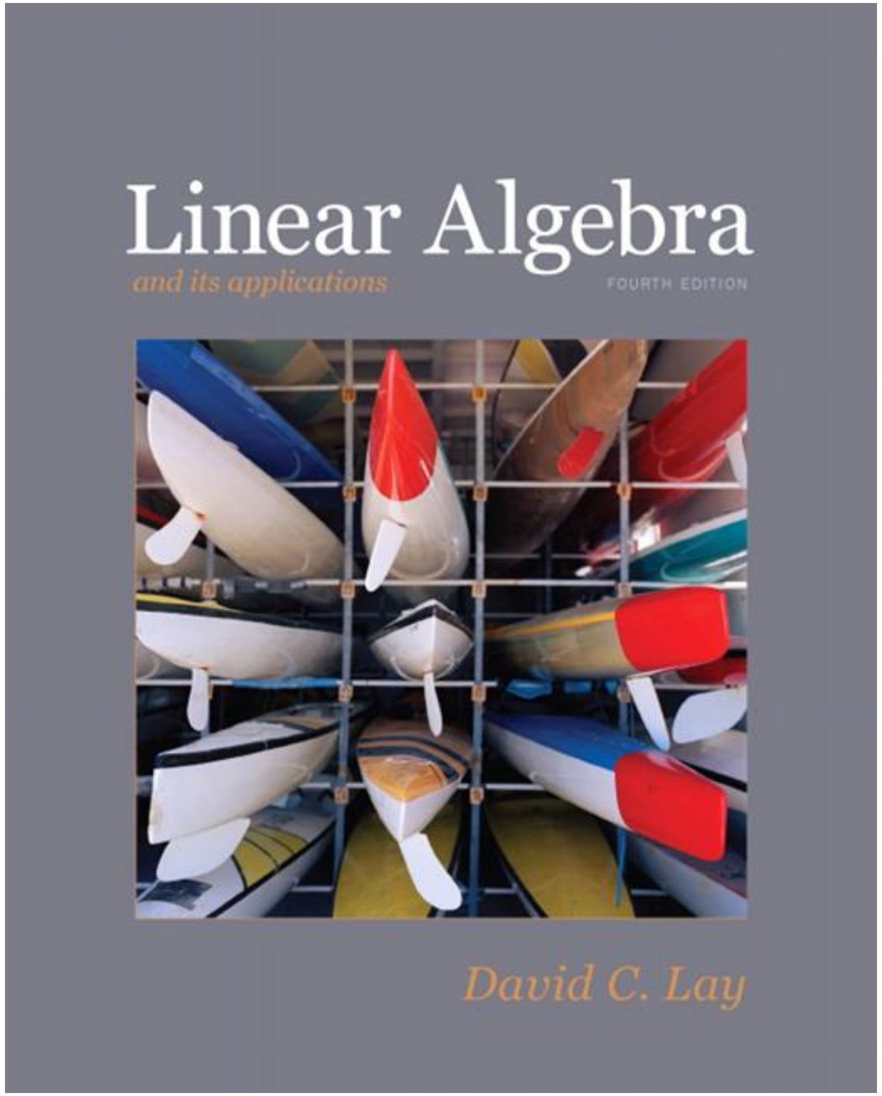
Tema 1

Funciones y matrices básico

UNIVERSIDAD FRANCISCO DE VITORIA
VINCE IN BONO MALUM

FUENTE Y REFERENCIAS



Funciones

Introducción a las funciones

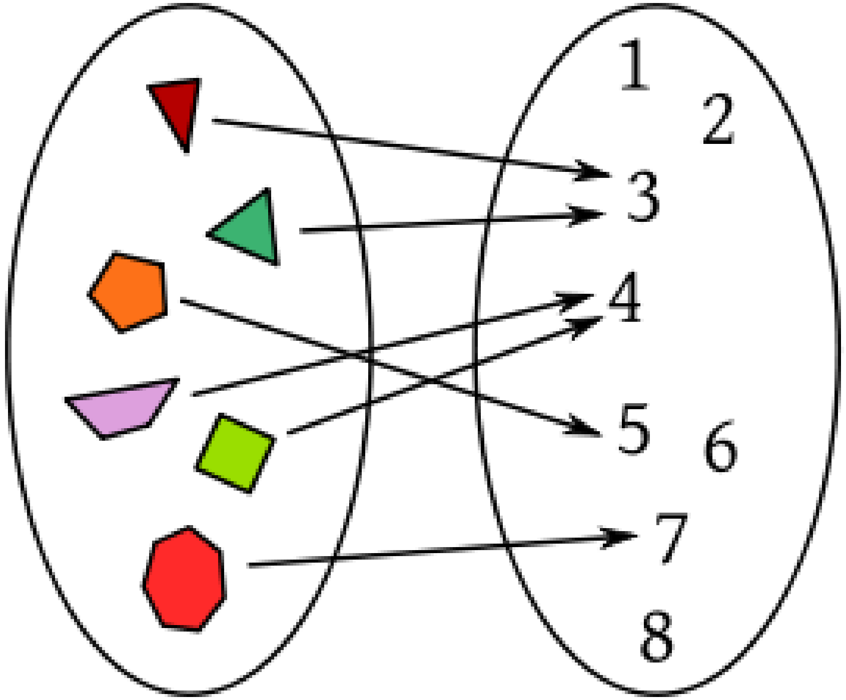
UNIVERSIDAD
FRANCISCO DE VITORIA
VINCE IN BONO MALUM

