 0$. Por otro lado,

Sea $A = (a_{ij}), \quad B = (b_{ij})$ y $\tilde{z}_i = (\tilde{a}_{i1}, ..., \tilde{a}_{in})$. Entonces

$$
\begin{aligned}
& h_B(z_1, \ldots, \alpha z_i + \beta \tilde{z}_i, \ldots, z_n) \\
&= \begin{pmatrix}
\sum_{j=1}^{n} a_{1j}b_{j1} & \cdots & \sum_{j=1}^{n} a_{1j}b_{jn} \\
\vdots & & \vdots \\
\sum_{j=1}^{n} (\alpha a_{ij} + \beta \tilde{a}_{ij})b_{j1} & \cdots & \sum_{j=1}^{n} (\alpha a_{ij} + \beta \tilde{a}_{ij})b_{jn} \\
\vdots & & \vdots \\
\sum_{j=1}^{n} a_{nj}b_{j1} & \cdots & \sum_{j=1}^{n} a_{nj}b_{jn}
\end{pmatrix} \\
&= \alpha det(AB) + \beta det \begin{pmatrix}
\sum_{j=1}^{n} a_{1j}b_{j1} & \cdots & \sum_{j=1}^{n} a_{1j}b_{jn} \\
\vdots & & \vdots \\
\sum_{j=1}^{n} \tilde{a}_{ij}b_{j1} & \cdots & \sum_{j=1}^{n} \tilde{a}_{ij}b_{jn} \\
\vdots & & \vdots \\
\sum_{j=1}^{n} a_{nj}b_{j1} & \cdots & \sum_{j=1}^{n} a_{nj}b_{jn}
\end{pmatrix} \\
&= \alpha h_B(z_1, ..., z_n) + \beta h_B(z_1, ..., \tilde{z}_1, ..., z_n)
\end{aligned}
$$

Esto demuestra que h_B es una función de volumen. Entonces

$$\underbrace{h_B(z_1, ..., z_n)}_{=det(AB)} = C(B)det \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = C(B)det(A).$$

Si $A = I$, entonces $C(B) = C(B)det(I) = det(IB) = det(B)$, luego $det(AB) = det(A)det(B)$.

4.1.3 Observación. Como consecuencias de los teoremas (117),(119)(1) y (119)(2):

1. $$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ \alpha a_{i1} + \beta \tilde{a}_{i1} & a_{i2} & & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & & a_{nn} \end{vmatrix} = \alpha \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} + \beta \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ \tilde{a}_{i1} & \cdots & \tilde{a}_{in} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}$$

2. Si $i \neq j$ $$\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{i1} + \alpha a_{j1} & \cdots & a_{in} + \alpha a_{jn} \\ \vdots & & \vdots \\ a_{n1} & & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}$$

3. Si se intercambian dos filas en (a_{ij}), entonces $det(a_{ij})$ se cambia con factor -1. (Similar para columnas).

4.1.4 Ejemplo. Demuestre que:

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ -1 & 0 & 1 & 1 \\ 3 & -1 & 4 & 0 \\ 4 & 3 & 2 & 1 \end{vmatrix} = -45.$$

4.1.5 Ejercicio. Sean $A \in (\mathcal{R})_m$, $B \in (\mathcal{R})_n$ y $C \in (\mathcal{R})_{n,m}$. Entonces

$$det \begin{pmatrix} A & 0 \\ C & B \end{pmatrix} = det(A)det(B).$$

Definición 122.

Sea $A = (a_{ij} = \in (\mathcal{R})_n$. Definimos:

$$A_{ij} := det \begin{pmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & & & & \\ 0 & \cdots & 1 & \cdots & 0 \\ \vdots & & & & \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn} \end{pmatrix}$$

(La i-esima fila de A se reemplaza por e_j).

$$\begin{aligned} A_{ij} &= (-1)^{i-1} det \begin{pmatrix} 0 & \cdots & 1 & \cdots & 0 \\ a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & & & & \\ a_{i-11} & \cdots & a_{i-1j} & \cdots & a_{i-1n} \\ \vdots & & & & \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn} \end{pmatrix} \\ &= (-1)^{i-1+j-1} det \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 \\ a_{1j} & a_{11} & \cdots & a_{1j-1} & \cdots & a_{1n} \\ \vdots & \vdots & & & & \vdots \\ a_{i-1j} & a_{i-11} & \cdots & a_{i-1j-1} & \cdots & a_{i-1n} \\ \vdots & \vdots & & & & \vdots \\ a_{nj} & a_{n1} & \cdots & a_{nj-1} & \cdots & a_{nn} \end{pmatrix} \\ &= (-1)^{i+j} det \underbrace{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}}_{\in (\mathbb{R})_{n-1}}. \end{aligned}$$

(Si $n = 1$, definimos $A_{11} := 1$). Definamos $\tilde{A} := (a_{ij})^t$.

Teorema 123.

Sea $A = (a_{ij} =\in (\mathcal{R})_n$.

1. $A\tilde{A} = det(A)I$, es decir, se cumple que $\sum_{j=1}^{n} a_{ij}A_{ij} = \delta_{ik}det(A)$.

   Caso especial: $i = k, \quad det(A)\sum_{j=1}^{n} a_{ij}A_{ij}$.

   (Desarrollo del determinante de A por la i-esima fila).

2. $\tilde{A}A = det(A)I$, es decir, se cumple que $\sum_{i=1}^{n} A_{ij}a_{ik} = \delta_{jk}det(A)$.

   Caso especial: $j = k, \quad det(A)\sum_{i=1}^{n} A_{ij}a_{ij}$.

   (Desarrollo del determinante de A por la j-esima columna).

