# Matemáticas

Roberto Cadena Vega

2 de enero de 2015

# Índice general

# Todo list

# Capítulo 1

# Álgebra abstracta

## 1.1. Grupos

### Definiciones

**Definición 1.1.1.** Un grupo es un conjunto no vacio G en el que esta definida la operacion $\star$, tal que:

$$\begin{aligned} \star\colon G, G &\to G \\ (a, b) &\to (a \star b) \end{aligned} \tag{1.1.1}$$

Existen definiciones parciales de grupo dependiendo de las propiedades que cumple su operación:

**Cerradura** $a \star b \in G \quad \forall a, b \in G$

**Asociatividad** $a \star (b \star c) = (a \star b) \star c \quad \forall a, b, c, \in G$

**Identidad** $\exists e \in G \ni a \star e = e \star a = a \quad \forall a \in G$

**Inverso** $\exists b \in G \ni a \star b = b \star a = e \quad \forall a \in G$

Cuando se cumplen las propiedades de *cerradura* y *asociatividad* se le llama *semigrupo*; si adicionalmente se cumple la propiedad de *existencia de identidad* se le llama *monoide*; si adicionalmente se cumple la propiedad de *existencia de inverso* se le llama *grupo*.

**Ejercicio 1.1.1.** Demostrar que el grupo cimpuesto por las matrices de la forma:

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}, \quad \forall \theta \in \mathbb{R}$$

es un grupo.

**Definición 1.1.2.** Se dice que un grupo $G$ es abeliano si:

$$a \star b = b \star a \tag{1.1.2}$$

**Ejemplo 1.1.1.** El conjunto $\mathbb{Z}/n\mathbb{Z}$

**Ejercicio 1.1.2.** Consideremos a $\mathbb{Z}$ con el producto usual ¿Es este un grupo?

**Ejercicio 1.1.3.** Consideremos a $\mathbb{Z}^+$ con el producto usual ¿Es este un grupo?

**Ejercicio 1.1.4.** Sea $G = \mathbb{R} \setminus \{0\}$. Si definimos $a \star b = a^2 b$ ¿$G$ es un grupo?

**Definición 1.1.3.** Orden de un grupo es el numero de elementos que tiene dicho grupo y se denota por $|G|$.
Un grupo $G$ será finito si tiene orden finito, de lo contrario será infinito.

**Ejemplo 1.1.2.** Si $G = \{e\}$, su orden será $|G = \{e\}| = 1$

**Ejemplo 1.1.3.** El orden del conjunto de numeros reales es infinito $|\mathbb{R}| = \infty$.

**Proposición 1.1.1.** *Si $G$ es un grupo, entonces:*

1. *El elemento identidad es único.*
2. *El elemento inverso $a^{-1} \quad \forall a \in G$ es único.*
3. *El elemento inverso del inverso del un elemento del grupo es el mismo elemento $\left(a^{-1}\right)^{-1} = a \quad \forall a \in G$.*
4. *El elemento inverso de la operación de dos elementos del grupo es la operacion de los inversos de los elementos en orden inverso $(a \star b)^{-1} = b^{-1} \star a^{-1}$*
5. *En general lo anterior se cumple para cualquier numero de elementos $(a_1 \star a_2 \star \ldots \star a_n)^{-1} = a_n^{-1} \star \ldots \star a_2^{-1} \star a_1^{-1}$.*

*Demostración.*

1. Dados $e_1$ y $e_2$ identidades del grupo, son identicos. Si aplicamos la identidad $e_2$ a $e_1$, tenemos como resultado $e_1$, y si aplicamos la identidad $e_1$ a $e_2$ obtenemos como resultado $e_2$:

$$e_1 = e_2 \star e_1 = e_1 \star e_2 = e_2$$

por lo que podemos ver que ambas identidades son la misma.

2. Sean $b, c$ inversos de $a$, entonces:

$$\begin{aligned} b \star a &= e \\ a \star c &= e \end{aligned}$$

por lo que podemos ver que:

$$b = b \star e = b \star (a \star c) = (b \star a) \star c = e \star c = c$$

3. Sabemos que existe un inverso $a^{-1}$ tal que:

$$a \star a^{-1} = a^{-1} \star a = e \quad \forall a \in G$$

asi pues, se sigue que:

$$\left(a^{-1}\right)^{-1} \star a^{-1} = e$$

y como sabemos que el elemento que operado con el inverso sea la identidad es el elemento mismo tenemos que:

$$\left(a^{-1}\right)^{-1} = a$$

4. Si operamos por la izquierda el termino $b^{-1} \star a^{-1}$ con $a \star b$:

$$\left(b^{-1} \star a^{-1}\right) \star (a \star b) = b^{-1} \star \left(a^{-1} \star a\right) b = b^{-1} \star e \star b = b^{-1} \star b = e$$

de la misma manera si operamos por la derecha:

$$(a \star b) \star \left(b^{-1} \star a^{-1}\right) = a^{-1} \star \left(b^{-1} \star b\right) a = a^{-1} \star e \star a = a^{-1} \star a = e$$

por lo tanto:

$$b^{-1} \star a^{-1} = (a \star b)^{-1}$$

□

## Reglas de cancelación

**Proposición 1.1.2.** *Sea* $G$ *un grupo y* $a, b, c \in G$*, tendremos que:*

$$\begin{aligned} a \star b = a \star c &\implies b = c \\ b \star a = c \star a &\implies b = c \end{aligned} \tag{1.1.3}$$

*Demostración.* Si tomamos en cuenta que $a \star b = a \star c$:

$$b = e \star b = \left(a^{-1} \star a\right) \star b = a^{-1} \star (a \star b) = a^{-1} \star (a \star c) = \left(a^{-1} \star a\right) \star c = e \star c = c$$

de la misma manera para $b \star a = c \star a$:

$$b = b \star e = b \star \left(a \star a^{-1}\right) = (b \star a) \star a^{-1} = (c \star a) \star a^{-1} = c \star \left(a \star a^{-1}\right) = c \star e = c$$

□

## Subgrupos

**Definición 1.1.4.** Un subconjunto no vacio $H$ de un grupo $G$ se llama subgrupo si $H$ mismo forma un grupo respecto a la operación de $G$.
Cuando $H$ es subgrupo de $G$ se denota $H < G$ o $G > H$.

*Observación* 1.1.1. Todo grupo $G$ tiene automaticamente dos subconjuntos triviales, el mismo $G$ y la identidad $\{e\}$.

**Proposición 1.1.3.** *Un subconjunto no vacio $H \subset G$ es un subgrupo de $G$ si y solo si $H$ es cerrado respecto a la operación de $G$ y $a \in H \implies a^{-1} \in H$.*

*Demostración.* Teniendo que $H$ es un subgrupo de $G$ tenemos que $H$ es un grupo, por lo que automaticamente se cumple la cerradura y la existencia del inverso dentro del subgrupo.

Teniendo que $H$ es cerrado, no vacio y $a^{-1} \in H \quad \forall a \in H$. Sabemos que $a^{-1} \star a = e \in H$ debido a que $H$ es cerrado. Ademas para $a, b, c \in H$ sabemos que $a \star (b \star c) = (a \star b) \star c$ debido a que se cumple en $G$ y $H$ hereda esta propiedad.

Por lo que $H$ es un grupo, y por lo tanto subgrupo de $G$. □

**Ejemplo 1.1.4.** Sea $G = \mathbb{Z}$ con la suma usual y sea $H$ el conjunto de los enteros pares, es decir:

$$H = \{2n | n \in \mathbb{Z}\}$$

¿Es $H$ un subgrupo de $G$?
Empecemos con dos elementos $a, b \in H$, por lo que tenemos que:

$$\begin{array}{rcl} a & = & 2q \quad q \in \mathbb{Z} \\ b & = & 2q' \quad q' \in \mathbb{Z} \end{array}$$

y al sumarlos tenemos que:

$$a + b = 2q + 2q' = 2(q + q') = 2q'' \quad q'' \in \mathbb{Z}$$

por lo que $a + b \in H$.
Por otro lado, para $a \in H$ existe un $q \in \mathbb{Z}$ tal que $a = 2q$. Su inverso será:

$$-a = -2q = 2(-q)$$

por lo que existe $q' = -q \in \mathbb{Z}$ tal que:

$$2q' = -a \in H$$

y por lo tanto $H < \mathbb{Z}$.

**Ejemplo 1.1.5.** Consideremos $G = \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ con el producto usual, y un subconjunto $\mathcal{U}$

$$\mathcal{U} = \{z \in \mathbb{C}^* \mid |z| = 1\}$$

¿Es $\mathcal{U}$ un subgrupo de G?
Dados dos elementos $z_1, z_2 \in \mathcal{U}$ sabemos que $|z_1| = |z_2| = 1$, por lo tanto:

$$|z_1 z_2| = |z_1||z_2| = 1$$

por lo que $z_1 z_2 \in \mathcal{U}$.
Por otro lado, para $z \in \mathcal{U}$ tenemos que $|z| = 1$, y por lo tanto:

$$|z^{-1}| = |z|^{-1} = \frac{a}{|z|} = 1$$

por lo que $z^{-1} \in \mathcal{U}$ y $\mathcal{U} < \mathbb{C}^*$

**Ejemplo 1.1.6.** Sea G un grupo, $a$ un elemento del grupo y $C(a) = \{g \in G \mid g \star a = a \star g\}$ ¿Es $C(a)$ subgrupo de G?
Primero notamos que $C(a)$ es no vacio debido a que al menos tiene a la identidad.

$$e \star a = a \star e \implies e \in C(a)$$

Ahora tomemos dos elementos $g_1, g_2 \in C(a)$, para los cuales:

$$\begin{aligned} g_1 \star a &= a \star g_1 \\ g_2 \star a &= a \star g_2 \end{aligned}$$

Ahora, si operamos estos dos elementos tendremos:

$$(g_1 \star g_2) \star a = g_1 \star (g_2 \star a) = g_1 \star (a \star g_2) = (g_1 \star a) \star g_2 = (a \star g_1) \star g_2 = a \star (g_1 \star g_2)$$

por lo que $g_1 \star g_2 \in C(a)$.
Por ultimo, podemos ver que:

$$a = a \star e = a \star \left(g \star g^{-1}\right) = (g \star a) \star g^{-1}$$

En donde para que el elemento inverso exista en $C(a)$, se debe de cumplir que $g^{-1} \star a = a \star g^{-1}$:

$$g^{-1} \star a = g^{-1} \star \left((g \star a) \star g^{-1}\right) = g^{-1} \star (g \star a) \star g^{-1} = g^{-1} \star g \star a \star g^{-1} = e \star a \star g^{-1} = a \star g^{-1}$$

Por lo que $C(a) < G$.

**Ejercicio 1.1.5.** Sea $X$ un conjunto no vacio. Consideremos $G = \delta X$. Sea $a \in X$, $H(a) = \{f \in \delta X \mid f(a) = a\}$. Verificar que $H \subset G$ es un subgrupo bajo la composición de funciones. Note que $H(a)$ es no vacio, debido a que $id_X \in H(a)$.

**Definición 1.1.5.** Sea $G$ un grupo y $a \in G$. El conjunto

$$A = \langle a \rangle = \left\{ a^i \mid i \in \mathbb{Z} \right\} \tag{1.1.4}$$

es un subgrupo de $G$.
$A$ es no vacio, puesto que $a^0 = e \in A$.
Por otro lado, para dos elementos $a^i, a^j \in A$ tenemos que:

$$a^i a^j = a^{i+j} \in A$$

y para un elemento $a^i \in A$, tenemos que:

$$a^{-i} = \left(a^i\right)^{-1} = \left(a^{-1}\right)^i \in A$$

por lo que $\langle a \rangle$ es un subgrupo. A este se le llama subgrupo cíclico de $G$ generado por $a$.

**Definición 1.1.6.** Sea $G$ un grupo, decimos que $G$ es cíclico si $G = \langle a \rangle$ para algun $a \in G$.

**Ejemplo 1.1.7.** Dado el grupo $G = \{e\}$, tenemos que el subgrupo cíclico generador de $G$ es:

$$\langle e \rangle = \left\{ e^i \in G \mid i \in \mathbb{Z} \right\}$$

al operar este subgrupo tenemos:

$$\begin{aligned} e^1 &= e \\ e^2 &= e \star e = e \\ e^3 &= e \star e \star e = e \end{aligned}$$

por lo que obtenemos todos los elementos del grupo.

**Ejemplo 1.1.8.** Dado el grupo $G = \{a, e\}$, y la siguiente tabla para la operación del grupo:

| $\star$ | e | a |
|---|---|---|
| e | e | a |
| a | a | e |

con esto, tenemos que el subgrupo ciclico generador de $G$ es:

$$\langle a \rangle = \left\{ a^i \in G \mid i \in \mathbb{Z} \right\}$$

y al operar este subgrupo tenemos:

$$\begin{aligned} a^1 &= a \\ a^2 &= a \star a = e \end{aligned}$$

y obtenemos todos los elementos del grupo.

**Ejercicio 1.1.6.** Dado el grupo $G = \{e, a, b\}$ y la operación:

| $\star$ | e | a | b |
|---|---|---|---|
| e | e | a | b |
| a | a | b | e |
| b | b | e | a |

Encontrar el subgrupo cíclico generador.

**Ejercicio 1.1.7.** Dado el grupo $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2 = \{[0], [1]\}$ con la operación $[a] + [b]$; encontrar el subgrupo cíclico generador.

**Ejercicio 1.1.8.** Sea G un grupo en el que $x^2 = e$ para todo $x \in G$. Verificar que G es abeliano, es decir $a \star b = b \star a$.

**Definición 1.1.7.** Sea G un grupo, H un subgrupo de G ($H < G$), para $a, b \in G$, decimos que $a$ es congruente con $b \mod H$, denotado por:

$$a \cong b \mod H \tag{1.1.5}$$

si

$$a \star b^{-1} \in H \tag{1.1.6}$$

**Ejercicio 1.1.9.** Demostrar que $\cong$ es una relación de equivalencia.

**Definición 1.1.8.** Si H es un subgrupo de G y $a \in G$, entonces

$$Ha = \{ha \mid h \in H\} \tag{1.1.7}$$

se llama clase lateral derecha de H en G.

**Lema 1.1.1.** *Para todo $a \in G$ se tiene que:*

$$Ha = \{x \in G \mid a \cong x \mod H\} \tag{1.1.8}$$

*Demostración.* Sea un conjunto definido como $[a] = \{x \in G \mid a \cong x \mod H\}$, por verificar que $Ha = [a]$. Para verficar esto, tenemos que verificar que $Ha \subseteq [a]$ y despues que $[a] \subseteq Ha$.