Cuestiones a repasar

UNIVERSIDAD FRANCISCO DE VITORIA

- Funciones y tipos de funciones
- Matriz cuadrada
- Matriz diagonal
- Matriz identidad
- Traza de una matriz
- Matriz transpuesta
- Suma de matrices
- Producto de matrices
- Determinante de una matriz
- Sistema de ecuaciones HOMOGÉNEO

Función



Estructura algebraica

- Sea *E* un conjunto no vacío, una función *f*

$$f : E \times E \mapsto E$$

  se llama **ley de composición interna** (operación) sobre *E*. Además, la imagen *f*(*a*,*b*) se llama el operado de *a* y *b*.
- Es usual representar las operaciones internas con algunos símbolos especiales, en vez de letras, como *, Δ, $\perp$, entre otros.
- Por definición, si * es una ley de composición interna sobre *E*, entonces es **cerrada** sobre *E*, es decir, se cumple que

$$\forall a, b \in E\left[a * b \in E\right]$$

Estructuras Algebraicas (cont.)

- Si * es una ley de composición interna sobre *E*, se dice que (*E*,*) posee una **estructura algebraica**.
- Una **estructura algebraica** es una *n*-tupla $(a_1, a_2, \ldots, a_n)$, donde a_1 es un conjunto dado no vacío, y $\{a_2, \ldots, a_n\}$ un conjunto de operaciones aplicables a los elementos de dicho conjunto.
- Si * es una ley de composición interna sobre *E*, se dice que *:
  - Es **asociativa:** para cualesquiera elementos del grupo no importa el orden en que se operen las parejas de elementos, mientras no se cambie el orden de los elementos, siempre dará el mismo resultado.

$$\text{Si } \forall a, b \in E \text{ se cumple } (a * b) * c = a * (b * c)$$

Estructuras Algebraicas (cont.)

- Si * es una ley de composición interna sobre *E*, se dice que *:
  - Posee **elemento neutro o elemento identidad** (comúnmente denotado como *e*, letra inicial de la palabra alemana ***einheit***, que significa "unidad"): existe un elemento que al ser operado con cualquier otro, no lo modifica (como el cero en la suma o el 1 en la multiplicación). La unicidad del elemento neutro es fácilmente demostrable.

$$\text{Si } \exists e \in \forall a \in E \text{ tal que } a * e = e * a = a$$

  - Tiene **elementos opuestos o inversos**: todos los elementos del grupo tienen un elemento opuesto (o inverso), con el que al operarse dan por resultado el elemento neutro *e*. El elemento inverso de uno dado es único.

$$\text{Si } \forall a \in E \wedge \exists b \in E \text{ tal que } a * b = b * a = e$$

$$\text{en cuyo caso se escribe } a^{-1} = b$$

Estructuras Algebraicas (cont.)

- Si * es una ley de composición interna sobre *E*, se dice que *:
  - Es **conmutativa**: para cualesquiera elementos del grupo no importa el orden de los elementos siempre dará el mismo resultado. $\text{Si } \forall a,b \in E \text{ se cumple } a * b = b * a$
- Un elemento *h* es **absorbente** por la izquierda si $h * a = h$ y lo es por la derecha si $a * h = h$ para todo *a*. Se dice que es el elemento absorbente si lo es por la derecha y por la izquierda.

Estructuras Algebraicas (cont.)