3. Si existe $(det(A))^{-1}$ en $\mathcal{R}$, entonces

$$A^{-1} = (det(A))^{-1}\tilde{A}.$$

   (Si $\mathcal{R}$ es un cuerpo, la existencia de A^{-1} significa solo que $det(A) \neq 0$.

DEMOSTRACIÓN.

1. Se cumple:

$$\sum_{j=1}^{n} a_{ij}A_{kj} = \sum_{j=1}^{n} a_{ij} \begin{vmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & & & & \\ 0 & \cdots & 1 & \cdots & 0 \\ \vdots & & & & \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn} \end{vmatrix}$$

$$= \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \\ a_{i1} & \cdots & a_{in} \\ \vdots & & \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = \delta_{ik}det(A).$$

2. Como en la definición (122) se obtiene también que

$$A_{ij} = det \begin{pmatrix} a_{11} & \cdots & 0 & \cdots & a_{1n} \\ \vdots & & & & \\ a_{i1} & \cdots & 1 & \cdots & a_{in} \\ \vdots & & & & \\ a_{n1} & \cdots & 0 & \cdots & a_{nn} \end{pmatrix}.$$

   Entonces (2) se sigue de la misma forma como obtuvimos en (1).

3. Sabemos que $A\tilde{A} = det(A)I$. Si $(det(A))^{-1}$ existe en $\mathcal{R}$ se tiene:

$$A(det(A))^{-1}\tilde{A} = I \text{ y } (det(A))^{-1}\tilde{A}A = I.$$

Por lo tanto A es invertible y $A^{-1} = (det(A))^{-1}\tilde{A}$.

4.1.6 Ejemplo. 1. Desarrollemos el determinante del ejemplo (4.1.4) por la primera fila:

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

$$= (-1)\begin{vmatrix} -1 & 0 \\ 3 & 1 \end{vmatrix} + \begin{vmatrix} -1 & 4 \\ 3 & 2 \end{vmatrix} + (-2)\left(-\begin{vmatrix} 4 & 0 \\ 2 & 1 \end{vmatrix} - \begin{vmatrix} 3 & 0 \\ 4 & 1 \end{vmatrix} + \begin{vmatrix} 3 & 4 \\ 4 & 2 \end{vmatrix}\right)$$

$$+3\left(-\begin{vmatrix} -1 & 0 \\ 3 & 1 \end{vmatrix} + \begin{vmatrix} 3 & -1 \\ 4 & 3 \end{vmatrix}\right) - 4\left(-\begin{vmatrix} -1 & 4 \\ 3 & 2 \end{vmatrix} + \begin{vmatrix} 3 & -1 \\ 4 & 3 \end{vmatrix}\right)$$

$$= -45$$

2. Sea $n > 1$ y $A \in (\mathcal{R})_n$ con

$$A = \begin{pmatrix} a & b & b & \cdots & b & b \\ b & a & b & \cdots & b & b \\ \vdots & & & & & \\ b & b & b & \cdots & a & b \\ b & b & b & \cdots & b & a \end{pmatrix}$$

Definamos $f(a,b,n) := det(A)$. Entonces: Restando la segunda columna de la primera se tiene:

$$\begin{aligned} det(A) &= \begin{vmatrix} a-b & b & \cdots & b \\ b-a & a & \cdots & b \\ \vdots & \vdots & \vdots & \\ 0 & b & & a \end{vmatrix} \\ &= (a-b)f(a,b,n-1) - (b-a)\begin{vmatrix} b & b & \cdots & b \\ b & a & \cdots & b \\ \vdots & \vdots & & \\ b & b & \cdots & a \end{vmatrix} \\ &= (a-b)f(a,b,n-1) + (a-b)\begin{vmatrix} b & 0 & 0 & \cdots & 0 \\ b & a-b & 0 & \cdots & 0 \\ \vdots & & \ddots & & \\ b & 0 & 0 & \cdots & a-b \end{vmatrix} \\ &= (a-b)f(a,b,n-1) + (a-b)b(a-b)^{n-2} \end{aligned}$$

Entonces la fórmula de recurrencia es:

$$f(a,b,n) = (a-b)f(a,b,n-1) + b(a-b)^{n-1}.$$

Afirmación: $f(a,b,n) = (a-b)^{n-1}[a+(n-1)b]$.
Demostración por inducción sobre n:

$n=1 \quad A=(a); \quad det(A) = a$ y $f(a,b,1) = (a-b)^0(a+0b) = a$

$n=2 \qquad A = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \quad \Rightarrow \quad det(A) = a^2 - b^2 = (a-b)(a+b)$

Supongamos que $f(a,b,n-1) = (a-b)^{n-2}(a+(n-2)b)$, entonces

$$\begin{aligned} f(a,b,n) &= (a-b)f(a,b,n-1) + b(a-b)^{n-1} \\ &= (a-b)[(a-b)^{n-2}(a+(n-2)b)] + b(a-b)^{n-1} \\ &= (a-b)^{n-1}(a+(n-2)b) + b(a-b)^{n-1} \\ &= (a-b)^{n-1}(a+(n-2)b+b) \\ &= (a-b)^{n-1}(a+(n-1)b) \end{aligned}$$

Si $\mathcal{R}$ es un cuerpo $det(A) = 0 \Leftrightarrow a = b \quad \vee \quad a+(n-1)b = 0$.

3. Sean $b_1, ..., b_n \in \mathcal{R}$. Consideremos el determinante de Vandermonde.

$$det \begin{pmatrix} 1 & b_1 & b_1^2 & \cdots & b_1^{n-1} \\ 1 & b_2 & b_2^2 & \cdots & b_2^{n-1} \\ \vdots & & & & \\ 1 & b_n & b_n^2 & \cdots & b_n^{n-1} \end{pmatrix} := f(b_1, ..., b_n).$$

Realizamos las siguientes transformaciones:

Multiplicamos la columna $(n-1)$ por b_1 y la restamos a n-esima.