Para verificar que $Ha \subseteq [a]$ definimos un elemento $h \in H$ y $ha \in Ha$, si ahora operamos $a$ con $(ha)^{-1}$ y verificamos que esta en H, podemos decir que $a \cong ha \mod H$:

$$a(ha)^{-1} = a(a^{-1}h^{-1}) = (aa^{-1})h^{-1} = h^{-1} \in H$$

por lo que podemos concluir que $a \cong ha \mod H$, lo que implica que $ha \in [a]$; pero como $ha$ es un elemento arbitrario de $Ha$, tenemos que:

$$Ha \subseteq [a]$$

Para verificar que $[a] \subseteq Ha$ empezamos con un elemento $x \in [a]$, es decir $a \cong x \mod H$, lo cual implica $ax^{-1} \in H$, en particular nos interesa:

$$(ax^{-1})^{-1} = xa^{-1} \in H$$

Por otro lado, sea $h = xa^{-1} \in H$, entonces tenemos que:

$$ha = (xa^{-1})a = x(a^{-1}a) = x \in Ha$$

por lo que podemos decir que:

$$[a] \subseteq Ha$$

y por lo tanto

$$[a] = Ha$$

$\square$

**Teorema 1.1.1.** *Sea* $G$ *un grupo finito y* $H \subset G$*, entonces el orden de* $H$ *divide al orden de* $G$

$$^{|H|}/_{|G|} \tag{1.1.9}$$

*y esto implica que existe una* $k \in \mathbb{Z}$ *tal que:*

$$|G| = k|H| \tag{1.1.10}$$

*A esto se le conoce como Teorema de Lagrange.*

*Demostración.* Dado $[a] = Ha$, las clases de equivalencia forman una partición de $G$:

$$\begin{aligned} [a_1] \cup [a_2] \cup \cdots \cup [a_k] &= G \\ [a_i] \cap [a_j] &= \varnothing \quad i \neq j \end{aligned}$$

Por otro lado, las clases laterales derechas forman una partición:

$$\begin{aligned} Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k &= G \\ Ha_i \cap Ha_j &= \varnothing \quad i \neq j \end{aligned}$$

Establezcamos una biyección:

$$\begin{aligned} Ha_i &\to H \\ ha_i &\to h \end{aligned}$$

es decir, el orden de $Ha_i$ es el orden de $H$

$$|Ha_i| = |H| \quad \forall 1 \leqslant i \leqslant k$$

entonces:

$$\begin{aligned} |G| &= |Ha_1| + |Ha_2| + \cdots + |Ha_k| \\ &= |H| + |H| + \cdots + |H| \\ |G| &= k|H| \end{aligned}$$

pero $k \in \mathbb{Z}$, entonces:

$$|H|/|G|$$

□

**Definición 1.1.9.** Si G es finito y H es un subgrupo de G llamamos $\frac{|G|}{|H|}$ el indice de H en G y lo denotamos por $i_G(H)$.

**Definición 1.1.10.** Si G es finito y $a \in G$, llamamos orden de $a$ al mínimo entero positivo $n$ tal que $a^n = e$ y lo denotamos por $O(a)$, por lo que se sigue que:

$$a^{O(a)} = e \tag{1.1.11}$$

**Proposición 1.1.4.** *Si* G *es finito y* $a \in G$, *entonces el orden de* $a$ *divide al orden de* G*:*

$$O(a)/|G| \tag{1.1.12}$$

*Demostración.* Supongamos $H = \langle a \rangle$, entonces $O(a) = |H|$. Podemos ver ahora, por el teorema de Lagrange:

$$|H|/|G| \implies O(a)/|G|$$

□

**Corolario 1.1.1.** *Si* G *es un grupo finito de orden* $n$, *entonces:*

$$a^n = e \quad \forall a \in G \tag{1.1.13}$$

*Demostración.* Por la proposición anterior tenemos que:

$$O(a)/|G| = O(a)/n$$

esto equivale a decir que existe un $k \in \mathbb{Z}$, tal que $n = kO(a)$, entonces podemos decir:

$$a^n = a^{kO(a)} = \left(a^{O(a)}\right)^k = e^k = e \quad \forall a \in G$$

□

## Subgrupo Normal

**Definición 1.1.11.** Un grupo $N$ de $G$ se dice que es un subgrupo normal de $G$ denotado por $N \triangle G$, si para todo $g \in G$ y para todo $n \in N$ se tiene que:

$$gng^{-1} \in N \tag{1.1.14}$$

**Lema 1.1.2.** $N$ *es un subgrupo normal de* $G$ *si y solo si:*

$$gNg^{-1} = N \quad \forall g \in G \tag{1.1.15}$$

*Demostración.* Si $gNg^{-1} = N \quad \forall g \in G$, entonces en particular tenemos que:

$$gNg^{-1} \subseteq N$$

por lo que se tiene que $gng^{-1} \in N \quad \forall n \in N$, por lo tanto $N \triangle G$.
Por otro lado, si $N$ es un subgrupo normal de $G$, entonces tenemos que:

$$gng^{-1} \in N$$

para todo $g \in G$ y para todo $n \in N$, esto implica que:

$$gNg^{-1} \subseteq N$$

Por ultimo, podemos ver que $g^{-1}Ng = g^{-1}N\left(g^{-1}\right)^{-1} \subseteq N$, ademas:

$$N = eNe = g\left(g^{-1}Ng\right)g^{-1} \subseteq gNg^{-1}$$

por lo tanto, podemos concluir que $gNg^{-1} = N$ □

**Lema 1.1.3.** *El subgrupo* $N$ *de* $G$*, es un subgrupo normal de* $G$ $(N \triangle G)$*, si y solo si toda clase lateral izquierda de* $N$ *en* $G$ *es una clase lateral derecha de* $N$ *en* $G$.

*Demostración.* Sea $aH = \{ah \mid h \in H\}$ la clase lateral izquierda de $H$.
Si $N$ es un subgrupo normal de $G$, para todo $g \in G$ y para todo $n \in N$, tenemos que:

$$gNg^{-1} = N$$

entonces tenemos que:

$$gN = gNe = gN\left(g^{1}g\right) = \left(gNg^{-1}\right)g = Ng$$

por lo que toda clase lateral izquierda coincide con la clase lateral derecha.
Por otro lado, si ahora suponemos que las clases laterales coinciden, entonces:

$$gNg^{-1} = (gN)\,g^{-1} = Ngg^{-1} = N$$

por lo que podemos concluir que se trata de un subgrupo normal. □

**Definición 1.1.12.** Denotamos ${}^{G}/_{N}$ a la colección de las clases laterales derechas de $N$ en $G$.

$$ {}^{G}/_{N} = \{Na \mid a \in G\} \tag{1.1.16} $$

**Teorema 1.1.2.** *Si $G$ es un grupo y $N$ es un subgrupo normal de $G$, entonces ${}^{G}/_{N}$ es tambien un grupo y se denomina grupo cociente.*

*Demostración.* Para demostrar la existencia de identidad primero verificamos que para un elemento $x \in {}^{G}/_{N}$, el elemento tiene la forma $x = Na \quad a \in G$, por lo que podemos ver que:

$$
\begin{aligned}
xNe = xN = NaN = NNa = Na &= x \\
Nex = Nx = NNa = Na &= x
\end{aligned}
$$

□

Para demostrar la existencia de un inverso definimos un elemento $x \in {}^{G}/_{N}$ y $Na^{-1} \in {}^{G}/_{N}$, y queremos demostrar que $x^{-1} = Na^{-1}$ es el inverso de $x = Na$. Al operar estos elementos por la derecha y la izquierda tenemos:

$$
\begin{aligned}
xx^{-1} = NaNa^{-1} = NNaa^{-1} = Ne &= N \\
x^{-1}x = Na^{-1}Na = NNa^{-1}a = Ne &= N
\end{aligned}
$$

por lo tanto $Na^{-1} = x^{-1}$ es el inverso de $x$. Por lo tanto, ${}^{G}/_{N}$ es un grupo.

## Homomorfismos de grupo

**Definición 1.1.13.** Sea una aplicación $\varphi\colon G \to \bar{G}$, $G$ un grupo con operacion $\circ$ y $\bar{G}$ un grupo con operación $\diamond$. Se dice que $\varphi$ es un homomorfismo si para $a, b \in G$ cualesquiera se tiene que:

$$ \varphi(a \circ b) = \varphi(a) \diamond \varphi(b) \tag{1.1.17} $$

**Ejemplo 1.1.9.** Sea $G = \mathbb{R}^{+} \setminus \{0\}$, bajo el producto usual y sea $\bar{G} = \mathbb{R}$ bajo la adición, definimos $\varphi\colon G \to \bar{G}$ como:

$$
\begin{aligned}
\varphi\colon \mathbb{R}^{+} \setminus \{0\} &\to \mathbb{R} \\
r &\to \ln r
\end{aligned}
$$

Sean $r_1, r_2 \in \mathbb{R}^{+} \setminus \{0\}$ tal que:

$$ \varphi(r_1 \cdot r_2) = \ln(r_1 \cdot r_2) = \ln r_1 + \ln r_2 = \varphi(r_1) + \varphi(r_2) $$

por lo que podemos asegurar que $\varphi$ es un homomorfismo.

**Lema 1.1.4.** *Supongamos que* $G$ *es un grupo y que* $N$ *es un subgrupo normal de* $G$. *Definamos la aplicación:*

$$\begin{aligned} \varphi\colon G &\to {}^{G}/_{N} \\ x &\to Nx \end{aligned}$$

*entonces* $\varphi$ *es es un homomorfismo.*

*Demostración.* Sean $x, y \in G$, entonces $\varphi(x) = Nx$ y $\varphi(y) = Ny$, por lo que podemos ver que:

$$\varphi(x \circ y) = Nxy = NNxy = NxNy = \varphi(x) \diamond \varphi(y)$$

por lo que $\varphi$ es un homomorfismo. □

**Definición 1.1.14.** Si $\varphi$ es un homomorfismo de $G$ en $\bar{G}$, el nucleo de $\varphi$, denominado $\ker \varphi$ se define:

$$\ker \varphi = \{x \in G \mid \varphi(x) = \bar{e}\} \tag{1.1.18}$$

donde $\bar{e}$ es la identidad de $\bar{G}$.

**Lema 1.1.5.** *Si* $\varphi$ *es un homomorfismo de* $G$ *es* $\bar{G}$, *entonces:*

1. $\varphi(e) = \bar{e}$
2. $\varphi(x^{-1}) = \varphi(x)^{-1} \quad \forall x \in G$

*Demostración.* Para demostrar la primera parte tenemos un elemento $x \in G$, por lo que:

$$\varphi(x) \diamond \bar{e} = \varphi(x) = \varphi(x \circ e) = \varphi(x) \diamond \varphi(e)$$

por lo que $\bar{e} = \varphi(e)$
Para demostrar la segunda parte, notamos que:

$$\begin{aligned} \bar{e} = \varphi(e) &= \varphi(x \circ x^{-1}) = \varphi(x) \diamond \varphi(x^{-1}) = \bar{e} \\ &= \varphi(x^{-1} \circ x) = \varphi(x^{-1}) \diamond \varphi(x) = \bar{e} \end{aligned}$$

por lo que $\varphi(x)^{-1} = \varphi(x^{-1})$. □

**Ejercicio 1.1.10.** Sea $G$ un grupo abeliano, tenemos que:

$$\begin{aligned} \varphi\colon G &\to G \\ a &\to a^2 \end{aligned}$$

Verificar que $\varphi$ es un homomorfismo.

**Ejercicio 1.1.11.** Sea $G$ y $G'$ dos grupos y sea $e'$ la identidad en $G'$, entonces:

$$\begin{aligned} \varphi\colon G &\to G' \\ g &\to e' \end{aligned}$$

verificar que $\varphi$ rd un homomorfismo.

**Ejercicio 1.1.12.** La identidad dada por:

$$\begin{aligned} id_G\colon G &\to G \\ g &\to g \end{aligned}$$

verificar que $id_G$ es un homomorfismo.

**Ejercicio 1.1.13.** Sea $G = \mathbb{Z}$ con la suma usual y $G' = \{1, -1\}$ con el producto usual. Si definimos:

$$\begin{aligned} \varphi\colon \mathbb{Z} &\to \{1,-1\} \\ n &\to \begin{cases} 1 & \text{si } n \text{ es par} \\ -1 & \text{si } n \text{ es impar} \end{cases} \qquad \forall n \in G \end{aligned}$$

¿Será $\varphi$ un homomorfismo?

**Ejercicio 1.1.14.** Sean $G = \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ con el producto correspondiente y $G' = \mathbb{R}^+$ con el producto correspondiente. Entonces definimos:

$$\begin{aligned} \varphi\colon \mathbb{C}^* &\to \mathbb{R}^+ \\ z &\to |z| \end{aligned}$$

¿Será $\varphi$ un homomorfismo?

**Ejercicio 1.1.15.** Definimos:

$$\begin{aligned} \varphi\colon \mathbb{Z} &\to \mathbb{Z}_n \\ a &\to [a] \end{aligned}$$

y sabemos que:

$$[a + b] = [a] + [b]$$

¿Será $\varphi$ un homomorfismo?

**Definición 1.1.15.** Un homomorfismo $\varphi\colon G \to G'$ se dice que es:

**Monomorfismo** si es inyectivo (1 - 1).

**Epimorfismo** si es suprayectivo (sobre).

**Isomorfismo** si es biyectivo (1 - 1 y sobre).

**Definición 1.1.16.** Si $\varphi\colon G \to G'$ es un isomorfismo, decimos que $G$ y $G'$ son isomorfos y escribimos:

$$G \cong G' \tag{1.1.19}$$

**Proposición 1.1.5.** *Si $\varphi\colon G \to G'$ es un homomorfismo, entonces:*

$$\operatorname{im}\varphi < G' \tag{1.1.20}$$

*donde:*

$$\operatorname{im}\varphi = \left\{x \in G, y \in G' \mid \varphi(x) = y\right\} \subset G' \tag{1.1.21}$$

*Demostración.* Para demostrar que $\operatorname{im}\varphi$ es un subgrupo de $G'$, tenemos que demostrar que esta contenido en $G'$ y que es grupo, pero por definición sabemos que $\operatorname{im}\varphi \subset G'$, por lo que solo nos queda demostrar que es un grupo. Para demostrar que es un grupo, pasamos a verificar la cerradura y la existencia de un inverso.

Para demostrar la propiedad de cerradura, tomamos dos elementos $y_1, y_2 \in \operatorname{im}\varphi$ tales que tienen la forma:

$$\begin{aligned} y_1 &= \varphi(x_1) \in G' \qquad & x_1 \in G \\ y_2 &= \varphi(x_2) \in G' \qquad & x_2 \in G \end{aligned}$$

por lo que al operarlos entre si tenemos:

$$y_1 y_2 = \varphi(x_1)\varphi(x_2) = \varphi(x_1 x_2) = y_1 y_2 \in \operatorname{im}\varphi$$

Por otro lado, para demostrar la existencia de un inverso, operamos un elemento $y = \varphi(x) \in \operatorname{im}\varphi$ con el elemento $\varphi(x^{-1})$, el cual queremos demostrar es el inverso.

$$\begin{aligned} \varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(e) &= e' \in G' \\ \varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(e) &= e' \in G' \end{aligned}$$

por lo que se concluye que el inverso es:

$$\varphi(x)^{-1} = \varphi(x^{-1})$$

y por lo tanto $\operatorname{im}\varphi$ es subgrupo de $G'$. □

**Definición 1.1.17.** Sea $\varphi\colon G \to G'$ un homomorfismo, el nucleo de $\varphi$ es:

$$\ker \varphi = \left\{a \in G \mid \varphi(a) = e'\right\} \subset G \tag{1.1.22}$$

*Observación* 1.1.2.

$$\ker \varphi = \left\{\varphi^{-1}(e') \mid a = \varphi^{-1}(e'), a \in G\right\} \tag{1.1.23}$$

son las preimagenes de $e'$.