- Un elemento *a* es **idempotente** si $a * a = a$ para todo *a*.
- Un elemento *a* es **involutivo** si $a * a = e$ para todo *a*.
- Un elemento *a* es **central** si conmuta con todos los elementos de *E*, el conjunto formado por todos los elementos centrales se llama el **centro de *E*** y se denota por $C(E)$.
  - $(C(E),*)$ es un subgrupo de $(E,*)$.

$$C(E) = \{a \in E \mid ab = ba, \forall b \in E\}$$

- Si G es un conjunto no vacío y * es una operación interna definida sobre G. Se dice que $(G,*)$ es:
  - Un **semigrupo** si * es asociativa.
  - Un **monoide** si es un semigrupo con elemento neutro.
  - Un **grupo** si es un monoide que cumple la propiedad de los inversos, es decir, $(G,*)$ es un grupo si * es cerrada, asociativa, posee elemento neutro y cada elemento tiene inverso.
  - Un **grupo abeliano** o **grupo conmutativo** si es un grupo y se cumple la conmutatividad. En el caso de que no sea un grupo, se dice que la estructura algebraica es conmutativa.

- Notaciones:
  - La notación multiplicativa $\otimes$.
    - Operación: $*$, $\times$, $\bullet$, llamada producto.
    - Elemento neutro: 1.
    - Elemento inverso: x^{-1}.
  - La notación aditiva $\oplus$.
    - Operación: +, llamada suma.
    - Elemento neutro: 0.
    - Elemento opuesto de un elemento x del grupo: $-x$.

Grupos (cont.)

- Si $(G,*)$ es un monoide, se tiene que $a^0 = e$, y para n natural, con $n \geq 1$:

$$a^n = a * a^{n-1}$$

$$a^n = \underbrace{a * a * a * \ldots * a}_{n \text{ veces } a}$$

- Si además cumple con la propiedad de los inversos, los exponentes negativos se definen como:

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

- **Teorema 1.** Si $(G,*)$ es un grupo, en general se tiene que

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

$$\left(a^{-1}\right)^{-1} = a \qquad (2)$$

- **Demostración.**

(1)

$$(a*b)*(a*b)^{-1} = e$$

$$\begin{aligned}(a*b)*\left(b^{-1}*a^{-1}\right) &= a*\left(b*b^{-1}\right)*a^{-1}\\ &= a*e*a^{-1}\\ &= a*a^{-1}\\ &= e\end{aligned}$$

(2)

$$\begin{aligned}\left(a^{-1}\right)^{-1} &= \left(a^{-1}\right)^{-1}*e\\ &= \left(a^{-1}\right)^{-1}*\left(a^{-1}*a\right)\\ &= \left(\left(a^{-1}\right)^{-1}*a^{-1}\right)*a\\ &= e*a\\ &= a\end{aligned}$$

- Notar que si el grupo es abeliano se puede escribir

$$(a*b)^{-1}=a^{-1}*b^{-1}$$

- En caso contrario se debe respetar (1) del teorema 1.
- Si el grupo es finito, su **orden** se denota por $o(G)$ y corresponde a la cardinalidad como conjunto.

Otras cuestiones importantes

- Cuerpo: En álgebra, un cuerpo es una estructura algebraica en la cual las operaciones de adición, substracción, multiplicación, y división (excepto la división por cero) se pueden realizar y las reglas asociativas, conmutativas y distributivas valen, las que son familiares de la aritmética de números ordinarios
  - Los números reales ($\mathbb{R}$), los números racionales ($\mathbb{Q}$), o los números complejos ($\mathbb{C}$), son ejemplos de cuerpos

Anillos

- Un **anillo** es una estructura algebraica formada por un conjunto y dos operaciones que están relacionadas entre sí, mediante la propiedad distributiva, de manera que generalizan las nociones de número, especialmente en el sentido de su "operabilidad".
  - En un anillo se tienen un conjunto no vacío *A*, y dos operaciones binarias + y •.

Anillos (cont.)

- Un anillo es un triple $(A,*,\circ)$, lo cual es una estructura algebraica en la cual A es un conjunto no vacío y $*,\circ: A \times A \to A$ son dos operaciones binarias definidas sobre A que satisfacen las condiciones siguientes:
  - $(A,*)$ es un grupo abeliano.
  - $(A,\circ)$ es un semigrupo.
  - La operación $\circ$ es distributiva respecto a la operación $*$. Esto es, para todo $a,b \in A$

$$\begin{cases} a \circ (b * c) = (a \circ b) * (a \circ c) \\ (a * b) \circ c = (a \circ c) * (b \circ c) \end{cases}$$

Anillos (cont.)

- Cuando $(A,\circ)$ es un monoide se dice que A es un **anillo unitario** o **anillo con unidad** que representaremos por 1 (elemento neutro del producto).
- Cuando $(A,\circ)$ es un semigrupo conmutativo, se dice que A es **anillo conmutativo** o **anillo abeliano**.

Anillos (cont.)