Multiplicamos la columna $(n-2)$ por b_1 y la restamos a $(n-1)$-esima.

Multiplicamos la primera columna por b_1 y la restamos a la segunda.

Entonces tenemos:

$$\begin{aligned} f(b_1, ..., b_n) &= det \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & b_2 - b_1 & (b_2 - b_1)b_2 & \cdots & (b_2 - b_1)b_n^{n-2} \\ \vdots & \vdots & \vdots & & \\ 1 & b_n - b_1 & (b_n - b_1)b_n & \cdots & (b_n - b_1)b_n^{n-2} \end{pmatrix} \\ &= det \begin{pmatrix} b_2 - b_1 & (b_2 - b_1)b_2 & \cdots & (b_2 - b_1)b_n^{n-2} \\ \vdots & \vdots & & \\ b_n - b_1 & (b_n - b_1)b_n & \cdots & (b_n - b_1)b_n^{n-2} \end{pmatrix} \\ &= (b_2 - b_1)(b_3 - b_2) \cdots (b_n - b_1) f(b_2, ..., b_n) \end{aligned}$$

Afirmación: $f(b_2, ..., b_n) = \prod_{i>j}(b_i - b_j)$: Demostración por inducción sobre n:

$n=2 \quad : \quad f(b_1 b_2) = \begin{vmatrix} 1 & b_1 \\ 1 & b_2 \end{vmatrix} = b_2 - b_1$

Supongamos que $f(b_2,...,b_n) = \prod_{\substack{i,j=2 \\ i>j}} (b_i - b_j)$: Entonces

$$\begin{aligned} f(b_2,...,b_n) &= (b_2-b_1)(b_3-b_2)\cdots(b_n-b_1)f(b_2,...,b_n) \\ &= \prod_{\substack{i,j=2 \\ i>j}} (b_i - b_j) \end{aligned}$$

En particular $f(b_2,...,b_n) \neq 0 \Leftrightarrow$ todos los b_i son distintos dos a dos.

Teorema 124.

Sea $\mathcal{K}$ un cuerpo, $A \in (\mathcal{K})_n$. A es regular $\Leftrightarrow det(A) \neq 0$.

DEMOSTRACIÓN. En efecto:

1. Supongamos $det(A) \neq 0$, entonces del teorema (123)(3) se tiene que existe A^{-1} luego A es regular.
2. Supongamos que A es regular, esto es, $AA^{-1} = I$. Entonces $det(AA^{-1}) = det(I)$, luego $1 = det(A) \cdot det(A^{-1})$ por lo tanto $det(A) \neq 0$.

4.1.7 Observación. $\mathbf{G}L(n,\mathcal{K}) = \{A \in (\mathcal{K})_n : det(A) \neq 0\}$. Con respecto a la multiplicación de matrices, se tiene que $\mathbf{G}L(n,\mathcal{K})$ es un grupo. y del teorema (121) se tiene que $det : \mathbf{G}L(n,\mathcal{K}) \to \mathcal{K}^x$ es un homomorfismo de grupos.

$$\mathcal{N}(det) = \{A \in \mathbf{G}L(n,\mathcal{K}) : det(A) = 1\} =: SL(n,\mathcal{K})$$

Entonces $\mathbf{G}L(n,\mathcal{K})/_{SL(n,\mathcal{K})} \cong \mathcal{K}^x$.

Definición 125.

Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{K}$. $dim_k(\mathcal{V}) < \infty$ y sea $A \in Hom_k(\mathcal{V},\mathcal{V})$, definamos $det(A) := det_{\mathfrak{B}}(A)_{\mathfrak{B}}$.

Demostremos que $det(A) := det_{\mathfrak{B}}(A)_{\mathfrak{B}}$ no depende de la elección de $\mathfrak{B}$: Sean $\mathfrak{B}_1, \mathfrak{B}_2$ bases para $\mathcal{V}$. Por el teorema del cambio de base se tiene que existe $X \in (\mathcal{K})_n$ tal que

$$_{\mathfrak{B}_2}(A)_{\mathfrak{B}_2} = X^{-1}{}_{\mathfrak{B}_1}(A)_{\mathfrak{B}_1}X.$$

Entonces:

$$\begin{aligned} det_{\mathfrak{B}_2}(A)_{\mathfrak{B}_2} &= det(X^{-1}{}_{\mathfrak{B}_1}(A)_{\mathfrak{B}_1}X) \\ &= det(X^{-1})det_{\mathfrak{B}_1}(A)_{\mathfrak{B}_1}det(X) \\ &= det_{\mathfrak{B}_1}(A)_{\mathfrak{B}_1}\underbrace{det(X^{-1}X)}_{=1} \end{aligned}$$

Llamaremos a $det(A)$ el determinante de A.

Teorema 126.

Sean $A, B \in Hom_k(\mathcal{V},\mathcal{V})$, entonces $det(AB) = det(A) \cdot det(B)$.

DEMOSTRACIÓN.
Sea $\mathfrak{B}$ una base para $\mathcal{V}$, entonces

$$\begin{aligned} det(AB) = det_{\mathfrak{B}}(AB)_{\mathfrak{B}} &= det({}_{\mathfrak{B}}(A)_{\mathfrak{B}}{}_{\mathfrak{B}}(B)_{\mathfrak{B}}) \\ &= det_{\mathfrak{B}}(A)_{\mathfrak{B}} \cdot det_{\mathfrak{B}}(B)_{\mathfrak{B}} \\ &= det(A) \cdot det(B). \end{aligned}$$

4.2 Sistemas de ecuaciones lineales

Sea $\mathcal{K}$ un cuerpo y supongamos que están dadas una matriz $A = (a_{ij}) \in (\mathcal{K})_{m,n}$ y un vector

$$b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathcal{K}^m.$$

Un problema interesante es calcular (encontrar) un vector

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathcal{K}^n,$$

de tal forma que se verifique

$$AX = b.$$

Es decir

$$\sum_{j=1}^{n} a_{ij}x_j = b_i \quad i = 1, 2, ..., m \tag{4.1}$$

Si $b = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$, entonces (4.1) se denomina un sistema de ecuaciones lineales homogeneas.

