

TEMA 0: PRELIMINARES

1. CONJUNTOS

Un *conjunto* es una reunión en un todo de determinados objetos bien definidos y diferentes entre sí. A estos distintos objetos se les denominan *elementos*.

Con el fin de evitar contradicciones, se dan una serie de *requisitos* a la hora de definir un conjunto:

- evitar la ambigüedad
- los elementos han de ser distintos
- el propio conjunto no puede ser un elemento

Un ejemplo de contradicción es el siguiente: *sea el conjunto A formado por los conjuntos que se contienen a sí mismos.*

Un conjunto puede definirse de dos formas:

- por *extensión* Ej: $A = \{a, b, c, d\}$
- por *comprensión* Ejs: $A = \{x / x \text{ es primo}\}$
 $A = \{x \in N / x \text{ es primo}\}$

Existe el llamado *conjunto vacío*, que carece de elementos.

$$\emptyset = \{ \}$$

Dos conjuntos son iguales si tienen los mismos elementos.

$$A = B \rightarrow x \in A \Leftrightarrow x \in B$$

A es un subconjunto de B (está incluido en B) si todo elemento de A lo es también de B.

$$A \subseteq B \rightarrow x \in A \Rightarrow x \in B$$

Para todo conjunto A se cumple:

$$\emptyset \subseteq A \quad A \subseteq A$$

Al resto de los subconjuntos de A los llamaremos *subconjuntos propios*.

$$A = B \Leftrightarrow A \subseteq B \text{ y } B \subseteq A$$

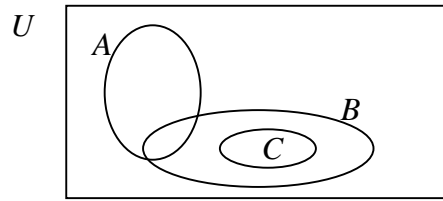
Diremos que A está contenido o incluido *estrictamente* en B si está incluido en B y no es el propio B.

$$A \subset B \Leftrightarrow A \subseteq B \text{ y } A \neq B$$

(con otra notación; $A \subseteq B \Leftrightarrow A \subset B \text{ y } A \neq B$)

Trabajaremos siempre con subconjuntos de un conjunto mayor al que llamaremos *universo* o conjunto universal U.

Para representar conjuntos se utilizan los llamados *diagramas de Venn*:



Dado un conjunto A llamaremos *partes de A* $\wp(A)$ al conjunto formado por todos los subconjuntos de A .

• *Ejemplo:* Sea $A = \{a, b, c, d\}$

$$\wp(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

$$\begin{array}{ll} \left\{ \begin{array}{l} \{a\} \in \wp(A) \\ a \notin \wp(A) \end{array} \right. & \left\{ \begin{array}{l} \{a\} \notin \wp(A) \\ \{\{a\}\} \subseteq \wp(A) \end{array} \right. & \left\{ \begin{array}{l} \emptyset \in \wp(A) \\ \emptyset \notin \wp(A) \end{array} \right. & \left\{ \begin{array}{l} \{\emptyset\} \notin \wp(A) \\ \{\emptyset\} \subseteq \wp(A) \end{array} \right. & \{ \{a, b, c\} \} \subseteq \wp(A) \end{array}$$

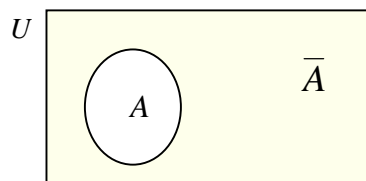
Ejercicio: Escribe un conjunto A tal que $\{\{a, b\}, \{b, c\}\} \subseteq \wp(A)$

2. OPERACIONES CON CONJUNTOS

Sea U el conjunto universal.

Dado $A \subseteq U$, llamamos *complementario de A* al conjunto de los elementos de U que no están en A .