- Para trabajar con una notación más familiar, el anillo $(A,+,\bullet)$, en el cual:
  - El neutro de $(A,+)$ se denota 0, y para todo $x \in A$, a su inverso (para la operación +) se denotará $-x$.
  - Si la operación $\bullet$ posee neutro en A, éste se denotará por 1 y se dice que $(A,+,\bullet)$ es un **anillo con unidad**.
  - Si $x \in A$ posee inverso para la operación $\bullet$, éste se denotará por x^{-1}. Si $\bullet$ es conmutativa, $(A,+,\bullet)$ se llamará **anillo conmutativo**.

Anillos (cont.)

- El ejemplo más sencillo y representativo de estructura de anillo se encuentra en (Z,+,•), el anillo de los enteros. Este anillo tiene unidad y es conmutativo.
- Por similitud con (Z,+,•), cuando tratemos con un anillo unitario cualquiera, en general se refiere a la suma y al producto como primera y segunda operación, respectivamente, y se utiliza el 0 y el 1 como neutros respectivos.
  - Para abreviar la notación, se escribe ab en lugar de $a \bullet b$.

Anillos (cont.)

- Los axiomas de anillo son una abstracción del comportamiento de los números enteros respecto de las operaciones aritméticas elementales: la suma y el producto.
- Otra clase importante de anillos abelianos unitarios finitos es $(Z_n,+,\bullet)$ el anillo de los enteros módulo n.

Anillos (cont.)

- Sea $(A,+,\bullet)$ un anillo, entonces:
  - $(\forall x \in A)\ 0 \bullet x = x \bullet 0 = 0$.
  - $(\forall x,y \in A)\ -(x \bullet y) = (-x) \bullet y = x \bullet (-y)$.
  - $(\forall x,y \in A)\ (-x) \bullet (-y) = x \bullet y$.
  - Si el anillo posee unidad, entonces $(\forall x \in A)\ -x = (-1) \bullet x = x \bullet (-1)$.
- La **ley de simplificación** es otra propiedad importante que cumplen los números enteros, es decir, para todo $a,b,c \in Z^* = Z - \{0\}$ se verifica $ab = ac \Rightarrow b = c$.

Homomorfismos de Grupo

- Si $(G,*)$ y $(F,\perp)$ son dos grupos. Se dice que una aplicación $f: G \to F$ es un **homomorfismo de grupos** si para todo a y b en G se satisface que $f(a * b) = f(a) \perp f(b)$. Si, además de ser homomorfismo,
  - f es sobreyectiva, entonces f es un **epimorfismo**.
  - f es inyectiva, entonces f es un **monomorfismo**.
  - f es biyectiva, entonces f es un **isomorfismo**.
  - $G = F$, entonces f es un **endomorfismo**.
  - $G = F$ y biyectiva, entonces f es un **automorfismo**.

Homomorfismos de Grupo (cont.)

- Para un homomorfismo de grupos $f : G \to F$ se define el **núcleo de f** como el conjunto $N_f = f^{-1}(\{e'\})$, donde e' es el elemento neutro de F.
  - El núcleo de un homomorfismo está formado por los elementos cuya imagen es el neutro.
    - $ker_f = N_f = \{x \in G \mid f(x) = e'\}$

Imagen de φ [editar]

El conjunto de todos los elementos de H que son la imagen de algún elemento de G se llama la imagen de la aplicación, y se denota $\mathrm{Im}(\varphi)$ o $\varphi(G)$.[2] Formalmente:

$$\mathrm{Im}(\varphi) : \{\mathrm{h} \in \mathrm{H} : \mathrm{h} = \varphi(\mathrm{g}),\ \text{para algún } \mathrm{g} \in \mathrm{G}\}$$

La imagen de φ es un subgrupo de H.

El núcleo o kernel [editar]

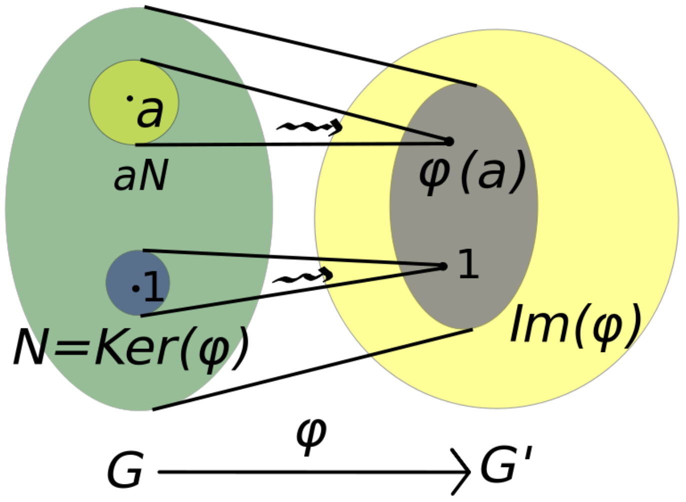
El conjunto de todos los elementos de G cuya imagen es el elemento identidad de H se llama núcleo (*kernel*) de φ:

$$\ker(\varphi) : \{g \in G : \varphi(g) = 1_H\}$$

El núcleo de φ es un subgrupo normal de *G*. El núcleo es importante porque no sólo determina qué elementos tienen por imagen la identidad, sino también qué elementos tienen la misma imagen:[3]