Una expansión de (4.1) nos daría:

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

De manera abstracta podemos plantear el problema en términos de operadores lineales definidos sobre espacios vectoriales de dimensión finita:

Problema: Sean $\mathcal{V}$ y $\mathcal{W}$ espacios vectoriales sobre un cuerpo $\mathcal{K}$, $dim_k\mathcal{V} = n, \quad dim_k\mathcal{W} = m$. Dado $A \in Hom_k(\mathcal{V}, \mathcal{W})$ y $w_0 \in \mathcal{W}$, consideremos el sistema

$$Av = w_0 \tag{4.2}$$

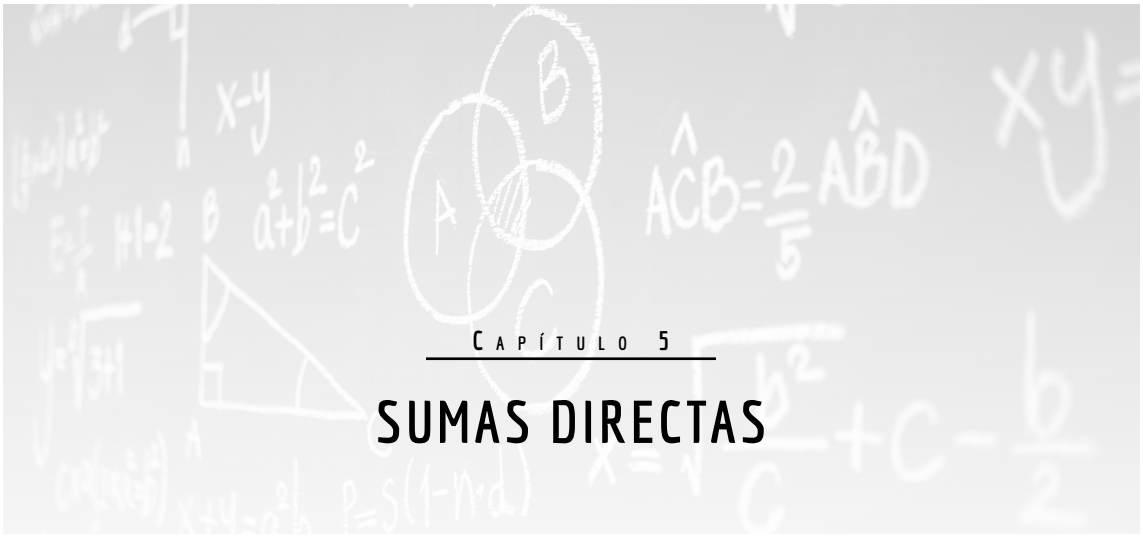
Se trata entonces de encontrar el conjunto de los elementos $v \in \mathcal{V}$ que satisfacen (4.2). Estos v se denominan solución de (4.2).

Nota: Se verifica que (4.1) y (4.2) son equivalentes:

Sean $\mathfrak{B}_1 = (v_1, ..., v_n)$ y $\mathfrak{B}_2 = (w_1, ..., w_m)$ bases para $\mathcal{V}$ y $\mathcal{W}$ respectivamente.
Sea $Av_j = \sum_{i=1}^{m} a_{ij} w_i \quad (j = 1, 2, ..., n), \quad i.e \quad {}_{\mathfrak{B}_2}(A)_{\mathfrak{B}_1} = (a_{ij})$.
Sea $w_0 = \sum_{i=1}^{m} b_i w_i$ y $v = \sum_{j=1}^{n} x_j v_j$. Entonces

$$\begin{aligned}
Av = w_0 \quad &\Leftrightarrow \quad \sum_{i=1}^{m} b_i w_i = A(\sum_{j=1}^{n} x_j v_j) \\
&\Leftrightarrow \quad \sum_{i=1}^{m} b_i w_i = \sum_{j=1}^{n} x_j A v_j \\
&\Leftrightarrow \quad \sum_{i=1}^{m} b_i w_i = \sum_{j=1}^{n} x_j \sum_{i=1}^{m} a_{ij} w_i \\
&\Leftrightarrow \quad \sum_{i=1}^{m} b_i w_i = \sum_{i=1}^{m} (\sum_{j=1}^{n} x_j a_{ij}) w_i \\
&\Leftrightarrow \quad \sum_{j=1}^{n} a_{ij} x_j = b_i \quad i = 1, 2, ..., m.
\end{aligned}$$

Por lo tanto (4.1) y (4.2) son equivalentes.



Capítulo 5

SUMAS DIRECTAS

Recordemos que si $\mathcal{V}$ un espacio vectorial sobre un cuerpo $\mathcal{K}$ y $\mathcal{U}, \mathcal{U}'$ subespacios de $\mathcal{V}$, entonces $\mathcal{V} = \mathcal{U} \oplus \mathcal{U}' \Leftrightarrow \begin{cases} 1. & \mathcal{V} = \mathcal{U} + \mathcal{U}' \\ 2. & \mathcal{U} \cap \mathcal{U}' = \{0\} \end{cases}$

Definición 127.