$$\bar{A} = \{x \in U / x \notin A\}$$



Dados los conjuntos A y B ($A, B \subseteq U$), se definen respectivamente la *unión* y la *intersección* como:

$$A \cup B = \{x \in U / x \in A \text{ ó } x \in B\}$$



$$A \cap B = \{x \in U / x \in A \text{ y } x \in B\}$$

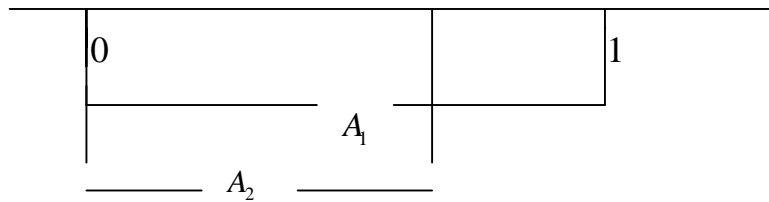


$$\bigcup_{i \in I} A_i = \{x \in U / \exists i \in I \text{ con } x \in A_i\}$$

$$\bigcap_{i \in I} A_i = \{x \in U / \forall i \in I \text{ } x \in A_i\}$$

• Ejemplo: $U = \mathbb{R} \quad A_i = \left[0, \frac{1}{i}\right] \quad i \in \{1, 2, 3, \dots\}$

$$A_1 = [0, 1]; \quad A_2 = [0, 1/2]; \quad A_3 = [0, 1/3] \dots$$



$$\bigcup_{i=1}^{\infty} A_i = [0, 1] = A_1$$

$$\bigcap_{i=1}^{\infty} A_i = \{0\}$$

Dos conjuntos A y B son *disjuntos* si su intersección es el conjunto vacío.

$$A \cap B = \emptyset$$

Ejercicio: Sean $A, B \subseteq U$ tales que $A \cup B = B$, demostrar que $A \cap B = A$.

Propiedades

Doble complementación: $\overline{\overline{A}} = A$

Conmutativa: $A \cup B = B \cup A$
 $A \cap B = B \cap A$

Asociativa: $(A \cup B) \cup C = A \cup (B \cup C)$
 $(A \cap B) \cap C = A \cap (B \cap C)$

Idempotencia: $A \cup A = A$
 $A \cap A = A$

Absorción: $A \cup (A \cap B) = A$
 $A \cap (A \cup B) = A$

Neutralidad:	$A \cup \emptyset = A$
	$U \cap A = A$
Dominación:	$U \cup A = U$
	$\emptyset \cap A = \emptyset$
Inversas:	$A \cup \bar{A} = U$
	$A \cap \bar{A} = \emptyset$
Inversas de Morgan:	$\overline{A \cup B} = \bar{A} \cap \bar{B}$
	$\overline{A \cap B} = \bar{A} \cup \bar{B}$
Distributiva:	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Otras operaciones

Sea U el universo, y $A, B \in U$, se define como *diferencia*:

$$A - B = \{x \in U / x \in A \text{ y } x \notin B\} = A \cap \bar{B}$$

Sea U el universo, y $A, B \in U$, se define como *diferencia simétrica*:

$$A \Delta B = \{x \in U / x \in A \text{ ó } x \in B \text{ pero } x \notin A \cap B\} = (A \cup B) - (A \cap B)$$

- *Ejemplo:*

$$U = N$$

$$A = \{0, 2, 4, 6, 8\}; \quad B = \{0, 3, 6, 9\}$$

$$A \cup B = \{0, 2, 3, 4, 6, 8, 9\}$$

$$A \cap B = \{0, 6\}$$

$$A - B = \{2, 4, 8\}$$

$$A \Delta B = \{2, 3, 4, 8, 9\}$$

Ejercicio: Demostrar, usando las propiedades anteriores, la siguiente igualdad:
 $A \Delta B = (A - B) \cup (B - A)$

Principio de inclusión y exclusión

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| + |A \cap B \cap C|$$

Producto cartesiano

Dados dos conjuntos A y B , llamaremos *par ordenado* a listas del tipo (a,b) , donde $a \in A$ y $b \in B$.

$$(a,b) = (a',b') \Leftrightarrow a = a' \text{ y } b = b'$$

Se define el producto cartesiano $A \times B$ como el conjunto de todos los pares ordenados en A y B .

$$A \times B = \{(a,b) / a \in A \text{ y } b \in B\}$$

Esta definición se puede extender a tres o más conjuntos.

El cardinal del producto cartesiano de dos conjuntos es igual al producto de los cardinales de éstos:

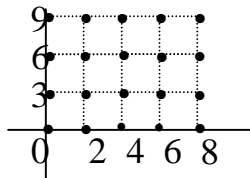
$$|A \times B| = |A| \cdot |B|$$

- *Ejemplo:* (mismos conjuntos que en el anterior)

$$A \times B = \{(0,0), (0,3), (0,6), (0,9), (2,0), \dots \dots (8,6), (8,9)\}$$

En este caso, el resultado no pertenece al universo (ley externa).