Dado $a \in G \to \varphi(a \circ k) = \varphi(a) \qquad \forall k \in \ker(\varphi)$
ya que $\varphi(a \circ k) = \varphi(a) * \varphi(k) = \varphi(a) * 1_H = \varphi(a)$

Los conjuntos de todos los elementos que comparten una misma imagen son las clases laterales del núcleo.



Homomorfismos de Grupo (cont.)

- **Teorema.** Si $f: G \to F$ es un homomorfismo de grupos, si e es el elemento neutro de G y además e' es el elemento neutro de F, entonces se cumple que

$$f(e) = e' \qquad (1)$$

$$f\left(x^{-1}\right) = [f(x)]^{-1} \qquad (2)$$

- **Demostración.**

(1)

$$f(x) = f(x * e) = f(x) \perp f(e)$$
$$f(x) = f(x) \perp f(e) = f(x) \perp e'$$
$$f(e) = e'$$

(2)

$$f(e) = e' \Rightarrow f\left(x * x^{-1}\right) = f(x) \perp f\left(x^{-1}\right)$$
$$f(x) \wedge f\left(x^{-1}\right) \text{son inversos entre sí}$$
$$f\left(x^{-1}\right) = [f(x)]^{-1}$$

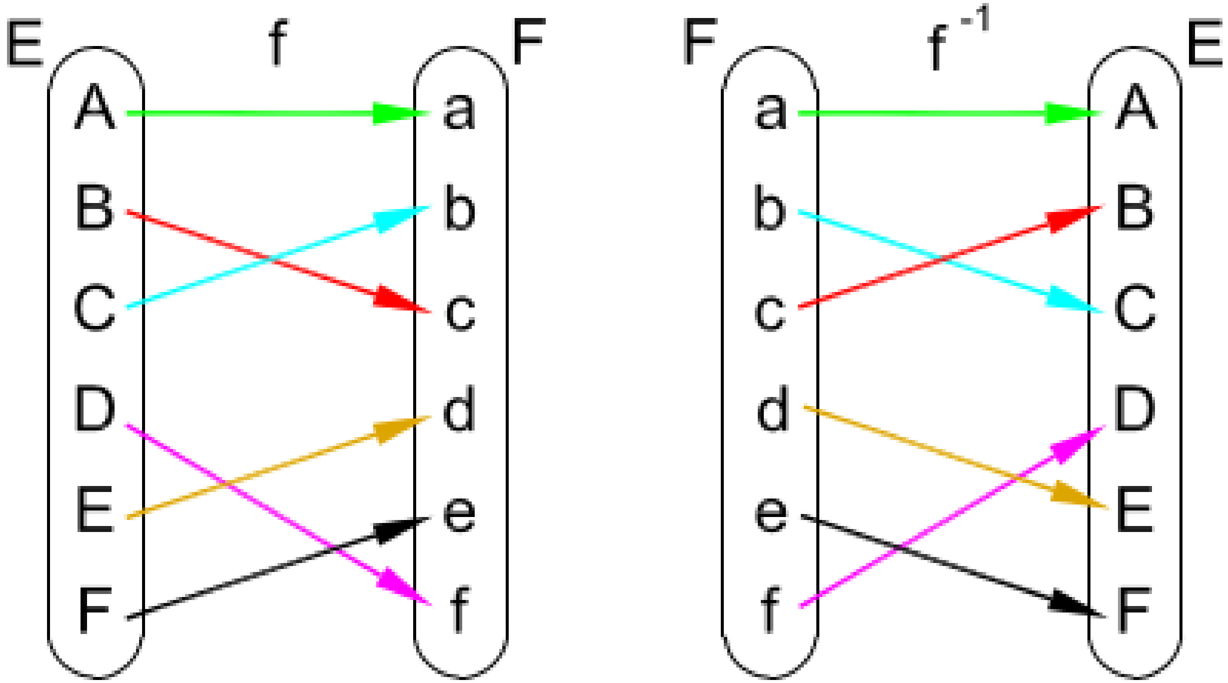
Homomorfismos de Grupo (cont.)