1. Sea $\mathcal{V}$ un espacio vectorial sobre un cuerpo $\mathcal{K}$ y sean $\mathcal{V}_1, \mathcal{V}_2, ..., \mathcal{V}_m$ subespacios de $\mathcal{V}$. Diremos que $\mathcal{V}$ es la suma directa (interna) de los $\mathcal{V}_i$ si se verifica:
   (a) $\mathcal{V} = \mathcal{V}_1 + \mathcal{V}_2 + ... + \mathcal{V}_m$.
   (b) Si $\sum_{i=1}^{m} v_i = 0$, con $v_i \in \mathcal{V}_i$, entonces $v_i = 0 \quad \forall i$.
2. sean $\mathcal{W}_1, \mathcal{W}_2, ..., \mathcal{W}_m$ espacios vectoriales sobre un cuerpo $\mathcal{K}$. El producto cartesiano $\mathcal{W}_1 \times \mathcal{W}_2 \times ... \times \mathcal{W}_m$ adquiere la estructura de espacio vectorial si definimos:

$$(w_1, ..., w_m) + (\tilde{w}_1, ..., \tilde{w}_m) := (w_1 + \tilde{w}_1, ..., w_m + \tilde{w}_m)$$
$$k(w_1, ..., w_m) := (kw_1, ..., kw_m)$$

   donde $w_i, \tilde{w}_i \in \mathcal{W}_i, \quad k \in \mathcal{K}$.
   $\mathcal{W} = \mathcal{W}_1 \times \mathcal{W}_2 \times ... \times \mathcal{W}_m$ se llama la suma directa externa de los $\mathcal{W}_i$. Utilizamos la misma notación como en (1).

Notación: $\mathcal{V} = \mathcal{V}_1 \oplus \mathcal{V}_2 \oplus ... \oplus \mathcal{V}_n = \bigoplus_{i=1}^{m} \mathcal{V}_i$.

5.0.1 Observación. Sea $\mathcal{K}$ un cuerpo. $\mathcal{K}^n = \underbrace{\mathcal{K} \oplus \mathcal{K} \oplus ... \oplus \mathcal{K}}_{n-sumandos}$.

1. Verificamos que la definición de suma directa presentada en el capítulo 2 y de la definición (127) son equivalentes.
   (a) Sea $\mathcal{V} = \mathcal{U} + \mathcal{U}'$ y $\mathcal{U} \cap \mathcal{U}' = \{0\}$.
   Sea $u + u' = 0$, con $u \in \mathcal{U}$ y $u' \in \mathcal{U}'$, entonces

$$u = -u' \in \mathcal{U} \cap \mathcal{U}' = \{0\}.$$

Por lo tanto $u = u' = 0$.

(b) Sea $\mathcal{V} = \mathcal{U} + \mathcal{U}'$ y supongamos que se cumple:
Si $u + u' = 0$, con $u \in \mathcal{U}$ y $u' \in \mathcal{U}'$, entonces $u = u' = 0$. Sea ahora $u \in \mathcal{U} \cap \mathcal{U}'$. Entonces $u + (-u) = 0 \quad u \in \mathcal{U}, -u' \in \mathcal{U}'$, entonces $u = 0$.

2. Sea $\mathcal{W} = \mathcal{W}_1 \oplus \mathcal{W}_2 \oplus ... \oplus \mathcal{W}_m$ una suma directa externa. Definamos

$$\mathcal{V}_i = \{(0, ..., 0, w_i, 0, ..., 0) : w_i \in \mathcal{W}_i\}.$$

Entonces $\mathcal{W} = \mathcal{W}_1 \oplus \mathcal{W}_2 \oplus ... \oplus \mathcal{W}_m$ es una suma directa interna con $\mathcal{W}_i \cong \mathcal{V}_i$.

Teorema 128.

Sea $\mathcal{V} = \bigoplus_{i=1}^{m} \mathcal{V}_i$ y $\mathfrak{B}_i = (v_{i1}, ..., v_{in_i})$ una base para $\mathcal{V}_i$. Entonces

1. $\mathfrak{B} := (v_{11}, ..., v_{1n_1}, v_{21}, ..., v_{2n_2}, ..., v_{m1}, ..., v_{mn_m})$ es una base para $\mathcal{V}$.

2. Sea $A \in Hom_k(\mathcal{V}, \mathcal{V})$ con $A(v_i) \subseteq \mathcal{V}_i$ para $i = 1, 2, ..., m$. Del teorema (75) se sigue que $Av_i : \mathcal{V}_i \to \mathcal{V}_i$ está definida. Entonces

$$\begin{pmatrix} {}_{\mathfrak{B}_1}(Av_1)_{\mathfrak{B}_1} & & 0 \\ & \ddots & \\ 0 & & {}_{\mathfrak{B}_m}(Av_m)_{\mathfrak{B}_m} \end{pmatrix}$$

DEMOSTRACIÓN.

1. Dado que $\mathcal{V} = \sum_{i=1}^{m} v_i$, se tiene que $\mathfrak{B}$ es un sistema de generadores para $\mathcal{V}$.
Supongamos por otro lado que

$$\sum_{i=1}^{m} \sum_{j=1}^{n_i} k_{ij} v_{ij} = 0; \quad k_{ij} \in \mathcal{K}.$$

Por hipótesis se tiene que $\sum_{j=1}^{n_i} k_{ij} v_{ij} = 0$ y por lo tanto $k_{ij} = 0$.

2. $Av_{ij} = Av_{ij}(v_{ij}) = \sum_{k=1}^{k_i} a_{kj} v_{ik}$.

Teorema 129.