**Proposición 1.1.6.** *Sea $\varphi\colon G \to G'$ un homomorfismo. Entonces $\varphi$ es un monomorfismo, si y solo si:*

$$\ker \varphi = \{0\} \tag{1.1.24}$$

*es decir $e = 0 \in G$.*

*Demostración.* Si suponemos que $\ker \varphi = \{0\}$, tenemos que para dos elementos $\varphi(x_1)$ y $\varphi(x_2)$ iguales:

$$\begin{aligned} \varphi(x_1) &= \varphi(x_2) \\ \varphi(x_1) - \varphi(x_2) &= 0 \\ \varphi(x_1 - x_2) &= 0 \end{aligned}$$

por lo que $x_1 - x_2 \in \ker \varphi$, lo cual implica que:

$$\begin{aligned} x_1 - x_2 &= 0 \\ x_1 &= x_2 \end{aligned}$$

por lo que podemos concluir que $\varphi$ es un monomorfismo. □

**Teorema 1.1.3.** *Si $\varphi$ es un homomorfismo, entonces se satisface que:*

1. $\ker \varphi < G$
2. $a^{-1} \ker \varphi a \subseteq \ker \varphi \quad \forall a \in G$

*Demostración.* Sabemos que $\ker \varphi \neq \varnothing$, ya que existe un $e \in G$ tal que $\varphi(e) = e'$. Por lo que pasamos a comprobar que $\ker \varphi$ es un grupo, ya que por definición $\ker \varphi \subset G$. Para comprobar que $\ker \varphi$ definimos dos elementos $x, y \in \ker \varphi$, por lo que al operarlos entre si tenemos:

$$\varphi(xy) = \varphi(x)\varphi(y) = e'e' = e'$$

por lo que $xy \in \ker \varphi$.
Por otro lado, para un elemento $x \in \ker \varphi$, para el cual $\varphi(x) = e'$, tenemos que:

$$\varphi(x^{-1}) = \varphi(x^{-1})e' = \varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(e) = e'$$

por lo que podemos ver que existe un inverso $x^{-1} \in \ker\varphi$ y por lo tanto conlcuir que $\ker\varphi < G$.

Para comprobar la segunda proposición tomamos un elemento $a \in G$ y un elemento $g \in \ker\varphi$, para el cual $\varphi(g) = e'$, por lo que queremos verificar que:

$$a^{-1}ga \in \ker\varphi \quad \forall g \in \ker\varphi$$

Sabemos que cualquier elemento en $\ker\varphi$, al evaluarlo en $\varphi$, obtendremos la identidad, por lo que procederemos a tratar de obtenerla:

$$\begin{aligned} \varphi(a^{-1}ga) &= \varphi(a^{-1})\varphi(g)\varphi(a) = \varphi(a^{-1})e'\varphi(a) \\ &= \varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(e) = e' \end{aligned}$$

por lo que podemos concluir que:

$$\varphi(a^{-1}ga) \in \ker\varphi$$

□

*Observación* 1.1.3. $\ker\varphi$ es un subgrupo normal de $G$.

**Ejercicio 1.1.16.** Sea $\varphi$ definida como:

$$\begin{aligned} \varphi\colon \mathbb{Z} &\to \{-1, 1\} \\ n &\to \begin{cases} -1 & \text{si } n \text{ es par} \\ 1 & \text{si } n \text{ es impar} \end{cases} \quad \forall n \in G \end{aligned}$$

Verificar si $\varphi$ es monomorfismo.

**Ejercicio 1.1.17.** Sea $\varphi$ definida como:

$$\begin{aligned} \varphi\colon \mathbb{C}^* &\to \mathbb{C}^* \\ z &\to |z| \end{aligned}$$

¿Será $\varphi$ un monomorfismo?

**Proposición 1.1.7.** *Sea $G$ un grupo y $N$ un subgrupo normal de $G$. Existe un epimorfismo $\varphi\colon G \to G/N$ cuyo nucleo es $N$.*

*Demostración.* Sea $\varphi$ definida como:

$$\begin{aligned} \varphi\colon G &\to G/N \\ a &\to [a] \end{aligned}$$

sean $a, b \in G$ tales que al operarlos tenemos que:

$$\varphi(ab) = [ab] = [a][b] = \varphi(a)\varphi(b)$$

por lo que podemos concluir que $\varphi$ es un homomorfismo. Ahora, como $\varphi$ es sobre por construcción, sabemos que $\varphi$ es un epimorfismo, es decir, si $[a] \in {}^{G}/_{N}$ existe un $a \in G$ tal que $\varphi(a) = [a]$. Si ahora tenemos un elemento $a \in \ker \varphi$, esto implica que $\varphi(a) = [e]$, es decir:

$$a \cong e \mod N$$

lo cual implica:

$$\begin{aligned} ae^{-1} &\in N \\ ae &\in N \\ a &\in N \end{aligned}$$

por lo que podemos concluir que $\ker \varphi \subseteq N$. $\square$

## Teoremas de isomorfismos

**Teorema 1.1.4.** *Sea $\varphi$ definido por:*

$$\begin{aligned} \varphi \colon G &\to G' \\ g &\to \varphi(g) \end{aligned}$$

*un epimorfismo con nucleo $K$, entonces:*

$${}^{G}/_{K} \cong G' \tag{1.1.25}$$

*Demostración.* Para demostrar que ${}^{G}/_{K}$ y $G'$ son isomorfos, debemos demostrar que existe un isomorfismo entre los dos grupos. Empezamos definiendo un mapeo $\bar{\varphi}$ definido por:

$$\begin{aligned} \bar{\varphi} \colon {}^{G}/_{K} &\to G' \\ Kg &\to \varphi(g) \end{aligned}$$

es decir $\bar{\varphi}(Kg) = \varphi(g)$.

Para demostrar que es un isomorfismo, debemos demostrar que es 1 - 1 y sobre. Para demostrar su inyectividad tomamos dos elementos $g_1, g_2 \in G$ y al evaluarlos e igualarlos, tenemos que:

$$\bar{\varphi}(Kg_1) = \bar{\varphi}(Kg_2) \implies \varphi(g_1) = \varphi(g_2)$$

Por otro lado, si operamos $g_1 g_2^{-1}$ tenemos que:

$$\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_2)\varphi(g_2^{-1}) = \varphi(g_2 g_2^{-1}) = \varphi(e) = e'$$

Esto es equivalente a decir que $g_1 g_2^{-1} \in K$, lo cual implica que:

$$\begin{aligned} g_1 &\cong g_2 \mod K \\ g_2 &\cong g_1 \mod K \end{aligned}$$

es decir:

$$\begin{aligned} [g_1] &= [g_2] \\ Kg_1 &= Kg_2 \end{aligned}$$

por lo que podemos concluir que $\bar{\varphi}$ es inyectiva.

Por otro lado, $\bar{\varphi}$ es sobre por construcción, por lo que podemos afirmar que es una biyección. □

**Ejercicio 1.1.18.** Verificar que $\varphi$ es un homomorfismo, es decir:

$$\bar{\varphi}(Kg_1Kg_2) = \bar{\varphi}(Kg_1)\bar{\varphi}(Kg_2)$$

**Teorema 1.1.5.** *Sea* $G$ *un grupo y* $H < G$ *y* $N \triangle G$*, entonces:*

$$\begin{aligned} HN &< G && (1.1.26) \\ H \cap N &\triangle H && (1.1.27) \\ N &\triangle HN && (1.1.28) \end{aligned}$$

*y ademas:*

$$^{HN}/_{N} \cong {}^{H}/_{H \cap N} \qquad (1.1.29)$$

**Teorema 1.1.6.** *Sea* $G$ *un grupo,* $N \triangle G$ *y* $K < N$ *con* $K \triangle G$*, entonces:*

$$^{G/K}/_{N/K} \cong {}^{G}/_{N} \qquad (1.1.30)$$

*Sea* $G_1, G_2, \ldots, G_n$ *grupos. Su producto directo o externo denotado por:*

$$G_1 \times G_2 \times \cdots \times G_n \qquad (1.1.31)$$

*es el conjunto de n-adas* $(a_1, a_2, \ldots, a_n)$*, donde cada* $a_i \in G_i$ *para todo* $i \in \mathbb{N}$ *y la operación en* $G_1 \times G_2 \times \cdots \times G_n$ *se define componente a componente:*

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n) \qquad (1.1.32)$$

*Tenemos que* $G = G_1 \times G_2 \times \cdots \times G_n$ *es un grupo, cuyo elemento identidad es* $(e_1, e_2, \ldots, e_n)$ *y el inverso de* $(a_1, a_2, \ldots, a_n)$ *es* $(a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$*.*

## 1.2. Anillos

### Definiciones

**Definición 1.2.1.** Un conjunto no vacio $R$ es un anillo si tiene definidas dos operaciones $(+, \cdot)$, tales que se cumplen las siguientes propiedades:

**Cerradura** $a + b \in R \quad \forall a, b \in R$

**Asociatividad** $a + (b + c) = (a + b) + c \quad \forall a, b, c \in R$

**Conmutatividad** $a + b = b + a \quad \forall a, b \in R$

**Identidad** $\exists 0 \in R \ni a + 0 = a \quad \forall a \in R$

**Inverso** $\exists b \in R \ni a + b = 0 \quad \forall a \in R$

De estas propiedades podemos concluir que $R$ es un grupo abeliano con respecto a $(+)$, pero aun tenemos lo siguiente:

**Cerradura** $a \cdot b \in R \quad \forall a, b \in R$

**Asociatividad** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

De estas propiedades podemos concluir que $R$ es un semigrupo con respecto a $(\cdot)$ y ademas:

**Distributividad** $a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall a, b, c \in R$

**Definición 1.2.2.** Diremos que un anillo $R$ es un anillo con identidad si existe un $1 \in R$ diferente de $0$ tal que:

$$a \cdot 1 = 1 \cdot a \quad \forall a \in R \tag{1.2.1}$$

**Definición 1.2.3.** Un anillo $R$ es un anillo conmutativo si:

$$a \cdot b = b \cdot a \forall a, b \in R \tag{1.2.2}$$

**Definición 1.2.4.** Sea $R$ un anillo y $a \in R$ con $a \neq 0$; diremos que $a$ es divisor de cero si existe un $b \in R$ con $b \neq 0$ tal que:

$$a \cdot b = 0 \tag{1.2.3}$$

a este se le llama divisor por la derecha, o bien si existe un $c \in R$ con $c \neq 0$ tal que:

$$c \cdot a = 0 \tag{1.2.4}$$

al que se le llama divisor por la izquierda.

**Definición 1.2.5.** Sea $R$ un anillo con identidad. Diremos que $R$ es un anillo con división si para todo $a \in R$ existe un $b \in R$ tal que:

$$a \cdot b = b \cdot a = 1 \tag{1.2.5}$$

**Definición 1.2.6.** Un campo es un anillo con división, que además es conmutativo. Un campo es un grupo abeliano con respecto a la suma y a la multiplicación.

**Definición 1.2.7.** Un anillo conmutativo con identidad es un dominio entero si:

$$a \cdot b = 0 \implies a = 0 \text{ o } b = 0 \tag{1.2.6}$$

es decir, no existen divisores de cero en el anillo.

*Observación* 1.2.1. Si $p$ es primo, entonces $\mathbb{Z}_p$ es campo.

**Ejercicio 1.2.1.** Sea $\mathcal{M}_{2\times 2}(\mathbb{R})$ definido como:

$$\mathcal{M}_{2\times 2}(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\} \tag{1.2.7}$$

Verificar que $\mathcal{M}_{2\times 2}(\mathbb{R})$ es un anillo con identidad no conmutativo y ademas no es dominio entero.

**Proposición 1.2.1.** *Sea* $R$ *un anillo y sean* $a, b \in R$*, entonces se cumplen las siguientes propiedades:*

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
3. $(-a) \cdot (-b) = (-(-a)) \cdot b = ab$
4. *Si* $1 \in R \implies (-1) \cdot a = -a$

*Demostración.* Para la verificación de la primer proposición tenemos que:

$$a \cdot 0 + 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

y cancelando $a \cdot 0$ de ambos lados:

$$0 = a \cdot 0$$

Para la verificación de la segunda proposición tenemos que:

$$a \cdot (-b) + a \cdot b = a \cdot (-b + b) = a \cdot (0) = 0$$

si conservamos los extremos de este procedimiento y despejamos el segundo termino del lado izquierdo, tenemos:

$$a \cdot (-b) = -(a \cdot b)$$

Para la verificación de la tercer proposición tenemos que:

$$(-a) \cdot (-b) + (-a) \cdot (b) = (-a) \cdot (-b + b) = (-a) \cdot (0) = 0$$

de nuevo, despejando el segundo termino del lado izquierdo, tenemos:

$$(-a) \cdot (-b) = -(-a) \cdot (b) = (-(-a)) \cdot (b)$$

al operar de nuevo con el mismo termino tenemos:

$$(-(-a)) \cdot (b) - (a) \cdot (b) = (b) \cdot (-a - (-a)) = (b) \cdot (0) = 0$$

lo cual nos da que:

$$(-(-a)) \cdot (b) = (a) \cdot (b) = (a \cdot b)$$

Para la ultima proposición tenemos que:

$$(-1) \cdot a + (1) \cdot a = a \cdot (1 - 1) = a \cdot (0) = 0$$

por lo que tenemos que:

$$(-1) \cdot a = -(1) \cdot a = -a$$

□

## Homomorfismos de anillo

**Definición 1.2.8.** Una función $\varphi \colon R \to R'$ es un homomorfismo si:

$$\varphi(a) + \varphi(b) = \varphi(a + b) \tag{1.2.8}$$
$$\varphi(a)\varphi(b) = \varphi(ab) \tag{1.2.9}$$

**Definición 1.2.9.** Sea $\varphi \colon R \to R'$ homomorfismo de anillos, a parte se dice que es:

**Monomorfismo** si $\varphi$ es inyectivo (1 - 1).

**Epimorfismo** si $\varphi$ es suprayectivo (sobre).

**Isomorfismo** si $\varphi$ es biyectivo (1 - 1 y sobre).

**Definición 1.2.10.** El nucleo de $\varphi$ es:

$$\ker \varphi = \{x \in R \mid \varphi(x) = 0\} \tag{1.2.10}$$

**Proposición 1.2.2.** *Sea $\varphi$ un homomorfismo de anillos, entonces:*

1. $\ker \varphi$ *es un subgrupo aditivo*
2. *Dados* $k \in \ker \varphi$ *y* $r \in R$ *se cumple que* $rk, kr, \in \ker \varphi$.

*Demostración.* Sean $k \in \ker \varphi$ y $r \in R$, entonces tenemos que:

$$\begin{aligned} \varphi(rk) = \varphi(r)\varphi(k) = \varphi(r) \cdot 0 &= 0 \\ \varphi(kr) = \varphi(k)\varphi(r) = 0 \cdot \varphi(r) &= 0 \end{aligned}$$

por lo que podemos concluir que:

$$kr, rk \in \ker \varphi$$

□

## Ideales

**Definición 1.2.11.** Sea $R$ un anillo e $I$ un subconjunto de $R$, se dice que $I$ es un ideal de $R$ si:

1. $I$ es un subgrupo aditivo de $R$
2. Dados $r \in R$ y $a \in I$, tenemos que se cumple $ra, ar \in I$. A esto se le conoce como la propiedad de absorción.

**Corolario 1.2.1.** *Si* $\varphi \colon R \to R'$ *es un homomorfismo, entonces* $K = \ker \varphi$ *es un ideal de* $R$.

**Definición 1.2.12.** Sea $R$ un anillo e $I$ un ideal de $R$, entonces $R/I$ es llamado anillo cociente y es un grupo, con la suma de clases de equivalencia:

$$(a + I) + (b + I) = (a + b) + I \tag{1.2.11}$$

para $a, b \in R$.

**Definición 1.2.13.** Definimos el producto como:

$$(a + I)(b + I) = ab + I \tag{1.2.12}$$

para $a, b \in I$

*Observación* 1.2.2. Sea $R$ un anillo, tenemos que $\{0\}$ y $R$ mismo son ideales triviales de $R$.

**Definición 1.2.14.** Si $I$ es un ideal de $R$ e $I \neq R$, decimos que $I$ es un ideal propio.

**Proposición 1.2.3.** *Sea* $R$ *un anillo con identidad e* $I$ *un ideal de* $R$ *tal que* $1 \in I$, *entonces* $I = R$.

*Demostración.* Para demostrar que $I = R$ primero tenemos que demostrar que $I \subseteq R$ y despues que $R \subseteq I$. Por definición $I \subseteq R$, por lo que solo resta demostrar $R \subseteq I$.