- **Teorema.** Sea $f: G \rightarrow F$ es un homomorfismo de grupos, con e el elemento neutro de G y e' el elemento neutro de F, si $N_f = \{e\}$ entonces f es inyectiva.
- **Demostración.**

$$
\begin{aligned}
f(a) = f(b) \Rightarrow f(a)[f(b)]^{-1} &= e' \\
\Rightarrow f(a)f\left(b^{-1}\right) &= e' \\
\Rightarrow f\left(ab^{-1}\right) &= e' \\
\Rightarrow ab^{-1} \in N_f &= \{e\} \\
\Rightarrow ab^{-1} &= \{e\} \\
\Rightarrow a &= b \\
f \text{ es inyectiva}
\end{aligned}
$$

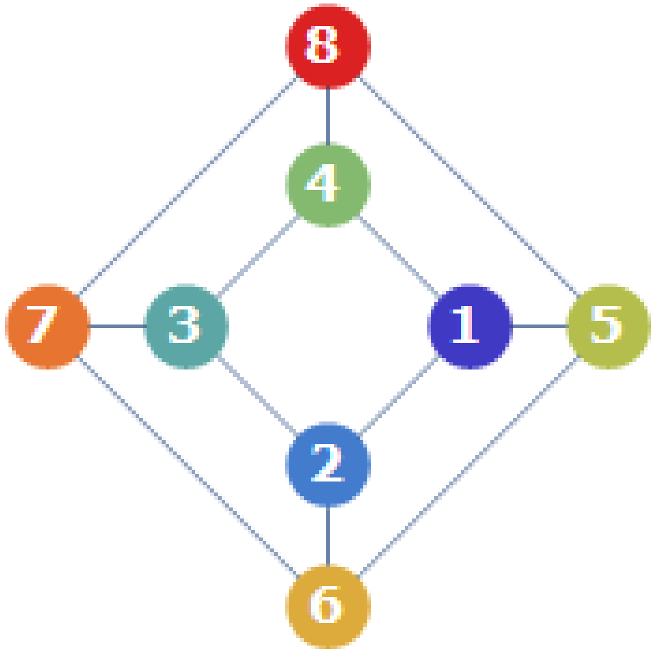
- A recordar:
  - Un homomorfismo que es también una biyección tal que su inversa es también un homomorfismo se llama isomorfismo; dos objetos isomorfos son totalmente indistinguibles por lo que a la estructura en cuestión se refiere.
  - Un homomorfismo de un conjunto a sí mismo se llama endomorfismo, y si es también un isomorfismo se llama automorfismo.
  - Un homomorfismo que es **sobreyectivo** se llama epimorfismo.
  - Un homomorfismo que es **inyectivo** se llama monomorfismo.