Sean $\mathcal{V}_1, \mathcal{V}_2, ..., \mathcal{V}_m$ subespacios de un espacio vectorial $\mathcal{V}$. Entonces son equivalentes:

1. $\mathcal{V} = \bigoplus_{i=1}^{m} \mathcal{V}_i$.
2. (a) $\mathcal{V} = \sum_{i=1}^{m} \mathcal{V}_i$.
   (b) Para todo j con $1 \leq j \leq m$ se cumple que
   $$(\sum_{i=1}^{m} \mathcal{V}_i) \cap \mathcal{V}_{j+1} = \{0\}.$$

DEMOSTRACIÓN.

(1)⇒(2) Supongamos que $\mathcal{V} = \bigoplus_{i=1}^{m} \mathcal{V}_i$. Entonces se cumple por definción que $\mathcal{V} = \sum_{i=1}^{m} \mathcal{V}_i$.

Supongamos que $\sum_{i=1}^{j} v_i = v_{j+1} \in (\sum_{i=1}^{m} \mathcal{V}_i) \cap \mathcal{V}_{j+1}$. Entonces

$$\sum_{i=1}^{j} v_i - v_{j+1} = 0$$

y se sigue que $v_{j+1} = 0$ (por definición (127)).

(2)⇒(1) Sea $\sum_{i=1}^{k} v_i = 0$, con $v_i \in \mathcal{V}_i$. Sea k maximal con la propiedad $v_k \neq 0$; $k \leq m$. Entonces

$$\sum_{i=1}^{k-1} v_i = -v_k \in (\sum_{i=1}^{k-1} \mathcal{V}_i) \cap \mathcal{V}_k = \{0\}.$$

Lo cual contradice $v_k \neq 0$. Entonces se tiene (b).

Definición 130.

Sea $\mathcal{V}$ un espacio vectorial sobre un cuerpo $\mathcal{K}$. Un operador $p \in Hom_k(\mathcal{V}, \mathcal{V})$ se llama una proyección, si se cumple que $p^2 = p$.

Teorema 131.

Sea $p \in Hom_k(\mathcal{V},\mathcal{V})$ una proyección

1. $\mathcal{V} = \mathcal{N}(p) \oplus Im(p)$.
2. $I - p$ es también una proyección y además
$$\mathcal{N}(p) = Im(I-p) \quad \wedge \quad Im(p) = \mathcal{N}(I-p).$$
3. Sí $\mathfrak{B}_1$ es una base para $Im(p)$ y $\mathfrak{B}_2$ es una base para $\mathcal{N}(p)$. Sea $\mathfrak{B} = (\mathfrak{B}_1, \mathfrak{B}_2)$ como en el teorema (128). Entonces
$${}_{\mathfrak{B}}(p)_{\mathfrak{B}} = \begin{pmatrix} 1 & & & & & 0 \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 0 \end{pmatrix}$$

DEMOSTRACIÓN.

1. (a) Sea $v \in \mathcal{N}(p) \cap Im(p)$. Entonces existe $v' \in \mathcal{V}$ tal que $pv' = v$. Además $Pv = 0$. Entonces
$$0 = pv = p(pv') = p^2v' = pv' = v \quad \Rightarrow \quad \mathcal{N}(p) \cap Im(p) = \{0\}.$$
(b) Sea $v \in \mathcal{V}$ cualquiera. Entonces
$$p(v - pv) = pv - p^2v = pv - pv = 0 \quad \Rightarrow \quad v - pv \in \mathcal{N}(p)$$
y además
$$v = (v - pv) + pv \in \mathcal{N}(p) + Im(p).$$
2. $(I-p)^2 = I^2 - Ip - pI + p^2 = I - p$.
Sea $v \in Im(p)$. Entonces $v = pv'$ para algún $v' \in \mathcal{V}$, entonces
$$pv = p(pv') = p^2v' = pv' = v.$$
Luego
$$v \in \mathcal{N}(p) \Leftrightarrow pv = 0 \Leftrightarrow (I-p)v = v \Leftrightarrow v \in Im(I-p).$$
3. Ejercicio.

5.0.2 Observación. Si $p \in Hom_k(\mathcal{V},\mathcal{V})$ es una proyección, entonces p es una preyección de $\mathcal{V}$ sobre $Im(p)$. Pero p no queda completamente determinado (de manera única) con la información sobre $Im(p)$. Es necesario conocer también $\mathcal{N}(p)$.

5.0.3 Ejemplo. Sea $\mathcal{V} = \langle v_1, v_2\rangle, \quad dim_k\mathcal{V} = 2$. Definamos
$$\begin{array}{ll} p_1v_1 = v_1 & p_2v_1 = v_1 \\ p_1v_2 = 0 & p_2v_2 = v_1 \end{array}$$
Es claro que

$$p_i^2 = p_i \quad i = 1, 2 \qquad Im(p_i) = \langle v_1 \rangle$$
$$\mathcal{N}(p_1) = \langle v_2 \rangle; \quad \mathcal{N}(p_2) = \langle v_1 - v_2 \rangle.$$

Teorema 132.

1. Sea $\mathcal{V} = \bigoplus_{i=1}^{m} \mathcal{V}_i$. Definamos p_i así: $p_i(\sum_{j=1}^{m} v_j) = v_i$ para $v_j \in \mathcal{V}_j$.
   Entonces $p_1, ..., p_m$ son proyecciones y además

$$\sum_{i=1}^{m} p_i = I \quad \text{y} \quad p_i p_j = \delta_{ij} p_i.$$

2. Sean $p_1, ..., p_m$ proyecciones de $\mathcal{V}$ con

$$\sum_{i=1}^{m} p_i = I \quad \text{y} \quad p_i p_j = \delta_{ij} p_i.$$

   Entonces $\mathcal{V} = \bigoplus_{i=1}^{m} Im(p_i)$.

DEMOSTRACIÓN.