Empecemos con un elemento general $a \in R$, entonces se cumple que:

$$a = a \cdot 1$$

en donde $1 \in I$ y $a \in R$, por lo que por la propiedad de absorción de un ideal podemos decir que $a \in I$. Y como $a$ es un elemento general de $R$, podemos concluir que:

$$R \subseteq I$$

□

**Ejemplo 1.2.1.** Sea $R$ un anillo conmutativo con identidad. Dado un elemento $a \in R$ tenemos que:

$$(a) = \{ax \mid x \in R\}$$

Verificar que $(a)$ es un ideal.

Primero notamos que $(a)$ es no vacio, ya que al menos existe un elemento:

$$a \cdot 0 = 0 \in (a)$$

Ahora, para comprobar la cerradura con respecto a $(+)$ tenemos que tomar dos elementos $ax_1, ax_2 \in (a)$ y operarlos, con lo que obtenemos:

$$ax_1 + ax_2 = a(x_1 + x_2)$$

y ya que $x_1 + x_2 \in R$, sabemos que el resultado esta en $(a)$.

Para comprobar la existencia del inverso, tenemos que:

$$-ax_1 + ax_1 = a(-x_1 + x_1) = a \cdot 0 = 0$$

por lo que se cumple la existencia del inverso, por lo que concluimos que $(a)$ es un subgrupo con respecto a $(+)$. Ahora solo nos queda por comprobar la propiedad de absorción del ideal.

Si tomamos un elemento $ax \in (a)$ y un elemento $y \in R$ tendremos que:

$$axy = a(xy) = yax$$

pero $xy \in R$, por lo que concluimos que la operación sigue estando en $(a)$, por lo que tenemos que $(a)$ es un ideal.

**Definición 1.2.15.** Sea $R$ anillo conmutativo con identidad, un ideal principal es un ideal de la forma $(a)$ para algun $a \in R$.

**Definición 1.2.16.** Sea $R$ un dominio entero, diremos que $R$ es un dominio de ideales principales, si todos los ideales de $R$ son principales.

**Definición 1.2.17.** Sean $I, J$ ideales del anillo $R$, definimos las operaciones de ideales como:

$$I + J = \{a + b \mid a \in I, b \in J\} \tag{1.2.13}$$

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{N}, a \in I, b \in J \right\} \tag{1.2.14}$$

**Ejercicio 1.2.2.** Verificar que $I + J$ es un ideal dado que $I \cap J$ es un ideal de $R$.

**Proposición 1.2.4.** *Tenemos que* $R/I$ *es un anillo con la suma y productos correspondientes:*

$$\begin{aligned} (a + I) + (b + I) &:= (a + b) + I \\ (a + I)(b + I) &:= ab + I \end{aligned}$$

*entonces la función:*

$$\begin{aligned} \varphi : R &\to R/I \\ a &\to a + I \end{aligned}$$

*es un epimorfismo.*

*Demostración.* Primero debemos verificar que $\varphi$ es un homomorfismo:

$$\begin{aligned} \varphi(a + b) &= a + b + I = (a + I) + (b + I) = \varphi(a) + \varphi(b) \\ \varphi(ab) &= (a + I)(b + I) = \varphi(a)\varphi(b) \end{aligned}$$

Tambien notamos que $\varphi$ es sobre por construcción, por lo que podemos concluir que es un epimorfismo. □

**Ejercicio 1.2.3.** Verificar que el nucleo de $\varphi$ definido como:

$$\ker \varphi = \{a \in R \mid \varphi(a) = 0 + I\}$$

coincide con el ideal $I$.

## Teoremas de isomorfismos

**Teorema 1.2.1.** *Sea* $\varphi\colon R \to R'$ *un epimorfismo de anillos, y* $K = \ker\varphi$*, entonces* $R/K$ *es isomorfo con* $R'$*, es decir:*

$$R/K \cong R' \tag{1.2.15}$$

**Teorema 1.2.2.** *Sea* $R$ *anillo, sean* $A$ *un subconjunto de* $R$ *(*$A$ *subanillo de* $R$*) y* $B$ *un ideal de* $R$*, entonces* $A+B$ *es un subanillo de* $R$ *y un ideal de* $A$*, ademas:*

$$A+B/B \cong A/A\cap B \tag{1.2.16}$$

**Teorema 1.2.3.** *Sean* $I, J$ *ideales del anillo* $R$*, con* $I \subseteq J$*, entonces* $J/I$ *es ideal de* $R/I$*, ademas:*

$$R/I/J/I \cong R/J \tag{1.2.17}$$

**Ejemplo 1.2.2.** Sea $n \in \mathbb{N}$, con $n > 1$ tenemos la aplicación:

$$\begin{array}{rcl} \varphi\colon \mathbb{Z} & \to & \mathbb{Z}' \\ a & \to & [a] \end{array}$$

por lo que $\varphi$ es un epimorfismo con:

$$\begin{array}{rcl} [a+b] & = & [a]+[b] \\ [ab] & = & [a][b] \end{array}$$

y su nucleo es:

$$\begin{array}{rcl} \ker\varphi & = & \{a \in \mathbb{Z} \mid \varphi(a) = [a] = [0]\} \\ & = & \{a \in \mathbb{Z} \mid a \cong 0 \mod n\} \\ & = & \{a \in \mathbb{Z} \mid n/a\} \\ & = & \{a \in \mathbb{Z} \mid a = nz, z \in \mathbb{Z}\} = n\mathbb{Z} \end{array}$$

por lo que podemos aplicar el primer teorema de isomorfismos y decir que:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}'$$

**Ejemplo 1.2.3.** Sea $F$ un campo, es decir, un anillo conmutativo con división, entonces $\{0\}$ es un ideal de $F$.

Sea $I$ un ideal diferente a $\{0\}$. Tenemos un elemento $a \in I$, con $a \neq 0$, entonces $1 = a^{-1}a$ con $a^{-1} \in F$ y $a \in I$, por lo que:

$$1 = a^{-1}a \in I$$

Si ahora tomamos un elemento cualquiera $r \in F$, el cual obviamente puede ser escrito como $r = 1 \cdot r$, con $1 \in I$ y $r \in F$ tenemos que:

$$r = 1 \cdot r \in I$$

y por lo tanto:

$$F \subseteq I$$

y por definición sabemos que $I \subseteq F$, por lo que este ideal es el mismo que el campo.

$$F = I$$

**Ejercicio 1.2.4.** Sea $R$ definido como:

$$R = \{f \colon [0,1] \to \mathbb{R} \mid f \text{ es continua}\}$$

con las operaciones definidas como:

$$\begin{aligned} (f+g)(x) &= f(x) + g(x) \\ (f \cdot g)(x) &= f(x)g(x) \end{aligned}$$

¿Es $R$ un anillo con identidad?

**Ejercicio 1.2.5.** Si definimos el nucleo como:

$$I = \left\{ f \in R \mid f\left(\frac{1}{2}\right) = 0 \right\}$$

y definimos una función $\varphi$ como:

$$\begin{aligned} \varphi \colon R &\to \mathbb{R} \\ f &\to f\left(\frac{1}{2}\right) \end{aligned}$$

¿Podemos decir que $R/I$ y $\mathbb{R}$ son isomorfos?

## 1.3. Dominios Enteros

### Definiciones

**Definición 1.3.1.** Se dice que $a \in \mathbb{Z}$ divide a $b \in \mathbb{Z}$ si existe un $q \in \mathbb{Z}$ tal que:

$$b = qa \tag{1.3.1}$$

y se denota por $a/b$

**Teorema 1.3.1.** *Si $a/b$ y $a/c$, entonces $a/bx + cy \quad \forall x, y \in \mathbb{Z}$.*

*Demostración.* Como $a/b$ sabemos que existe un $q \in \mathbb{Z}$ tal que $b = aq$ y como $a/c$ sabemos que existe un $q' \in \mathbb{Z}$ tal que $c = aq'$. Dados $x, y \in \mathbb{Z}$ generales, al multiplicar estos enteros por las relaciones anteriores obtenemos:

$$\begin{aligned} bx &= aqx \\ cy &= aq'y \end{aligned}$$

y si sumamos ambas relaciones obtendremos:

$$bx + cy = aqx + aq'y = a(qx + q'y)$$

y como $x, y, q, q' \in \mathbb{Z}$, podemos establecer la siguiente relación:

$$bx + cy = a\bar{q} \qquad \bar{q} \in \mathbb{Z}$$

por lo que es inmediato que:

$$a/bx + cy$$

□

**Definición 1.3.2.** Un entero $p \neq 0$ se dice primo si y solo si sus únicos divisores son $\pm 1$ y $\pm p$

### Máximo Común Divisor

**Definición 1.3.3.** Si $a/b$ y $a/c$ se dice que $a$ es divisor común de $b$ y $c$.
Si además, todo divisor común de $b$ y $c$ también es divisor de $a$, se dice que $a$ es el máximo común divisor de $b$ y $c$, es decir:

$$a = (b, c) \tag{1.3.2}$$

**Ejemplo 1.3.1.** Calcular el máximo común divisor de 24 y 60, es decir $(24, 60)$.

$$\begin{array}{cc|c} 24 & 60 & 2 \\ \hline 12 & 30 & 2 \\ 6 & 15 & 3 \\ 2 & 5 & \end{array}$$

$$(24, 60) = 12$$

## mínimo común multiplo

**Definición 1.3.4.** Aprovechando la definición dada del Máximo Común Divisor, simplemente damos una definición de la siguiente forma para el mínimo cumún multiplo:

$$\frac{ab}{(a, b)} \tag{1.3.3}$$

**Ejemplo 1.3.2.** Calcular el mínimo común multiplo de 24 y 60.

$$\frac{24 \cdot 60}{12} = 120$$

$$\begin{array}{cc|c} 24 & 60 & 2 \\ \hline 12 & 30 & 2 \\ 6 & 15 & 3 \\ 2 & 5 & 2 \\ 1 & 5 & 5 \\ 1 & 1 & \end{array}$$

**Ejemplo 1.3.3.**

**Ejemplo 1.3.4.**

**Ejercicio 1.3.1.** Calcular $(0, c)$ con $c \neq 0$, $c \in \mathbb{Z}$.

## Algoritmo de la división de Euclides

**Definición 1.3.5.** Para cualesquiera enteros no nulos $a, b$ existen $q, r$ únicos, denominados cociente y residuo respectivamente, tales que:

$$a = bq + r \tag{1.3.4}$$

Si $^{b}/_{a}$, entonces $r = 0$, de lo contrario $0 < r < |b|$.

**Proposición 1.3.1.** *Se puede verificar que un divisor común de $a$ y $b$ divide a $r$ y un divisor común de $b$ y $r$ divide a $a$, es decir:*

$$(a, b) = (b, r) \tag{1.3.5}$$

*Demostración.* Si $b$ no divide a $a$, entonces tenemos que:

$$a = bq + r \quad 0 < r < |b|$$

Primero demostraremos la primera afirmación de la proposición, para lo que decimos que existe un divisor común para $a$ y $b$, al cual llamamos $c$, esto es equivalente a decir que $^c/_a$ y $^c/_b$, lo cual implica que existen $\bar{q}, q' \in \mathbb{Z}$ tales que:

$$\begin{aligned} a &= c\bar{q} \\ b &= cq' \end{aligned}$$

lo cual implica que nuestro residuo se escribe como:

$$r = a - bq = c\bar{q} - cq'q = c(\bar{q} - q'q)$$

en donde $\bar{q} - q'q \in \mathbb{Z}$, por lo que podemos concluir que $^c/_r$.

Para demostrar la segunda afirmación, tenemos un divisor común de $b$ y de $r$ al que llamamos $l$, es decir, $^l/_b$ y $^l/_r$, lo cual implica que existen $\bar{m}, m' \in \mathbb{Z}$ tales que:

$$\begin{aligned} b &= l\bar{m} \\ r &= lm' \end{aligned}$$

lo cual implica que la ecuación original puede ser escrita como:

$$a = bq + r = l\bar{m}q + lm' = l(\bar{m}q + m')$$

en donde $\bar{m}q + m' \in \mathbb{Z}$, por lo que podemos concluir que $^l/_a$, y por lo tanto:

$$(a, b) = (b, r)$$

$\square$

**Teorema 1.3.2.** *Para dos enteros no nulos* $(a, b)$ *existen dos enteros únicos* $q, r$ *tales que:*

$$a = bq + r \quad 0 \leqslant r < |b| \tag{1.3.6}$$

*A este teorema se le conoce como el agoritmo de la división de Euclides.*

*Demostración.* Definimos un conjunto de la forma:

$$S = \{a - bx \mid x \in \mathbb{Z}\} \tag{1.3.7}$$

es decir, el conjunto de los residuos en esta ecuación. Primero queremos verificar que este residuo $r = a - bx \geqslant 0$, lo que es equivalente a decir:

$$S \subset \mathbb{Z}^+ \cup \{0\}$$

1. Si $b$ es negativo $(b < 0)$, entonces $b \leqslant -1$

$$b|a| \leqslant -|a| \leqslant a$$

$$a - b|a| \geqslant 0$$

2. Si $b$ es positivo $(b > 0)$, entonces $b \geqslant 1$

$$b(-|a|) \leqslant -|a| \leqslant a$$

$$a - b(-|a|) \geqslant 0$$

por lo que podemos concluir que $S \subset \mathbb{Z}^+ \cup \{0\}$ y por lo tanto que $r = a - bx \geqslant 0$. Ahora demostraremos que $r < |b|$.

Supongamos que $r$ es el menor de estos enteros no negativos y $r \in S$, ademas supongamos que $r \geqslant |b|$, o bien:

$$r - |b| \geqslant 0$$

Como $r \in S$, existe un $x = q \in \mathbb{Z}$ tal que $r = a - bq$, por lo que tenemos que:

$$r - |b| = a - bq - |b| = \begin{cases} a - b(q-1) & \text{Si } b < 0 \\ a - b(q+1) & \text{Si } b > 0 \end{cases}$$

Por otro lado, sabemos que los valores de $r - |b|$ son:

$$\begin{aligned} r - |b| &= r - b < r \text{ para } b > 0 \\ r - |b| &= r + b < r \text{ para } b < 0 \end{aligned}$$

pero asumimos que $r$ es el menor de los enteros positivos en $S$, por lo que llegamos a una contradicción y por lo tanto:

$$r < |b|$$

Si bien hemos demostrado la veracidad de esta ecuación, aun no hemos demostrdo que $q$ y $r$ sean únicos, por lo que ahora procederemos demostrando esto.