Biyección



Es biyectiva, luego tiene recíproca

Isomorfismo



$1 \rightarrow a$

$2 \rightarrow e$

$3 \rightarrow b$

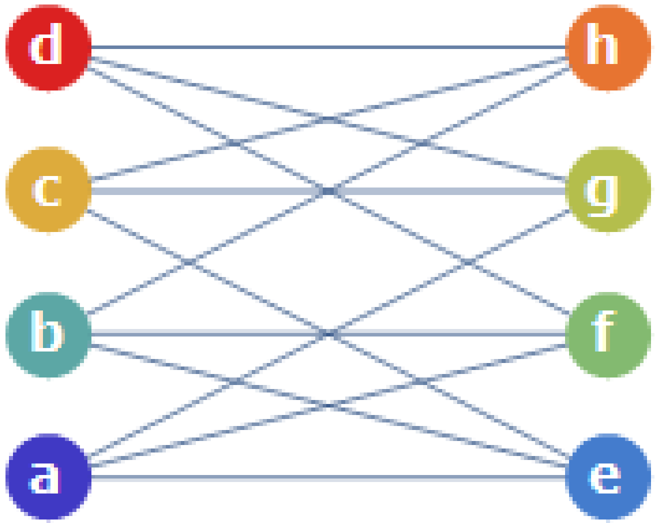
$4 \rightarrow f$

$5 \rightarrow g$

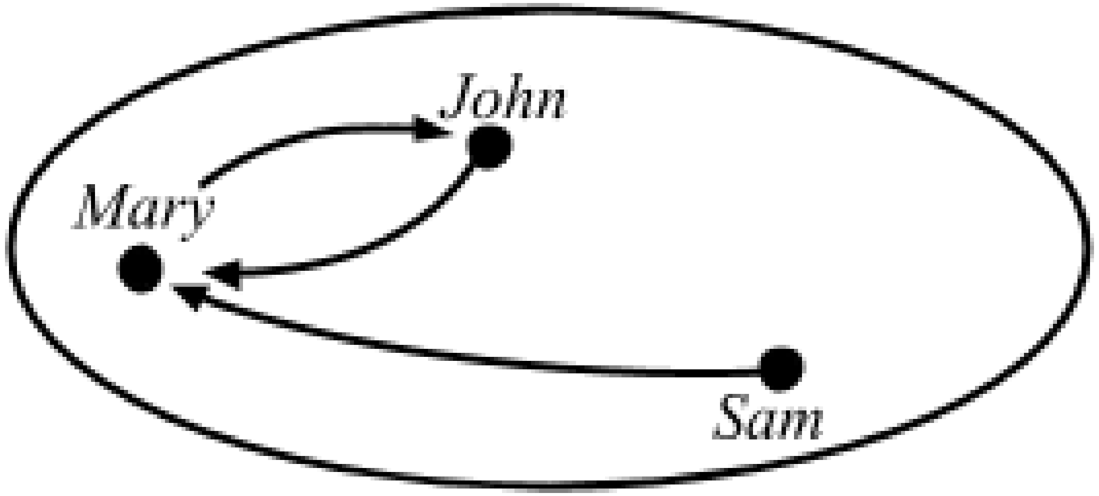
$6 \rightarrow c$

$7 \rightarrow h$

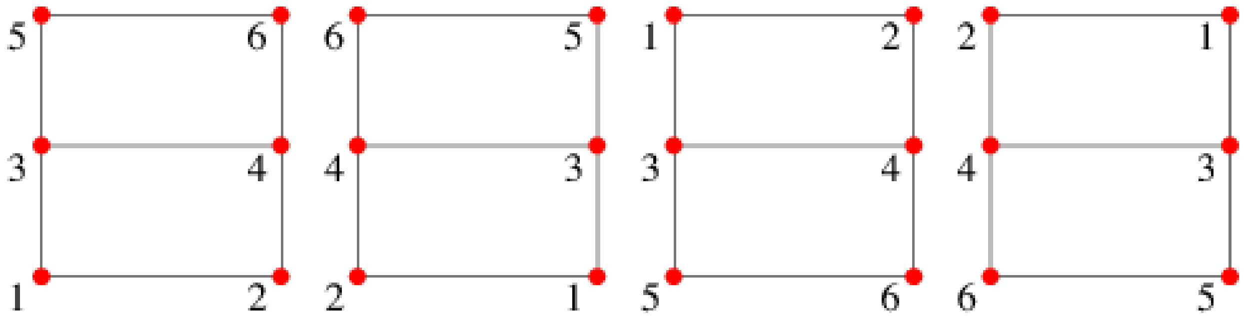
$8 \rightarrow d$



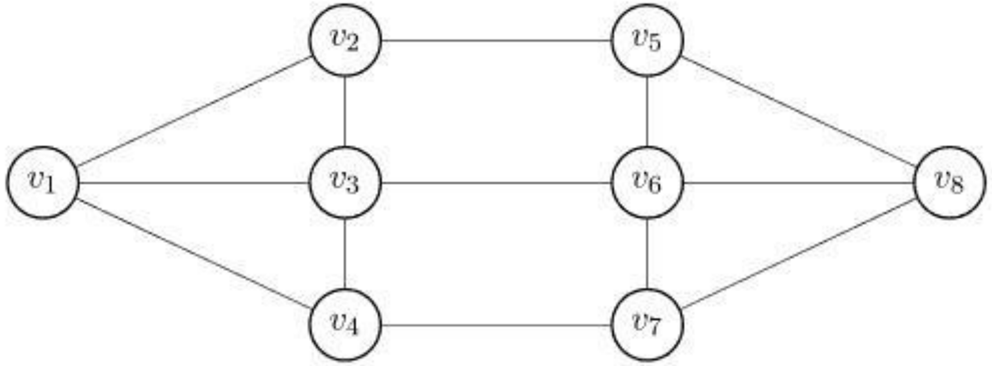
Endomorfismo



Automorfismo



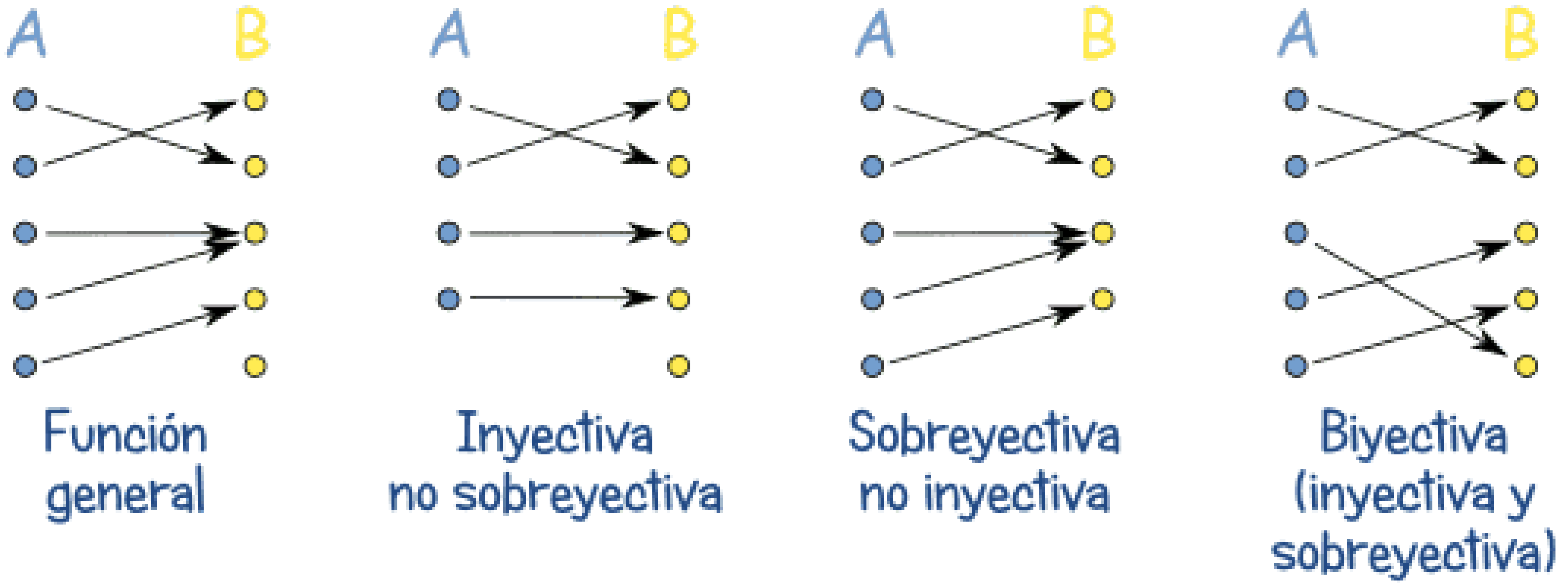
For example, the grid graph $G_{2,3}$ has four automorphisms: (1, 2, 3, 4, 5, 6), (2, 1, 4, 3, 6, 5), (5, 6, 3, 4, 1, 2), and (6, 5, 4, 3, 2, 1). These correspond to the graph itself, the graph flipped left-to-right, the graph flipped up-down, and the graph flipped left-to-right and up-down, respectively, illustrated above. More generally, as is clear from its symmetry,



Clave para entenderlo

An example for a graph with four automorphisms. For instance, ***interchanging vertices 2 and 4 as well as 5 and 7 produces the same drawing****.*

Función sobreyectiva – inyectiva…



Resumen gráfico

$$\begin{tikzcd} C \arrow[r, shift left, "g_1"] \arrow[r, shift right, "g_2"'] & A \arrow[r, "f"] & B \end{tikzcd}$$

(a) Monomorphism