1. Es fácil demostrar que cada p_i esta bien definida y que es una proyección.
   Sea $i \neq j$. Entonces

$$(p_i p_j)(\sum_{k=1}^{m} v_k) = p_i(p_j(\sum_{k=1}^{m} v_k)) = p_i v_j = 0$$

   Es decir $p_i p_j = 0$. Además

$$(\sum_{i=1}^{m} p_i)(\sum_{k=1}^{m} v_k) = \sum_{i,k} p_i v_k = \sum_{i=1}^{m} p_i v_i = \sum_{i=1}^{m} v_i.$$

   Entonces $\sum_{i=1}^{m} p_i = I$.

2. (a) Sea $v \in \mathcal{V}$. Entonces $v = Iv = (\sum_{i=1}^{m} p_i)v = \sum_{i=1}^{m} p_i v \in \sum_{i=1}^{m} Im(p_i)$,
   entonces $\mathcal{V} = \sum_{i=1}^{m} Im(p_i)$.

   (b) Sea $0 = \sum_{i=1}^{m} p_i v_i$ con $v_i \in \mathcal{V}$. Tenemos que demostrar que $p_i v_i = 0$ para todo i. Sea $j \neq i$, entonces

$$0 = p_j 0 = p_j(\sum_{i=1}^{m} p_i v_i) = p_j^2 v_j = p_j v_j.$$

5.0.4 Observación. Sea $A, B \in Hom_k(\mathcal{V}, \mathcal{V})$ con $AB = BA$. Entonces

$$B(\mathcal{N}(A)) \subseteq \mathcal{N}(A) \quad \wedge \quad B(Im(A)) \subseteq Im(A).$$

DEMOSTRACIÓN. Sea $v \in \mathcal{N}(A)$, entonces

$$A(Bv) = (AB)v = (BA)v = B(Bv) = B0 = 0 \quad \Rightarrow \quad Bv \in \mathcal{N}(A).$$

Sea ahora $v \in Im(A) \Rightarrow v = Av'$ para algún $v' \in \mathcal{V}$. Entonces

$$Bv = BAv' = ABv' \in Im(A).$$

Teorema 133 (Teorema de Maschke).

Sea $\mathcal{V}$ un espacio vectorial sobre un cuerpo $\mathcal{K}$. $dim_k\mathcal{V} < \infty$. Sea $\mathbf{G} \subseteq Hom_k(\mathcal{V},\mathcal{V})$, $|\mathcal{G}| < \infty$, $\mathbf{G}$ con respecto a la multiplicación de $Hom_k(\mathcal{V},\mathcal{V})$ sea un grupo.
Sea $Char(\mathcal{K}) = 0$ o $Char(\mathcal{K}) = p$ con $p \nmid |\mathbf{G}|$. Sea $\mathcal{U}$ un subespacio de $\mathcal{V}$ $\mathbf{G}$-invariante i.e $g(\mathcal{U}) \subseteq \mathcal{U}\ \forall g \in \mathbf{G}$. Entonces $\mathcal{U}$ admite un complemento en $\mathcal{V}$ que también es $\mathbf{G}$-invariante.

DEMOSTRACIÓN. Hemos demostrado en el capítulo 2 que $\mathcal{U}$ tiene un complemento $\mathcal{U}'$ en $\mathcal{V}$, i.e

$$\mathcal{V} = \mathcal{U} + \mathcal{U}' \quad ; \quad \mathcal{U} \cap \mathcal{U}' = \{0\}.$$

Definamos $p : \mathcal{V} \to \mathcal{V}$ así: $pv = u$ si $v = u + u'$ con $u \in \mathcal{U}, u' \in \mathcal{U}'$. Claramente p es una proyección.
Definamos ahora $Q \in Hom_k(\mathcal{V},\mathcal{V})$ así:

$$Q = \frac{1}{|\mathbf{G}|}\sum_{g\in\mathbf{G}} g^{-1}pg.$$

1. Si $u \in \mathcal{U}$, entonces $Qu = u$:
   Sea $u \in \mathcal{U}$. Entonces $gu \in \mathcal{U}$, ya que $\mathcal{U}$ es $\mathbf{G}$-invariante. Entonces $(g^{-1}pg)u = g^{-1}gu = u$ y se tiene que

$$Q(u) = \frac{1}{|\mathbf{G}|}\sum_{g\in\mathbf{G}} u = \frac{1}{|\mathbf{G}|}|\mathbf{G}|u = u.$$

2. Si $v \in \mathcal{V}$, entonces $Qv \in \mathcal{U}$:

$$(g^{-1}pg)v = \underbrace{g^{-1}\underbrace{(pgv)}_{\in\mathcal{U}}}_{\in\mathcal{U}} \in \mathcal{U} \quad \Rightarrow \quad Qv \in \mathcal{U}.$$

3. $Q^2 = Q$ y además $Im(Q) = \mathcal{U}$:
   Sea $v \in \mathcal{V}$. Entonces $Qv \in \mathcal{U}$ y $Q(Qv) = Qv \quad \Rightarrow \quad Q^2 = Q$.

4. Del teorema (131) se tiene que
   $\mathcal{V} = \mathcal{N}(Q) + Im(Q) = \mathcal{N}(Q) + \mathcal{U} = \mathcal{U} + \mathcal{N}(Q)$.