Empezaremos suponiendo que existen $q'$ y $r'$ enteros, ademas de $q$ y $r$ tales que:

$$\begin{aligned} a &= bq + r \\ a &= bq' + r' \end{aligned}$$

en donde $0 \leqslant r < |b|$ y $0 \leqslant r' < |b|$. Si estas expresiones las restamos entre si, obtendremos:

$$b(q - q') = r' - r$$

lo cual implica que $^{b}/_{r'-r}$, es decir, existe un $t \in \mathbb{Z}$, tal que:

$$r' - r = bt$$

Por otro lado, la expresión $b(q - q') = r' - r$ puede ser expresada como:

$$\begin{aligned} b(q - q') + (r - r') &= 0 \\ b(q' - q) + (r' - r) &= 0 \end{aligned}$$

lo cual, ya hemos comprobado que implica:

$$|r - r'| \leqslant |b|$$

o bien:

$$|bt| \leqslant |b|$$

Si tomamos en cuenta los valores que puede tomar $t$, nos daremos cuenta que:

1. Si $t = 0$

$$r' = r \implies q' = q$$

2. Si $t = -1$

$$|-b| \leqslant |b| \implies r' - r = -b \implies r' = r - b \geqslant 0 \implies r \geqslant b$$

lo cual es falso, por lo que $t \neq -1$

3. Si $t = 1$

$$|b| \leqslant |b| \implies r' - r = b \implies r = r' - b \geqslant 0 \implies r' \geqslant b$$

lo cual es falso, por lo que $t \neq 1$

y como el caso en que $t = 0$ es el único cierto, concluimos que $q, r$ deben ser únicos. □

## Procedimiento para hallar el Máximo Común Divisor de $a$ y $b$

A continuación se describe un procedimiento iterativo para encontrar el Máximo Común Divisor de un par $a, b$. Primero empezaremos asumiendo que $b$ no divide a $a$, por lo que tendremos que:

$$a = bq + r \quad 0 \leqslant r < |b| \tag{1.3.8}$$

El caso contrario es trivial, dado que si ${}^{b}/_{a}$, claramente

$$(a, b) = b$$

Si ahora nos concentramos en $r$, tenemos dos casos; si ${}^{r}/_{b}$, sabemos que $b = rq_1$ y $a = rq_1q + r = r(q_1q + 1)$, por lo que:

$$(a,b) = r$$

Si $r$ no divide a $b$ tenemos que:

$$b = q_1 r + r_1 \quad 0 \leqslant r_1 < |r| \tag{1.3.9}$$

Por lo que ahora revisamos a $r_1$; si ${}^{r_1}/_{r}$, sabemos que $r = r_1 q_2$ por lo que:

$$(b,r) = r_1$$

Si $r_1$ no divide a $r$ tenemos que:

$$r = q_2 r_1 + r_2 \tag{1.3.10}$$

Si proseguimos con estas iteraciones $k$ veces, obtendremos:

$$r_k = q_{k+2} r_{k+1} + r_{k+2} \quad 0 \leqslant r_{k+2} < |r_{k+1}|$$

Supongamos ahora que esta ultima iteración es donde tenemos que ${}^{r_{k+2}}/_{r_{k+1}}$, es decir:

$$r_{k+2} = (r_{k+1}, r_k) = \cdots = (r_1, r) = (r,b) = (b,a)$$

Por lo que hemos encontrado el Máximo Común Divisor del par original.
Si ahora despejamos a $r$ de la ecuación 1.3.8 tendremos:

$$r = a - bq = (1)a + (-q)b = m_1 a + n_1 b$$

y lo sustituimos en la ecuación 1.3.9

$$\begin{aligned} r_1 &= b - q_1 r = b - q_1(m_1 a + n_1 b) \\ &= (-m_1 q_1)a + (1 - n_1 q_1)b = m_2 a + n_2 b \end{aligned}$$

y lo sustituimos en la ecuación 1.3.10

$$\begin{aligned} r_2 &= r - q_2 r_1 = (m_1 a + n_1 b) - q_2(m_2 a + n_2 b) \\ &= (m_1 - m_2 q_2)a + (n_1 - n_2 q_2)b = m_3 a + n_3 b \end{aligned}$$

En general

$$r_k = m_{k+1} a + n_{k+1} b \tag{1.3.11}$$

**Teorema 1.3.3.** *Si $d = (a,b)$, entonces existen $m, n \in \mathbb{Z}$ tales que:*

$$d = (a,b) = ma + nb \tag{1.3.12}$$

*A esto se le conoce como la identidad de Bezout.*

**Ejemplo 1.3.5.** Calcular $(-2805, 119)$

**Ejemplo 1.3.6.** Calcular $(726, 275)$

**Ejemplo 1.3.7.** Expresar $(726, 275) = 11$, en terminos de 726 y 275.

**Definición 1.3.6.** Dos enteros $a$ y $b$, para los cuales $(a, b) = 1$ se dicen primos relativos.

**Teorema 1.3.4.** *Todo entero $a > 1$ tiene una factorización única en producto de primos positicos, es decir:*

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n} \quad \alpha_i \geqslant 1 \quad 1 \leqslant i \leqslant n \tag{1.3.13}$$

*y los $p_i$ son primos positivos distintos.*

**Ejemplo 1.3.8.** Hallar una factorización única para 2241756.

**Ejemplo 1.3.9.** Hallar una factorización única para 8566074.

**Ejemplo 1.3.10.** Hallar $(2241756, 8566074)$ a partir de sus factorizaciones únicas.

## El anillo de los polinomios

**Definición 1.3.7.** Sea $\mathbb{F}$ un campo, definimos el anillo de los polinomios:

$$\mathbb{F}[x] = \{p(x) = a_0 + a_1 x + \cdots + a_n x^n \mid n \in \mathbb{Z}, n \geqslant 0, a_i \in \mathbb{F}\} \tag{1.3.14}$$

En donde para dos elementos $p(x)$ y $q(x)$ de la forma:

$$\begin{aligned} p(x) &= a_0 + a_1 x + \cdots + a_n x^n \\ q(x) &= b_0 + b_1 x + \cdots + b_m x^m \end{aligned}$$

definimos la suma como:

$$p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \dots (a_s + b_s)x^s \tag{1.3.15}$$

en donde $s = \text{máx}(m, n)$. Y para el producto tenemos:

$$p(x)q(x) = c_0 + c_1 x + \cdots + c_l x^l \quad 0 \leqslant k \leqslant l \tag{1.3.16}$$

y los $c_k$ son de la forma:

$$c_k = \sum_{i+j=k} a_i + b_j = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0 \tag{1.3.17}$$

**Definición 1.3.8.** Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{F}[x]$ con $a_n \neq 0$, el grado de $f(x)$ esta dado por:

$$\operatorname{gr} f(x) = n \tag{1.3.18}$$

Además, si $a_n = 1$, $f(x)$ se dice mónico.
Para $p(x), q(x) \in \mathbb{F}[x]$, algunas propiedades notables de esta función gr, son:

1. $\operatorname{gr} p(x) + q(x) \leqslant \max \operatorname{gr} p(x), \operatorname{gr} q(x)$
2. $\operatorname{gr} p(x)q(x) = \operatorname{gr} p(x) + \operatorname{gr} q(x)$

*Observación* 1.3.1. Dados los polinomios $f(x), g(x) \in \mathbb{F}[x]$, con $g(x) \neq 0$, existen dos polinomios únicos $q(x), r(x) \in \mathbb{F}[x]$ tales que:

$$f(x) = q(x)g(x) + r(x) \quad \operatorname{gr} r(x) < \operatorname{gr} g(x) \tag{1.3.19}$$

Si además, ${}^{g(x)}/_{f(x)}$ entonces $r(x) = 0$.
Como en el caso de los enteros, puede definirse divisibilidad, Máximo Común Divisor y usar el algoritmo de la división de Euclides para encontrar el Máximo Común Divisor de $f(x)$ y $g(x)$.
Cualquiera de los polinomios dados se puede dividir por un factor que no divida al otro polinomio. Ese factor, por no ser común de ambos polinomios, no forma parte del Máximo Común Divisor. Entonces el residuo de cualquier división se puede dividir por un factor que no divida a los polinomios dados.

**Ejemplo 1.3.11.** Hallar $(f(x), g(x))$ con:

$$\begin{aligned} f(x) &= 2x^3 - 11x^2 + 10x + 8 \\ g(x) &= 2x^3 + x^2 - 8x - 4 \end{aligned}$$

**Ejercicio 1.3.2.** Hallar $(f(x), g(x))$ con:

$$\begin{aligned} f(x) &= 12x^3 - 26x^2 + 20x - 12 \\ g(x) &= 2x^3 - x^2 - 3x \end{aligned}$$

**Ejercicio 1.3.3.** Hallar $(f(x), g(x))$ con:

$$\begin{aligned} f(x) &= x^3 - 6x + 7 \\ g(x) &= x + 4 \end{aligned}$$

# Capítulo 2

# Álgebra lineal

## 2.1. Espacios vectoriales

### Definiciones

**Definición 2.1.1.** Un espacio vectorial $V$ consta de lo siguiente:

1. Un campo $\mathbb{F}$ de escalares
2. Un conjunto no vacio de objetos denominados vectores
3. Una operación denominada suma o adición que asocia a cada par de vectores $\alpha, \beta \in V$, un vector $\alpha + \beta \in V$ llamado suma de $\alpha$ y $\beta$, que cumple lo siguiente

   *a*) $\alpha + \beta = \beta + \alpha \quad \forall \alpha, \beta \in V$

   *b*) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma \quad \forall \alpha, \beta, \gamma \in V$

   *c*) $\exists ! \vec{0} \ni \alpha + \vec{0} = \alpha$

   *d*) $\exists ! - \alpha \in V \ni \alpha + (-\alpha) = \vec{0} \quad \forall \alpha \in V$

4. Una operación denominada multiplicación por escalares, que asocia a cada escalar $c \in \mathbb{F}$ un vector $c\alpha \in V$, de manera que:

   *a*) $(c_1 c_2)\alpha = c_1(c_2\alpha) \quad \forall c_1, c_2 \in \mathbb{F} \quad \forall \alpha \in V$

   *b*) $c(\alpha + \beta) = c\alpha + c\beta \quad \forall c \in \mathbb{F} \quad \forall \alpha, \beta \in V$

   *c*) $(c_1 + c_2)\alpha = c_1\alpha + c_2\alpha \quad \forall c_1, c_2 \in \mathbb{F} \quad \forall \alpha \in V$

   *d*) $1 \cdot \alpha = \alpha \quad \forall \alpha \in V$

**Ejercicio 2.1.1.** Verificar que un campo $\mathbb{F}$ es un espacio vectorial sobre si mismo.

**Ejercicio 2.1.2.** Verificar que $\mathbb{R}$ es un espacio vectorial sobre $\mathbb{R}$

**Ejercicio 2.1.3.** Verificar que $\mathbb{Q}$ es un espacio vectorial sobre $\mathbb{Q}$

**Ejercicio 2.1.4.** Verificar que $\mathbb{C}$ es un espacio vectorial sobre $\mathbb{C}$

**Ejercicio 2.1.5.** Verificar que $\mathbb{R}$ es un espacio vectorial sobre $\mathbb{Q}$

**Ejercicio 2.1.6.** Verificar que $\mathbb{C}$ es un espacio vectorial sobre $\mathbb{Q}$

**Ejercicio 2.1.7.** Verificar que $\mathbb{Q}$ es un espacio vectorial sobre $\mathbb{R}$

**Ejercicio 2.1.8.** Verificar que $\mathbb{R}$ es un espacio vectorial sobre $\mathbb{C}$

**Definición 2.1.2.** Sea $\mathbb{F}$ un campo y sea $n \in \mathbb{N}$. Definimos el espacio vectorial $\mathbb{F}^n$ como:

$$\mathbb{F}^n = \{\begin{pmatrix} x_1 & x_2 & \dots & x_n \end{pmatrix} \mid x_i \in \mathbb{F}\} \tag{2.1.1}$$

Dados los elementos $\alpha, \beta \in \mathbb{F}^n$ de la forma:

$$\begin{aligned} \alpha &= \begin{pmatrix} x_1 & x_2 & \dots & x_n \end{pmatrix} \\ \beta &= \begin{pmatrix} y_1 & y_2 & \dots & y_n \end{pmatrix} \end{aligned}$$

podemos definir la suma como:

$$\alpha + \beta = \begin{pmatrix} x_1 + y_1 & x_2 + y_2 & \dots & x_n + y_n \end{pmatrix} \tag{2.1.2}$$

y la multiplicación por escalar como:

$$c\alpha = \begin{pmatrix} cx_1 & cx_2 & \dots & cx_n \end{pmatrix} \quad \forall c \in \mathbb{F} \tag{2.1.3}$$

**Ejemplo 2.1.1.**

**Ejemplo 2.1.2.**

**Ejemplo 2.1.3.**

**Ejemplo 2.1.4.**

**Ejercicio 2.1.9.** Verificar que $\mathbb{F}^n$ es un espacio vectorial sobre $\mathbb{F}$, en particular si $\mathbb{F} = \mathbb{R}$ y $n = 2$.

**Proposición 2.1.1.** *Sea $V$ un espacio vectorial sobre $\mathbb{F}$, entonces se tiene que:*

$$0 \cdot \alpha = \vec{0} \quad \forall \alpha \in V \tag{2.1.4}$$

**Definición 2.1.3.** Se dice que $\beta \in V$ es una combinación lineal de vectores $\alpha_1, \alpha_2, \dots, \alpha_n$ si existen $c_1, c_2, \dots, c_n \in \mathbb{F}$ tales que:

$$\beta = \sum_{i=1}^{n} c_i \alpha_i \tag{2.1.5}$$

## Subespacios vectoriales

**Definición 2.1.4.** Un subespacio de un espacio vectorial $V$, es un subconjunto $W$ de $V$ que con las operaciones heredadas de $V$, es un espacio vectorial sobre $\mathbb{F}$

*Observación* 2.1.1. Si $V$ es un espacio vectorial, $V$ y $\{\vec{0}\}$ se denominan los subespacios triviales de $V$.

**Proposición 2.1.2.** *Un subconjunto no vacio $W$ de $V$, es un subespacio vectorial si y solo si $W$ es cerrado con respecto a las operaciones de $V$.*

**Definición 2.1.5.** Sean $\alpha_1, \alpha_2, \ldots, \alpha_k \in V$, definimos:

$$\mathcal{L}(\alpha_1, \alpha_2, \ldots, \alpha_k) = \{v \mid v \text{ es combinación lineal de } \alpha_1, \alpha_2, \ldots, \alpha_k\} \tag{2.1.6}$$

es decir, es un subespacio vectorial de $V$ y se llama subespacio generado por $\alpha_i$ con $1 \leqslant i \leqslant k$, o bien se dice que $\alpha_1, \alpha_2, \ldots, \alpha_k$ generan a $\mathcal{L}(\alpha_1, \alpha_2, \ldots, \alpha_k)$.
En general, si $A \neq 0$ y si $A \subset V$, entonces

$$\mathcal{L}(A) = \{v \mid v \text{ es combinacion lineal de los elementos de } A\} \tag{2.1.7}$$

**Proposición 2.1.3.** *La intersección de cualquier colección de subespacios vectoriales de $V$ es un subespacio vectorial de $V$.*

*Demostración.* Sea $Wa = \{wa \mid a \in I\}$ y sea $W = \cap Wa$.

En primer lugar notamos que $W$ es no vacio, ya que $\vec{0} \in Wa$ para todo $a \in I$.

Despues tomamos dos elementos $\alpha, \beta \in W$, los cuales estan tambien en $Wa$ para todo $a \in I$. Si los operamos entre si, sabemos que $\alpha + \beta \in Wa$ para todo $a \in I$, por lo que sigue que tambien $\alpha + \beta \in W$.

Por ultimo, si tomamos un elemento $\beta \in W$ y un elemento $r \in \mathbb{F}$, sabemos que $r\beta \in Wa$ para todo $a \in I$, por lo que se sigue que $r\beta \in W$.