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, shift left, "g_1"] \arrow[r, shift right, "g_2"'] & C \end{tikzcd}$$

(b) Epimorphism

$$\begin{tikzcd} A \arrow[r, "f"] & A \end{tikzcd}$$

(c) Endomorphism

$$\begin{tikzcd} A \arrow[r, shift left, "f"] & B \arrow[l, shift left, "f^{-1}"] \end{tikzcd}$$

(d) Isomorphism

Ejemplo 1.

Sea $h : (I\!R, +) \longrightarrow (I\!R - \{0\}, \cdot)$, se define $h(x) = 3^x$. Vemos que

$$\begin{aligned} h(x+y) &= 3^{x+y}, \\ &= 3^x 3^y, \\ &= h(x)h(y). \end{aligned}$$

Así h es un homomorfismo. Por otro lado, se tiene que

$$\frac{dh(x)}{dx} = ln3 \cdot 3^x > 0, \ \forall x \in I\!R,$$

esto significa que h es creciente estrictamente y por lo tanto inyectiva, así que h es un monomorfismo.

Ejemplo 2

Considerar el grupo de los números reales con la suma $(\mathbb{R}, +, 0)$ y el grupo de los números reales con el producto $(\mathbb{R} - \{0\}, \cdot, 1)$. ¿Es la aplicación $f : (\mathbb{R}, +, 0) \to (\mathbb{R} - \{0\}, \cdot, 1)$, con $f(x) = e^x$, un homomorfismo de grupos? ¿Es un epimorfismo? ¿Es un monomorfismo?

Nota

UNIVERSIDAD FRANCISCO DE VITORIA

- Con estructuras algebraicas, grupos, anillos y homomorfismos se trabajará más en:

  - ***MATEMÁTICAS DISCRETAS***