Demostremos que $\mathcal{N}(Q)$ es $\mathbf{G}$-invariante. note que

$$\begin{aligned} g'Q &= \frac{1}{|\mathbf{G}|}\sum_{g\in\mathbf{G}} g'g^{-1}pg \\ &= \frac{1}{|\mathbf{G}|}\sum_{g\in\mathbf{G}} (g'g^{-1})p(gg'^{-1})g' \\ &= \frac{1}{|\mathbf{G}|}\sum_{g\in\mathbf{G}} (g'g^{-1})p(g'g^{-1})^{-1}g' \\ &= \frac{1}{|\mathbf{G}|}\sum_{h\in\mathbf{G}} (hph^{-1})g' \\ &= Qg' \quad \forall g'\in\mathbf{G} \end{aligned}$$

La conclusión se sigue de la observación (5.0.4). En efecto

$$\forall g\in\mathbf{G} \qquad g(\mathcal{N}(Q)\subseteq\mathcal{N}(Q)$$

Luego $\mathcal{N}(Q)$ es $\mathbf{G}$- invariante.

Nota: La función $\mathbf{G}\ni g\to gg^{-1}\in\mathbf{G}$ es una biyección.

5.0.5 Ejemplo. La condición en el teorema (133) $Char(\mathcal{K})\nmid|\mathbf{G}|$ es necesaria:
Sea $\mathcal{K}=\mathbb{Z}/_{p\mathbb{Z}}$ el cuerpo con p-elementos. Sea $\mathcal{V}=\langle v_1,v_2\rangle$ i.e $dim_k\mathcal{V}=2$. Definamos $A\in Hom_k(\mathcal{V},\mathcal{V})$ así:

$$\begin{aligned} Av_1 &= v_1 \\ Av_2 &= v_1+v_2 \end{aligned}$$

Entonces

$$\begin{aligned} A^j(v_1) &= v_1 \\ A^j(v_2) &= jv_1+v_2 \end{aligned}$$

entonces $A^p=I$ y $\mathbf{G}:=\langle A\rangle$ es un grupo de orden p. Por ejemplo

$$\begin{aligned} A^2(v_2) &= A(Av_2) \\ &= A(v_1+v_2) \\ &= Av_1+Av_2 \\ &= v_1+v_1+v_2 \\ &= 2v_1+v_2 \end{aligned}$$

Sea $\mathcal{U}:=\langle v_1\rangle$. Claramente $\mathcal{U}$ es $\mathbf{G}$-invariante.
Supongamos que $\mathcal{W}$ es un complemento para $\mathcal{U}$, que es $\mathbf{G}$-invariante. Entonces $\mathcal{W}=\langle w\rangle$ y $Aw=aw$ para algún $a\in\mathcal{K}$. Sea $w=xv_1+yv_2$, entonces

$$\begin{aligned} Aw &= xAv_1+yAv_2 \\ &= xv_1+yv_1+yv_2 \\ &= axv_1+ayv_2 \end{aligned}$$

Entonces $ax=x+y \quad\wedge\quad ay=y \quad\Rightarrow\quad a=1;\quad y=0.$

BIBLIOGRAFÍA & REFERENCIAS

[1] Siegfried Bosch. Lineare Algebra. Springer Verlag, 20063.

[2] N. Bourbarki. Eléments de mathématique, Paris, 1962.

[3] P.R. Halmos. Finite-Dimensional Vector Spaces. Springer Verlag, New York , 1974 (engl.).

[4] N. Jacobson. Lecture in Abstract Algebra II. Toronto etc., 1953.

[5] K. Jänisch. Lineare Algebra. Springer Verlag, Berlin etc., 200410.

[6] M. Koecher. Lineare Algebra und Analytische Geometrie. Springer Verlag, Berlin etc.,1983.

[7] Serge Lang. Linear Algebra. Addison-Wesley, Reading, 1970 (engl.).

[8] Serge Lang. Introduction to Linear Algebra. Springer, 1986 (engl.)

[9] S. Lipschutz. Theory and problems of linear algebra. Schaums Überblick/Aufgaben. McGraw-Hill, 1977.

[10] L. Mirsky. An introduction to linear algebra. London, 1965.

[11] G. Strong. Linear Algebra and its applications. Academic Press, 1976.

[12] R. Baer. Linear Algebra and projective geometry. Academic Press, New York, 1952.

[13] J. Herstein. Topics in algebra. Waltham, 1964.

[14] N. Jacobson. Basic Algebra I. San Francisco, 1974.

[15] Serge Lang. Algebra Structures. Addison-Wesley, Reading, 1967.

ACERCA DE LOS AUTORES

Stiven Díaz

Magíster en Matemáticas de la Universidad del Norte, Colombia (2015). Licenciado en Matemáticas de la Universidad del Atlántico, Colombia (2010). Miembro del grupo de Investigación en Matemáticas Uninorte y del grupo de investigación Sistemas Dinámicos y EDOS de la Universidad del Atlántico categorizados en A1 por Colciencias. Entre sus publicaciones se encuentran artículos referentes al estudio de Ecuaciones Diferenciales y Ecuaciones en Diferencias.

Jorge Rodríguez Contreras

Licenciado en Matemática de la Universidad del Atlántico, Colombia (1977). Especialista en Matemática Avanzada de la universidad Nacional, Colombia (1984). Magíster en Matemática de la Universidad Autónoma de Barcelona, España (2000). Doctor en Matemática de la Universidad de Barcelona, España (2003). Director del Grupo de investigación Sistemas Dinámicos y EDOS categorizado en A1 por Colciencias. Entre sus publicaciones se encuentran libros y artículos referentes a las Ecuaciones Diferenciales y Sistemas Dinámicos.

Yesneri Zuleta

Magíster en Matemáticas de la Universidad del Norte, Colombia (2014). Matemático de la Universidad del Atlántico, Colombia (2009). Miembro del Grupo de investigación Sistemas Dinámicos y EDOS categorizado en A1 por Colciencias. Posee una amplia experiencia como docente universitaria y su interés de investigación actual es Ecuaciones Diferenciales, teoría de codificación clásica, codificación de red y sus aplicaciones.