Por lo que concluimos que $W$ es un subespacio vectorial. □

*Observación* 2.1.2. La union de subespacios vectoriales, no necesariamente es un subespacio vectorial.
Por ejemplo, si en $\mathbb{R}^2$ definimos:

$$W_1 = \{(x_1 \quad 0) \mid x_1 \in \mathbb{R}\} \subset \mathbb{R}$$
$$W_2 = \{(0 \quad x_2) \mid x_2 \in \mathbb{R}\} \subset \mathbb{R}$$

La union de estos subespacios vectoriales sería:

$$W_1 \cup W_2 = \{(x_1 \quad 0), (0 \quad x_2) \mid x_1, x_2 \in \mathbb{R}\}$$

por lo que si tomamos un elemento de cada subespacio vectorial y los sumamos, obtendremos:

$$\begin{pmatrix} x_1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & x_2 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 \end{pmatrix} \notin W_1 \cup W_2$$

**Definición 2.1.6.** Sean $S, T$ subespacios vectoriales de $V$, definimos la suma de $S$ y $T$ como:

$$S + T = \{s + t \mid s \in S, t \in T\} \tag{2.1.8}$$

**Proposición 2.1.4.** *Si $S$ y $T$ son subespacios vectoriales de $V$, entonces $S + T$ es un subespacio de $V$.*

**Definición 2.1.7.** Si $S$ y $T$ son subespacios vectoriales de $V$, tales que $V = S + T$ y $S \cap T = \{0\}$, decimos que $V$ es la suma directa de $S$ y $T$, y la denotamos por:

$$V = S \oplus T \tag{2.1.9}$$

**Proposición 2.1.5.** *Si $V = S \oplus T$, entonces existen únicos $s$ y $t$ tales que:*

$$\alpha = s + t \quad \forall \alpha \in V \tag{2.1.10}$$

*Demostración.* Sean $s, s' \in S$ y $t, t' \in T$ elementos para los que se cumple que un $\alpha \in V$, tenga la siguiente forma:

$$\alpha = s + t = s' + t'$$

Si a los dos ultimos terminos de esta ecuación les restamos $s + t'$, tendremos:

$$s + t - s - t' = s' + t' - s - t'$$

es decir:

$$t - t' = s' - s$$

pero el lado izquierdo de la ecuación es algo que está en $T$ y el segundo termino es algo que está en $S$, es decir, estamos preguntando que elementos hay en común en $S$ y $T$. Como $V = S \oplus T$, sabemos que la intersección entre $S$ y $T$ es $\{0\}$, por lo que nos quedan las siguientes relaciones:

$$\begin{aligned} t - t' &= 0 \\ s' - s &= 0 \end{aligned}$$

lo cual implica que:

$$
\begin{aligned}
t &= t' \\
s' &= s
\end{aligned}
$$

$\square$

**Definición 2.1.8.** Sea $A$ una matriz $m \times n$ con entradas en $\mathbb{F}$, los vectores fila de $A$ son:

$$
\begin{aligned}
\alpha_1 &= \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \end{pmatrix} \\
\alpha_2 &= \begin{pmatrix} a_{21} & a_{22} & \dots & a_{2n} \end{pmatrix} \\
&\vdots \\
\alpha_m &= \begin{pmatrix} a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}
\end{aligned}
$$

y los vectores columna son:

$$
\begin{aligned}
\beta_1 &= \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \end{pmatrix}^T \\
\beta_2 &= \begin{pmatrix} a_{12} & a_{22} & \dots & a_{m2} \end{pmatrix}^T \\
&\vdots \\
\beta_n &= \begin{pmatrix} a_{1n} & a_{2n} & \dots & a_{mn} \end{pmatrix}^T
\end{aligned}
$$

es decir:

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

El subespacio de $\mathbb{F}^m$ generado por $\alpha_1, \alpha_2, \dots, \alpha_m$ se denomina espacio fila de $A$. El subespacio de $\mathbb{F}^n$ generado por $\beta_1, \beta_2, \dots, \beta_n$ se denomina espacio columna de $A$.

**Definición 2.1.9.** Si $A$ y $B$ son matrices equivalentes (por filas, mediante operaciones elementales), entonces el espacio fila de $A$ coincide con el espacio fila de $B$.

## Dependencia e independencia lineal

**Definición 2.1.10.** Los vectores $\alpha_1, \alpha_2, \dots, \alpha_k$ se dicen linealmente dependientes si existen escalares $a_1, a_2, \dots, a_k$ no todos cero, tales que:

$$\sum_{i=1}^{k} a_i \alpha_i = 0 \tag{2.1.11}$$

Los vectores $\alpha_1, \alpha_2, \ldots, \alpha_k$ se dicen linealmente independientes si no son linealmente dependientes.

**Definición 2.1.11.** Un conjunto $A$ de vectores se dice linealmente independiente si cualquier subconjunto finito de $A$ es linealmente independiente.

**Definición 2.1.12.** Un conjunto $A$ de vectores se dice linealmente dependiente si existe un subconjunto finito de $A$ no vacio que sea linealmente dependiente.

*Observación* 2.1.3. Por convención, el conjunto $\varnothing$ es linealmente independiente.

**Ejemplo 2.1.5.** Verificar si $\left\{ \begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 9 \end{pmatrix}, \begin{pmatrix} 0 & 3 \end{pmatrix} \right\}$ es linealmente dependiente o independiente.

**Ejercicio 2.1.10.** Verificar si $\left\{ \begin{pmatrix} 20 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 0 \end{pmatrix} \right\}$ es linealmente dependiente o independiente en $\mathbb{R}^2$

**Ejercicio 2.1.11.** Verificar si $\left\{ \begin{pmatrix} 0 & 0 & 0 \end{pmatrix} \right\}$ es linealmente dependiente o independiente en $\mathbb{R}^3$.

**Ejercicio 2.1.12.** Verificar si $\{e_1, e_2, e_3\}$ es linealmente dependiente o independiente en $\mathbb{R}^4$.

**Proposición 2.1.6.** *Un conjunto de vectores* $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$*, con* $\alpha_i \neq 0$ *para* $1 \leqslant i \leqslant n$ *es linealmente dependiente si y solo si algún* $\alpha_k$ *es combinación lineal de los vectores que le proceden, con* $1 \leqslant k \leqslant n$.

**Proposición 2.1.7.** *Si* $\alpha_1, \alpha_2, \ldots, \alpha_k$ *con* $\alpha_i \neq 0$ *para* $1 \leqslant i \leqslant k$ *son vectores que generan a un espacio vectorial* $V$*, entonces existe un subconjunto linealmente independiente de estos generadores que tambien generan a* $V$.

*Demostración.* Para demostrar la proposición anterior, debemos tomar un subconjunto de los vectores originales y eliminar cualquier vector linealmente dependiente, para lograr que sea linealmente independiente, y que siga generando al espacio vectorial.

Primero debemos de tomar el primer vector $\alpha_1$ [1] y revisar si es linealmente dependiente con el siguiente vector $\alpha_2$, si es cierto esto, se procede a eliminar el vector $\alpha_2$ y se toma el siguiente vector, y asi hasta terminar con el conjunto.

Al finalizar este proceso, tendremos un subconjunto $\{\alpha_1, \alpha_{n_1}, \ldots, \alpha_{n_j}\}$ que es linealmente independiente por construcción y que sigue generando al espacio vectorial. □

[1] Realmente no importa el orden que tengan los vectores, ya que si un par es linealmente dependiente, tan solo debemos elimnar a uno de ellos.

**Ejercicio 2.1.13.** Sea $V$ un espacio vectorial, y sean $\alpha_1, \alpha_2, \alpha_3 \in V$ tales que:

$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$

Verificar que:

$$\mathcal{L}\{\alpha_1, \alpha_2\} = \mathcal{L}\{\alpha_2, \alpha_3\}$$

**Ejercicio 2.1.14.** Sea el conjunto $A$ definido por:

$$A = \left\{x \in \mathbb{R} \mid x = a\sqrt{1} + b\sqrt{s} + c\sqrt{3}, a, b, c \in \mathbb{Q}\right\}$$

Verificar que $A$ es un espacio vectorial sobre $\mathbb{Q}$.
Verificar que $\sqrt{1}, \sqrt{2}, \sqrt{3}$ son linealmente independientes y generan a $A$.

**Ejercicio 2.1.15.** Verificar que:

$$\left\{1, 1 + x, 1 + x + x^2, \ldots, 1 + x + x^2 + \cdots + x^n\right\}$$

es un conjunto con elementos linealmente independientes.

**Definición 2.1.13.** Sea $V$ un espacio vectorial de dimensión $n$, un conjunto de $n$ vectores forma una base para $V$ si es linealmente independiente y genera a $V$.

**Ejercicio 2.1.16.** Encontrar una base para $\mathbb{R}^3$ que incluya a $\begin{pmatrix}1 & 1 & 0\end{pmatrix}$ y $\begin{pmatrix}0 & 1 & 0\end{pmatrix}$.

## 2.2. Isomorfismos

### Definiciones

**Definición 2.2.1.** Sean $V$ y $V'$ espacios vectoriales sobre un campo $\mathbb{F}$, se dice que $V$ y $V'$ son isomorfos, si existe una función $\varphi \colon V \to V'$ inyectiva y suprayectiva, tal que:

1. $\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta) \quad \forall \alpha, \beta \in V$
2. $\varphi(r\alpha) = r\varphi(\alpha) \quad \forall r \in \mathbb{F} \quad \forall \alpha \in V$

**Proposición 2.2.1.** *El isomorfismo entre espacios vectoriales es una relación de equivalencia.*

**Teorema 2.2.1.** *Todo espacio vectorial $V$ sobre $\mathbb{F}$ de dimensión $n > 0$ es isomorfo a $\mathbb{F}^n$, es decir:*

$$V \cong \mathbb{F}^n \tag{2.2.1}$$

*Demostración.* Sea $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ una base de V. Dado $\alpha \in V$, este tiene la forma:

$$\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$$

Ahora, si definimos una función $\varphi$ tal que:

$$\varphi(\alpha) = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \end{pmatrix}$$

es decir:

$$\begin{aligned} \varphi\colon V &\to \mathbb{F}^n \\ \alpha &\to \begin{pmatrix} a_1 & a_2 & \ldots & a_n \end{pmatrix} \end{aligned}$$

Por lo que tenemos que demostrar, es que esta función es isomorfismo. Para empezar, demostraremos que esta función es inyectiva.

Para esto tomamos dos elementos $\alpha, \beta \in V$, tales que:

$$\begin{aligned} \alpha &= a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n \\ \beta &= b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n \end{aligned}$$

Por lo que si asumimos que $\varphi(\alpha) = \varphi(\beta)$, es decir:

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_n \end{pmatrix} = \begin{pmatrix} b_1 & b_2 & \ldots & b_n \end{pmatrix} \tag{2.2.2}$$

tenemos que esto implica que:

$$\begin{aligned} a_1 &= b_1 \\ a_2 &= b_2 \\ &\vdots \\ a_n &= b_n \end{aligned}$$

y por lo tanto $\alpha = \beta$, por lo que $\varphi$ es inyectiva.

Por otro lado, sabemos que $\varphi$ es suprayectiva por construcción.

Ahora tomamos dos elementos $\alpha, \beta \in V$ y los operamos, por lo que tendremos que:

$$\begin{aligned} \varphi(\alpha + \beta) &= \varphi(a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n + b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n) \\ &= \varphi((a_1 + b_1)\alpha_1 + (a_2 + b_2)\alpha_2 + \cdots + (a_n + b_n)\alpha_n) \\ &= \begin{pmatrix} a_1 + b_1 & a_2 + b_2 & \ldots & a_n + b_n \end{pmatrix} \\ &= \begin{pmatrix} a_1 & a_2 & \ldots & a_n \end{pmatrix} + \begin{pmatrix} b_1 & b_2 & \ldots & b_n \end{pmatrix} \\ &= \varphi(\alpha) + \varphi(\beta) \end{aligned}$$

Por otro lado, si tomamos un elemento $r \in \mathbb{F}$ y un elemento $\alpha \in V$, tendremos que:

$$\begin{aligned}
\varphi(r\alpha) &= \varphi(r(a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n)) \\
&= \varphi(ra_1\alpha_1 + ra_2\alpha_2 + \cdots + ra_n\alpha_n) \\
&= \begin{pmatrix} ra_1 & ra_2 & \ldots & ra_n \end{pmatrix} \\
&= r\begin{pmatrix} a_1 & a_2 & \ldots & a_n \end{pmatrix} = r\varphi(\alpha)
\end{aligned}$$

Por lo que queda demostrado que $\varphi$ es un isomorfismo y por lo tanto:

$$V \cong \mathbb{F}^n$$

□

**Ejercicio 2.2.1.** Sea un espacio vectorial $V$ definido como:

$$V = \{p(x) = a_0 + a_1x \mid \operatorname{gr} p(x) = 1\}$$

Verfiicar que $V \cong \mathbb{R}^2$ dada la siguiente función:

$$\begin{aligned}
\varphi\colon V &\to \mathbb{R}^2 \\
\alpha &\to \begin{pmatrix} a_0 & a_1 \end{pmatrix}
\end{aligned}$$

**Proposición 2.2.2.** *Si $S$ y $T$ son subespacios vectoriales de un espacio vectorial de dimensión finita, entonces tenemos que:*

$$\dim(S+T) + \dim(S\cap T) = \dim S + \dim T \tag{2.2.3}$$

*Demostración.* Sea $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ una base de $S\cap T$, podemos completar con $\{\beta_1, \beta_2, \ldots, \beta_{r-k}\}$ a una base de $S$, por lo que la dimensión de $S$ sería:

$$\dim S = k + (r-k) = r$$

Similarmente podemos completar a una base de $T$ con $\{\gamma_1, \gamma_2, \ldots, \gamma_{m-k}\}$, por lo que su dimensión es:

$$\dim T = k + (m-k) = m$$

Veamos que:

$$\{\underbrace{\overbrace{\alpha_1, \alpha_2, \ldots, \alpha_k}^{k}, \overbrace{\beta_1, \beta_2, \ldots, \beta_{r-k}}^{r-k}}_{r}, \overbrace{\gamma_1, \gamma_2, \ldots, \gamma_{m-k}}^{m-k}\}$$

es una base de $S+T$, por lo que:

$$\begin{aligned}
\dim(S+T) &= r + m - k \\
\dim(S+T) &= \dim S + \dim T - \dim(S\cap T)
\end{aligned}$$

Aqui aun falta verificar que esta base es linealmente independiente y que genera a $S+T$, pero puede verse inmediatamente el resultado final. □

**Ejercicio 2.2.2.** Verificar que en $\mathbb{R}^3$ la suma de dos subespacios de dimensción igual a dos, tiene dimensiones no cero.

## 2.3. Transformaciones lineales

### Definiciones

**Definición 2.3.1.** Sean $V, W$, espacios vectoriales sobre un campo $\mathbb{F}$, con una función $T\colon V \to W$. Se dice que $T$ es una transformación lineal de $V$ a $W$ si:

1. $T(\alpha+\beta) = T(\alpha) + T(\beta) \quad \forall \alpha, \beta \in V$
2. $T(c\alpha) = cT(\alpha) \quad \forall c \in \mathbb{F} \quad \forall \alpha \in V$

**Proposición 2.3.1.** *Sea* $T\colon V \to W$ *una transformación lineal, sean* $c_1, c_2, \ldots, c_k \in \mathbb{F}$ *y* $\alpha_1, \alpha_2, \ldots, \alpha_k \in V$*, entonces:*

$$T(c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n) = c_1T(\alpha_1) + c_2T(\alpha_2) + \cdots + c_nT(\alpha_n)$$

*es decir:*

$$T\left(\sum_{i=1}^{n} c_i\alpha_i\right) = \sum_{i=1}^{n} c_iT(\alpha_i) \quad n \in \mathbb{N} \tag{2.3.1}$$

**Proposición 2.3.2.** *Si* $T\colon V \to W$ *es una transformación lineal, entonces:*

$$T(0_V) = 0_W \tag{2.3.2}$$

*Demostración.* Si sumamos $0_W$ a $T(0_V)$, tendremos.

$$0_W + T(0_V) = T(0_V) = T(0_V + 0_V) = T(0_V) + T(0_V)$$

y cancelando un $T(0_V)$ en ambos lados de esta ecuación, tenemos:

$$0_W = T(0_V)$$

□

**Ejercicio 2.3.1.** Dada la función:

$$\begin{aligned} 0\colon V &\to V \\ \alpha &\to 0 \end{aligned}$$

Verificar si es transformación lineal, si es inyectiva y si es suprayectiva.

**Ejercicio 2.3.2.** Dada la función:

$$\begin{aligned} T\colon \mathbb{R} &\to \mathbb{R} \\ x &\to x^2 \end{aligned}$$

Verificar si es transformación lineal, si es inyectiva y si es suprayectiva.

**Ejercicio 2.3.3.** Dada la función:

$$\begin{aligned} T\colon \mathbb{R}^3 &\to \mathbb{R}^2 \\ \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} &\to \begin{pmatrix} x_1 & x_3 \end{pmatrix} \end{aligned}$$

Verificar si es transformación lineal, si es inyectiva y si es suprayectiva.

**Ejercicio 2.3.4.** Dada la función:

$$\begin{aligned} T\colon \mathbb{R}^2 &\to \mathbb{R}^3 \\ \begin{pmatrix} x_1 & x_2 \end{pmatrix} &\to \begin{pmatrix} 0 & x_1 & x_2 \end{pmatrix} \end{aligned}$$

Verificar si es transformación lineal, si es inyectiva y si es suprayectiva.

**Teorema 2.3.1.** *Sea $V, W$ espacios vectoriales sobre un campo $\mathbb{F}$, $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ una base de $V$ y $\{w_1, w_2, \dots, w_n\}$ una base de $W$, existe una única transformación lineal $T\colon V \to W$ tal que:*

$$T(\alpha_i) = w_i \quad 1 \leqslant i \leqslant n \tag{2.3.3}$$

*Demostración.* Sea $\alpha \in V$, entonces $\alpha$ se escribe de manera única como:

$$\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$$

y definimos $T$ como:

$$\begin{aligned} T\colon V &\to W \\ \alpha &\to a_1w_1 + a_2w_2 + \cdots + a_nw_n \end{aligned}$$

en particular tenemos que:

$$\begin{aligned} \alpha_i &= 0\alpha_1 + 0\alpha_2 + \cdots + \alpha_i + \cdots + 0\alpha_n \\ w_i &= 0w_1 + 0w_2 + \cdots + w_i + \cdots + 0w_n \end{aligned}$$

tal que:

$$T(\alpha_i) = w_i \in W \quad 1 \leqslant i \leqslant n$$

por lo que $T$ es lineal.

Si ahora tenemos dos elementos $\alpha, \beta \in V$ de la forma:

$$\begin{aligned}
\alpha &= a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n \\
\beta &= b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n
\end{aligned}$$

por lo que tenemos que:

$$\begin{aligned}
T(\alpha+\beta) &= T(a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n + b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n) \\
&= T((a_1+b_1)\alpha_1 + (a_2+b_2)\alpha_2 + \cdots + (a_n+b_n)\alpha_n) \\
&= (a_1+b_1)w_1 + (a_2+b_2)w_2 + \cdots + (a_n+b_n)w_n \\
&= a_1w_1 + a_2w_2 + \cdots + a_nw_n + b_1w_1 + b_2w_2 + \cdots + b_nw_n \\
&= T(\alpha) + T(\beta)
\end{aligned}$$

y dado un $c \in \mathbb{F}$, tenemos que:

$$\begin{aligned}
T(c\alpha) &= T(c(a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n)) \\
&= T(ca_1\alpha_1 + ca_2\alpha_2 + \cdots + ca_n\alpha_n) \\
&= ca_1w_1 + ca_2w_2 + \cdots + ca_nw_n \\
&= cT(\alpha)
\end{aligned}$$

$\square$

**Definición 2.3.2.** Sea $T\colon V \to W$ una transformación lineal, definimos el nucleo de $T$ como:

$$\ker T = \{v \in V \mid T(v) = 0\} \subset V \tag{2.3.4}$$

y definimos la imagen de $T$ como:

$$\operatorname{im} T = \{T(v) \mid v \in V\} \subset W \tag{2.3.5}$$

## Propiedades

**Proposición 2.3.3.** *Si $T\colon V \to W$ es una transformación lineal y $\ker T$ y $\operatorname{im} T$ son subespacios vectoriales de $V$ y $W$ respectivamente.*

**Proposición 2.3.4.** *Sea $T\colon V \to W$ una transformación lineal donde $V$ es un espacio vectorial de dimensión finita y $W$ un espacio vectorial. Entonces, si $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ es una base de $V$ tenemos que:*

$$\mathcal{L}\{T(\alpha_1), T(\alpha_2), \ldots, T(\alpha_n)\} = \operatorname{im} T \subset W \tag{2.3.6}$$

*Demostración.* Dado un $\beta \in \operatorname{im} T$ existe un $\alpha \in V$ tal que $T(\alpha) = \beta$.

Tenemos pues un $\alpha \in V$ de la forma:

$$\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n \quad a_i \in \mathbb{F} \quad 1 \leqslant i \leqslant n$$

por lo que $\beta$ tiene la forma:

$$\begin{aligned} \beta = T(\alpha) &= T(a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n) \\ &= a_1T(\alpha_1) + a_2T(\alpha_2) + \cdots + a_nT(\alpha_n) \end{aligned}$$

por lo que podemos ver que:

$$\beta \in \mathcal{L}\{T(\alpha_1), T(\alpha_2), \ldots, T(\alpha_n)\}$$

□

**Definición 2.3.3.** Sean $V, W$ espacios vectoriales sobre $\mathbb{F}$ y sean $T_1 \colon V \to W$ y $T_2 \colon W \to U$ transformaciones lineales.
Definimos la composicion $\circ$ como:

$$\begin{aligned} T_2 \circ T_1 \colon V &\to U \\ v &\to T_2(T_1(v)) \end{aligned} \tag{2.3.7}$$

**Proposición 2.3.5.** *Si* $T_1 \colon V \to W$ *y* $T_2 \colon W \to U$ *son transformaciones lineales, entonces:*

$$T_2 \circ T_1 = \mathcal{L}(V, U) \tag{2.3.8}$$

**Teorema 2.3.2.** *Sea* $T \colon V \to W$ *una transformación lineal con* $V$ *espacio de dimensión finita y* $W$ *es un espacio vectorial, entonces:*

$$\dim V = \dim \ker T + \dim \operatorname{im} T \tag{2.3.9}$$

*Demostración.* Para demostrar este teorema, vamos a considerar tres posibilidades acerca de la $\dim \ker T$, empezaremos con el caso en que $\dim \ker T$, lo cual implica que $\ker T = \{0\}$.

Sea $\alpha_1, \alpha_2, \ldots, \alpha_n$ una base de $V$.

Sabemos que:

$$\mathcal{L}\{T(\alpha_1), T(\alpha_2), \ldots, T(\alpha_n)\} = \operatorname{im} T$$

Ahora veamos que $T(\alpha_1), T(\alpha_2), \ldots, T(\alpha_n)$ son linealmente independientes. Supongamos que $c_1T(\alpha_1) + c_2T(\alpha_2) + \cdots + c_nT(\alpha_n) = 0$. Esto, ya que $T$ es lineal, nos da que:

$$T(c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n) = 0$$

lo cual implica que:

$$c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n \in \ker T = \{0\}$$

es decir:

$$c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n = 0$$

y como $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ es una base de V, tenemos que:

$$c_i = 0 \quad 1 \leqslant i \leqslant n$$

lo cual implica que tambien los $T(\alpha_i)$ son linealmente independientes, esto nos dice que:

$$\dim \operatorname{im} T = n$$

y por lo tanto:

$$\dim V = n = 0 + n = \dim \ker T + \dim \operatorname{im} T$$

Si ahora consideramos el caso en que $\ker T = V$ tenemos que:

$$\ker T = \{\alpha \in V \mid T(\alpha) = 0\} = V$$

Si analizamos la imagen, tendremos:

$$\begin{aligned} \operatorname{im} T &= \{T(\alpha) \mid \alpha \in V\} \\ &= \{T(\alpha) = 0 \mid \alpha \in V\} = \{0\} \end{aligned}$$

y por lo tanto:

$$\dim V = n = n + 0 = \dim \ker T + \dim \operatorname{im} T$$

Si por ultimo, ahora consideramos que $0 < \dim \ker T < n$. Sea $\alpha_1, \alpha_2, \ldots, \alpha_k$ una base de $\ker T$ la cual podemos completar a $\alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n$ para hacer una base de V. Por lo que resta por ver que $T(\alpha_{k+1}), \ldots, T(\alpha_n)$ es una base de $\operatorname{im} T$. Veamos pues que estos generan.

Si $\beta \in \operatorname{im} T$, entonces existe un $\alpha \in V$ tal que:

$$T(\alpha) = \beta$$

con $\alpha$ de la forma:

$$\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_k\alpha_k + a_{k+1}\alpha_{k+1} + \cdots + a_n\alpha_n \quad a_i \in \mathbb{F} \quad 1 \leqslant i \leqslant n$$

por lo que $\beta$ queda de la forma:

$$\begin{aligned} \beta = T(\alpha) &= T(a_1\alpha_1 + a_2\alpha_2 + \cdots + a_k\alpha_k + a_{k+1}\alpha_{k+1} + \cdots + a_n\alpha_n) \\ &= a_1T(\alpha_1) + a_2T(\alpha_2) + \cdots + a_kT(\alpha_k) + a_{k+1}T(\alpha_{k+1}) + \cdots + a_nT(\alpha_n) \end{aligned}$$

pero $a_1\alpha_1 + a_2\alpha_2 + \cdots + a_k\alpha_k$ esta en el nucleo, por lo que:

$$\begin{aligned} \beta = T(\alpha) &= 0 + a_{k+1}T(\alpha_{k+1}) + \cdots + a_n T(\alpha_n) \\ &= a_{k+1}T(\alpha_{k+1}) + \cdots + a_n T(\alpha_n) \end{aligned}$$

por lo que $T(\alpha_{k+1}), \ldots, T(\alpha_n)$ genera a $\operatorname{im} T$.

Veamos ahora que son linealmente independientes. Supongamos que $c_{k+1}T(\alpha_{k+1}) + \cdots + c_n T(\alpha_n) = 0$, por lo que se sigue que:

$$T(c_{k+1}\alpha_{k+1} + \cdots + c_n \alpha_n) = 0$$

por lo que podemos ver que:

$$c_{k+1}\alpha_{k+1} + \cdots + c_n \alpha_n \in \ker T$$

Luego entonces, se puede escribir esto en terminos de:

$$c_{k+1}\alpha_{k+1} + \cdots + c_n \alpha_n = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_k\alpha_k$$

es decir:

$$-a_1\alpha_1 - a_2\alpha_2 - \cdots - a_k\alpha_k + c_{k+1}\alpha_{k+1} + \cdots + c_n\alpha_n = 0$$

del cual, ya sabemos que los coeficientes deben ser todos nulos, por lo que demostramos que $\alpha_{k+1}, \ldots, \alpha_n$ son linealmente independientes. Luego entonces:

$$\dim \operatorname{im} T = n - k$$

y por lo tanto:

$$\dim V = n = k + n - k = \dim \ker T + \dim \operatorname{im} T$$

□

## Ejemplo en un sistema físico

Sea el sistema:

$$\begin{aligned} \dot{x} &= Ax + Bu \\ y &= Cx \end{aligned}$$

con $x(t_0) = x_0$ y $x \in \mathbb{R}^n$, $u \in \mathbb{R}^m$ y las matrices A, B y C son de tamaño apropiado.

Si tomamos como ejemplo el movimiento de un cuerpo en el espacio sometido a una fuerza externa, tendremos que:

$$F = m\frac{d^2r}{dt^2}$$

Si ademas tomamos en cuenta que la masa del cuerpo es unitaria, tenemos que:

$$F = \frac{d^2r}{dt^2}$$

Podemos darnos cuenta que esta fuerza, es nuestro medio de interacción con la dinámica del sistema, por lo que nos conviene definir:

$$u = F = \frac{d^2 r}{dt^2}$$

y la manera en que medimos la respuesta del sistema es por la posición $r$ de la masa. De esta manera tenemos una realización de estado:

$$\begin{aligned} x_1 &= r \\ x_2 &= \dot{r} \end{aligned}$$

y por lo tanto

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= u \end{aligned}$$

lo que nos deja con la siguiente representación matricial del sistema:

$$\begin{aligned} \dot{x} &= \begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} u \\ y &= x_1 = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \end{aligned}$$

Definimos pues las matrices de controlabilidad y observabilidad como:

$$\begin{aligned} Co &= \begin{pmatrix} B & AB & \dots & A^{n-1}B \end{pmatrix} \\ Ob &= \begin{pmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{pmatrix} \end{aligned}$$

las cuales, para nuetro sistema, quedan de la forma:

$$\begin{aligned} \text{rango}\, Co &= \text{rango} \begin{pmatrix} B & AB \end{pmatrix} = \text{rango} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 2 \\ \text{rango}\, Ob &= \text{rango} \begin{pmatrix} C \\ CA \end{pmatrix} = \text{rango} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 2 \end{aligned}$$

Por otro lado, si definimos un sistema auxiliar:

$$\begin{aligned} \dot{\hat{x}} &= A\hat{x} + Bu + k(y - \hat{y}) \\ \hat{y} &= C\hat{x} \end{aligned}$$

en donde el error de este sistema auxiliar estará dado por:

$$e = x - \hat{x}$$

y la derivada del error es:

$$\begin{aligned}
\dot{e} &= \dot{x} - \dot{\hat{x}} = A(x - \hat{x}) - k(Cx - C\hat{x}) \\
&= (A - kC)e = \tilde{A}e
\end{aligned}$$

En donde hemos definido un nuevo sistema para el error del sistema auxiliar. Para que este error tienda a ser cero, pediremos que:

$$\Re\lambda(\tilde{A}) < 0$$

por lo que procederemos a investigar los valores propios de este nuevo sistema.

$$|\tilde{A} - \lambda I| = P(\lambda) = (\lambda - \lambda_1)(\lambda - \lambda_2)$$

en donde $\lambda_1$ y $\lambda_2$ son los valores propios del sistema del error. Cabe mencionar que dado un sistems $2 \times 2$, es facil ver que el desarrollo de este polinomio es:

$$\lambda - (\overbrace{\lambda_1 + \lambda_2}^{\text{traza } \tilde{A}})\lambda + \overbrace{\lambda_1\lambda_2}^{\det \tilde{A}}$$

y la matriz $\tilde{A}$ tiene la forma:

$$\tilde{A} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

**Definición 2.3.4.** Dos estados iniciales $x_1$ y $x_2$ son distinguibles por una entrada $u$ si las salidas producidas por los dos estados iniciales, son diferentes.
Si no son distinguibles, se dice que son indistinguibles. La indistinguibilidad es una relación de equivalencia.


Grafica de dos salidas de un sistema bajo estados distinguibles.

**Teorema 2.3.3.** *Un sistema es completamente observable si y solamente si, la matriz de observabilidad:*

$$\mathrm{Ob} = \begin{pmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{pmatrix} \qquad (2.3.10)$$

*tiene rango igual a la dimensión del espacio de estado.*

*Demostración.* Supongamos que el sistema no es completamente observable, entonces existen $x_1$ y $x_2$ estados diferentes ($x_1 \neq x_2$) no distinguibles, es decir:

$$y(x_1, t, u) = y(x_2, t, u) \quad \forall u \quad \forall t \geqslant 0$$

Dado esto, del sistema original podemos sacar la siguiente conclusión:

$$\begin{aligned}
\dot{x} &= Ax + Bu \\
\dot{x} - Ax &= Bu \\
\exp(-At)(\dot{x} - Ax) &= \exp(-At)Bu \\
(\exp(-At)x)' &= \exp(-At)Bu \\
\exp(-At)x &= \int_0^t \exp(-A\tau)Bu(\tau)d\tau + k \\
x &= \exp(At)\int_0^t \exp(-A\tau)Bu(\tau)d\tau + k\exp(At) \\
x &= \int_0^t \exp A(t-\tau)Bu(\tau)d\tau + \exp(At)x_0
\end{aligned}$$

teniendo que la ecuación de salida es:

$$\begin{aligned}
y(x_1) &= Ce^{At}x_1 + \int_0^t e^{A(t-\tau)}Bu(\tau)d\tau \\
y(x_2) &= Ce^{At}x_2 + \int_0^t e^{A(t-\tau)}Bu(\tau)d\tau
\end{aligned}$$

pero tenemos que $y(x_1) = y(x_2)$, por lo que:

$$C\exp(At)(x_1 - x_0) = 0 \quad x_1 \neq x_0$$

Dada esta ecuación, podemos construir un sistema derivando de la siguiente manera:

$$\begin{aligned}
C\exp(At)(x_1 - x_0) &= 0 \\
CA\exp(At)(x_1 - x_0) &= 0 \\
&\vdots \\
CA^{n-1}\exp(At)(x_1 - x_0) &= 0
\end{aligned}$$

reemplazando a $x_1 - x_0$ simplemente con $x$, tenemos que:

$$\begin{pmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{pmatrix} \exp{(At)} x = 0$$

y ya que por definición $\exp{(AT)} \neq 0$, tenemos que:

$$\begin{pmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{pmatrix} x = 0$$

es decir:

$$x \in \ker \begin{pmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{pmatrix}$$

y como $x_1 - x_0 = x \neq 0$, sabemos que:

$$\dim \ker \begin{pmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{pmatrix} \neq 0$$

Por otro lado, tenemos que:

$$\dim Ob = \dim \begin{pmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{pmatrix} = n$$

y dado que:

$$\begin{aligned} \dim Ob &= \dim \ker Ob + \dim \operatorname{im} Ob \\ n &= a + b \end{aligned}$$

con $a \neq 0$, lo que nos da que rango $Ob < n$, lo cual no es posible si el sistema es completamente observable, luego la hipotesis es falsa y concluimos que para que el sistema sea completamente observable $Ob$ debe ser de rango pleno. $\square$

## 2.4. Operadores lineales

### Definiciones

**Definición 2.4.1.** Sea $V$ un espacio vectorial con una transformación lineal $T\colon V \to V$. A $T$ se le llama operador lineal.

*Observación* 2.4.1. Si $T$ es operador lineal en $V$, escribimos:

$$T^2 = T \circ T \tag{2.4.1}$$

y en general:

$$T^n = \overbrace{T \circ T \circ T \cdots \circ T}^{n \text{ veces}} \tag{2.4.2}$$

o bien:

$$T^n = T^{n-1} \circ T \tag{2.4.3}$$

para $n \geqslant 2$.

**Proposición 2.4.1.** *Sea $T\colon V \to W$ una transformación lineal, entonces el hecho de que $T$ se isomorfismo, implica que $T$ sea invertible y bisceversa, es decir:*

$$T \text{ es isomorfismo} \iff T \text{ es invertible} \tag{2.4.4}$$

*Recordando que $T$ es invertible si existe una $T^{-1}$ por la izquierda y por la derecha, tal que:*

$$\begin{aligned} T^{-1} \circ T &= I_V \\ T \circ T^{-1} &= I_W \end{aligned} \tag{2.4.5}$$

*Demostración.* Para comprobar esta proposición empezaremos asumiendo que $T$ es invertible, esto es existe un $T^{-1}$.

Supongamos ahora que:

$$T(x_1) = T(x_2) \quad x_1, x_2 \in V \tag{2.4.6}$$

si componemos con $T^{-1}$ por la izquierda:

$$\begin{aligned} T^{-1} \circ T(x_1) &= T^{-1} \circ T(x_2) \\ I_V(x_1) &= I_V(x_2) \\ x_1 &= x_2 \end{aligned}$$

por lo que $T$ es inyectiva.
Si ahora, tenemos un $y \in W$ tal que $x = T^{-1}(y)$, por lo que:

$$T(x) = T(T^{-1}(y)) = T \circ T^{-1}(y) = I_W(y) = y$$

Por lo que $T$ es suprayectiva, y por lo tanto $T$ es isomorfismo. □

**Proposición 2.4.2.** *Si $T$ es transformación lineal de $V$ en $W$ y $T$ es invertible, entonces: $T^{-1}\colon W \to V$ es lineal.*

# 2.5. Funcionales lineales

## Definiciones

**Lema 2.5.1.** *Sea $\mathbb{F}$ un campo y $V$ un espacio vectorial sobre $\mathbb{F}$.*
*$\mathbb{F}$ como espacio vectorial sobre $\mathbb{F}$ tiene dimensión uno.*

*Demostración.* Sea $\{1\}$ un generador y un elemento linealmente independiente.

1. $k \cdot 1 = 0 \implies k = 0$, por lo que $1$ es linealmente independiente.

2. $a \in \mathbb{F}$, $a = a \cdot 1$, por lo que $1$ es generador.

por lo que $1$ es base y $\mathbb{F}$ es de dimensión $1$. □

**Definición 2.5.1.** Un funcional lineal de $V$ es una transformación lineal, tal que:

$$f\colon V \to \mathbb{F} \tag{2.5.1}$$

# 2.6. Espacio dual

## Definiciones

**Definición 2.6.1.** El espacio dual de $V$ es denotado por $V^*$, tal que:

$$V^* = \{f \mid f \text{ es funcional lineal de } V\} = \mathcal{L}(V, \mathbb{F}) \tag{2.6.1}$$

*Observación* 2.6.1. Sea $V, W$ espacios vectoriales sobre $\mathbb{F}$, si $\dim V = n$ y $\dim W = m$.

$$\dim \mathcal{L}(V, W) = m \cdot n \tag{2.6.2}$$

*Observación* 2.6.2. Utilizando la observación anterior, podemos decir que:

$$\dim V^* = \dim \mathcal{L}(V, \mathbb{F}) = 1 \cdot n = n = \dim V \tag{2.6.3}$$

por lo que $V^*$ es isomorfo a $V$.

**Definición 2.6.2.** Si $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ es una base de $V$, consideremos $\{1\}$ una base para $\mathbb{F}$, entonces definimos:

$$f_i(\alpha_k) = \delta_{ik} = \begin{cases} 1 & \text{Si } i = k \\ 0 & \text{Si } i \neq k \end{cases} \tag{2.6.4}$$

**Definición 2.6.3.** Si $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ es base de $V$, la base $\{f_1, f_2, \ldots, f_n\}$ de $V^*$ dada por 2.6.4 se llama base dual a la base $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$

**Ejemplo 2.6.1.**

**Ejemplo 2.6.2.**

**Ejemplo 2.6.3.**

**Ejemplo 2.6.4.**

**Proposición 2.6.1.** *Si $\{f_i\}_{1\leqslant i\leqslant n}$ es la base dual de $V^*$ a la base $\{\alpha_i\}_{1\leqslant i\leqslant n}$ de $V$, entonces tenemos que:*

1. *Si $f \in V^*$, entonces $f = \sum_{i=1}^{n} f(\alpha_i) f_i$*
2. *Si $\alpha \in V$, entonces $\alpha = \sum_{i=1}^{n} f_i(\alpha)\alpha_i$*

*Demostración.* Sea $\alpha \in V$ de la forma:

$$\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$$

$$\begin{aligned} \left[\sum_{i=1}^{n} f(\alpha_i) f_i\right](\alpha) &= \sum_{i=1}^{n} f(\alpha_i) f_i(\alpha) \\ &= \sum_{i=1}^{n} f(\alpha_i) f_i(a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n) \\ &= \sum_{i=1}^{n} f_i(\alpha) a_i \end{aligned}$$

$\square$

**Ejercicio 2.6.1.** Determinar explicitamente la base dual a la base $v_1 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}, v_2 = \begin{pmatrix} 0 & 1 & 1 \end{pmatrix}$ y $v_3 = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}$ de $\mathbb{R}^3$.

**Ejercicio 2.6.2.** Sea $f$ el funcional lineal en $\left(\mathbb{R}^3\right)^*$ dado por:

$$f(\begin{pmatrix} x & y & z \end{pmatrix}) = x + y + z$$

Exprese $f$ como combinación lineal de la base dual encontrada en $a$.

## 2.7. Teorema de Cayley - Hamilton

**Definición 2.7.1.** Toda matriz es un cero de su polinomio caracteristico

*Demostración.* Sea $A$ una matriz cuadrada arbitraria de tamaño $n \times n$ y $P(\lambda)$ su polinomio caracteristico, es decir:

$$P(\lambda) = |\lambda I - A| = \lambda^n + \cdots + a_1\lambda + a_0$$

Supongamos ahora que $B(\lambda)$ representa a la adjunta de la matriz $\lambda I - A$, entonces los elementos de $B(\lambda)$ son los cofactores de la matriz $\lambda I - A$ y por lo tanto son polinomios en $\lambda$ de grado no mayor que $n-1$. Por lo tanto $B(\lambda)$ tiene la forma:

$$B(\lambda) = B_{n-1}\lambda^{n-1} + \cdots + B_1\lambda + B_0$$

donde $B_i$ son matrices $n \times n$ sobre un campo $K$.

Por la propiedad fundamental de la adjunta:

$$(\lambda I - A)B(\lambda) = |\lambda I - A|I$$

de aqui tenemos que:

$$(\lambda I - A)(B_{n-1}\lambda^{n-1} + \cdots + B_1\lambda + B_0) = (\lambda^n + \cdots + a_1\lambda + a_0)I$$

Quitando los parentesis e igualando los coeficientes de las mismas potencias de $\lambda$, tenemos:

$$\begin{aligned}
B_{n-1} &= I && (\lambda^n)\\
B_{n-2} - AB_{n-1} &= a_{n-1}I && (\lambda^{n-1})\\
B_{n-3} - AB_{n-2} &= a_{n-2}I && (\lambda^{n-2})\\
&\vdots\\
B_0 - AB_1 &= a_1 I && (\lambda^1)\\
-AB_0 &= a_0 I && (\lambda^0)
\end{aligned}$$

Si ahora multiplicamos estas ecuaciones matriciales por $A^n, A^{n-1}, \ldots, A, I$, tendremos:

$$\begin{aligned}
A^n B_{n-1} &= A^n && (\lambda^n)\\
A^{n-1}B_{n-2} - A^n B_{n-1} &= a_{n-1}A^{n-1} && (\lambda^{n-1})\\
A^{n-2}B_{n-3} - A^{n-1}B_{n-2} &= a_{n-2}A^{n-2} && (\lambda^{n-2})\\
&\vdots\\
AB_0 - A^2B_1 &= a_1 I && (\lambda^1)\\
-AB_0 &= a_0 I && (\lambda^0)
\end{aligned}$$

Y al sumar todas las ecuaciones tendremos:

$$0 = A^n + a_{n-1}A^{n-1} + a_{n-2}A^{n-2} + \cdots + a_1 A + a_0 I = P(A)$$

□

**Ejemplo 2.7.1.** El polinomio caracteristico de la matriz:

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

Obtenemos su polinomio caracteristico:

$$\begin{aligned} |\lambda I - A| &= \det(\lambda I - A) = |A - \lambda I| \\ &= \begin{vmatrix} 1-\lambda & 2 \\ 3 & 2-\lambda \end{vmatrix} = (1-\lambda)(2-\lambda) - 6 \\ &= \lambda^2 - 3\lambda - 4 = P(\lambda) \end{aligned}$$

y podemos ver que $A$ es un cero de $P(\lambda)$.

$$\begin{aligned} P(A) &= A^2 - 3A - 4I = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}^2 - 3\begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix} - 4\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 7 & 6 \\ 9 & 10 \end{pmatrix} - \begin{pmatrix} 3 & 6 \\ 9 & 6 \end{pmatrix} - \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

## 2.8. Diagonalización

### Definiciones

**Definición 2.8.1.** Sea $V$ un espacio vectorial de dimensión finita $n$ y $T\colon V \to V$ un operador lineal, entonces $T$ puede representarse por una matriz $n \times n$ $A$. Por esta razón en algunas ocasiones nos vamos a referir a valores y vectores propios de matrices $n \times n$.

**Teorema 2.8.1.** *Sea $A$ una matriz $n \times n$. Entonces $\lambda$ es un valor propio de $A$ si y solo si:*

$$p(\lambda) = \det(A - \lambda I) = 0 \tag{2.8.1}$$

**Proposición 2.8.1.** *Sabemos que $p(\lambda)$ se puede escribir como:*

$$p(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0 = 0 \tag{2.8.2}$$

*Esta ecuación tiene $n$ raices, varias de las cuales pueden repetirse.*

*Si $\lambda_1, \lambda_2, \dots, \lambda_k$ son las diferentes raices de $p(\lambda)$ con multiplicidad $r_1, r_2, \dots, r_k$ respectivamente, entonces $p(\lambda)$ puede factorizarse como:*

$$p(\lambda) = (\lambda - \lambda_1)^{r_1}(\lambda - \lambda_2)^{r_2} \dots (\lambda - \lambda_k)^{r_k} = 0 \tag{2.8.3}$$

*en donde los numeros $r_1, r_2, \dots, r_k$ se llaman multiplicidades algebraicas de los valores propios $\lambda_1, \lambda_2, \dots, \lambda_k$ respectivamente.*
*Sea $\lambda$ un valor propio de $T$ y sea:*

$$E_\lambda = \{v : Tv = \lambda v\} = \{v : (T - \lambda I)v = 0\} \tag{2.8.4}$$

*El subespacio $E_\lambda$ (pues es el nucleo de la transformación lineal $T - \lambda I$) se llama espacio propio de $T$ correspondiente al valor propio $\lambda$.*
*Como $E_\lambda$ es un subespacio entonces $0 \in E_\lambda$, pero $\dim E_\lambda > 0$ pues por definición, si $\lambda$ es un valor propio, entonces existe un vector propio diferente de cero correspondiente a $\lambda$.*

**Teorema 2.8.2.** *Sea $V$ un espacio vectorial de dimensión finita $n$ y $T: V \to V$ un operador lineal y sean $\lambda_1, \lambda_2, \dots, \lambda_n$ valores propios diferentes de $T$ con sus correspondientes vectores propios $v_1, v_2, \dots, v_n$. Entonces $v_1, v_2, \dots, v_n$ son linealmente independientes.*

**Proposición 2.8.2.** *Sea $A$ una representación matricial de $T$. Supongamos que $A$ es una matriz de $3 \times 3$.*

1. *Si $A$ tiene tres diferentes valores propios $\lambda_1, \lambda_2, \lambda_3$ (cada uno con multiplicidad algebraica uno), entonces, por el primer teorema, sus respectivos vectores propios $v_1, v_2, v_3$ son linealmente independientes.*

2. *Si $A$ tiene dos vectores propios $\lambda_1$ y $\lambda_2$ con multiplicidad algebraica uno y dos respectivamente. Entonces $\dim E_{\lambda_2} \leqslant 2$, porque de otra manera, podriamos tener al menos cuatro vectores linealmente independientes en un espacio de tres dimensiones. Es decir, para $\lambda_2$ puede haber uno o deos vectores propios linealmente independientes.*

3. *Si $A$ tiene un valor propio $\lambda$ con multiplicidad algebraica tres, entonces $\dim E_\lambda \leqslant 3$, es decir, puede haber uno, dos o tres vectores propios linealmente independientes.*

**Teorema 2.8.3.** *Sea $\lambda$ un valor propio para $T$ operador lineal en un espacio vectorial de dimensión finita, entonces:*

$$1 \leqslant \dim E_\lambda \leqslant \textit{multiplicidad algebraica de } \lambda \tag{2.8.5}$$

## 2.9. Forma canónica de Jordan

## 2.10. Vectores propios generalizados

## Capítulo 3

# Ecuaciones diferenciales

### 3.1. Solución de una ecuación diferencial

### 3.2. Existencia y unicidad de las soluciones de una ecuación diferencial

### 3.3. Soluciones aproximadas

### 3.4. Relación entre soluciones aproximadas y exactas