Gráficamente:



3. RELACIONES

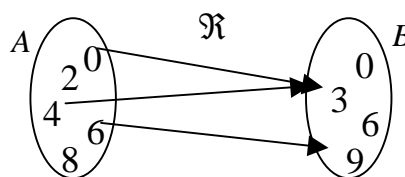
Llamamos *relación* de A en B a un subconjunto, \mathfrak{R} , de $A \times B$.

Si $(a,b) \in \mathfrak{R}$, se suele representar por $a\mathfrak{R}b$. En caso contrario, $a\not\mathfrak{R}b$.

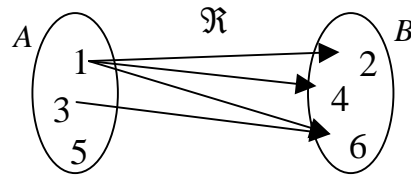
- *Ejemplo:* (mismos conjuntos que en el anterior)

$$\mathfrak{R} = \{(6,9), (0,3), (4,3)\} \quad 6\mathfrak{R}9, \text{etc.}$$

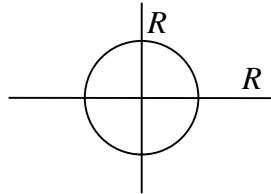
$$\mathfrak{R} = \{(0,3), (0,6), (8,6)\} \quad 0\mathfrak{R}3, \text{etc.}$$



- Ejemplo: $a\mathfrak{R}b$ si a es divisor de b



- Ejemplo: $R \times R$



$\mathfrak{R} = \{(x, y) \mid x^2 + y^2 = 1\} \rightarrow \text{circunferencia}$

$\mathfrak{R} = \{(x, y) \mid x^2 + y^2 \leq 1\} \rightarrow \text{círculo}$

Ejercicio: Si $|A| = n$ y $|B| = m$, calcular el número de relaciones que se pueden definir de A en B .

Dominio: $\text{Dom}(\mathfrak{R}) = \{x \in A \mid \exists b \in B \text{ con } x\mathfrak{R}b\}$

Imagen: $\text{Im}(\mathfrak{R}) = \{x \in B \mid \exists a \in A \text{ con } a\mathfrak{R}x\}$

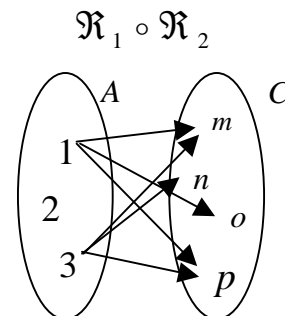
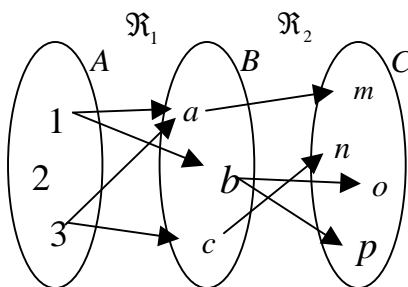
Composición de relaciones y relación inversa

Sean A, B y C conjuntos y $\mathfrak{R}_1 \subseteq A \times B$
 $\mathfrak{R}_2 \subseteq B \times C$

Se define la composición de \mathfrak{R}_1 con \mathfrak{R}_2 como la relación de A en C siguiente:

$$a(\mathfrak{R}_1 \circ \mathfrak{R}_2)c \Leftrightarrow \exists b \in B \text{ con } a\mathfrak{R}_1b \text{ y } b\mathfrak{R}_2c$$

- Ejemplo:



La composición de relaciones tiene propiedad asociativa. No tiene conmutativa, porque no habría ningún conjunto en común en medio.

Dada una relación \mathfrak{R} de A en B , podemos definir una relación \mathfrak{R}^{-1} de B en A , llamada *relación inversa*, como $b\mathfrak{R}^{-1}a \Leftrightarrow a\mathfrak{R}b$.

- *Ejemplo:* (mismos conjuntos que el anterior)

$$\mathfrak{R}^{-1} = \{(9,6), (3,0), (3,4)\}$$

Relaciones binarias

Decimos que una relación es binaria si el conjunto inicial y el final coinciden.

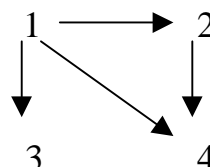
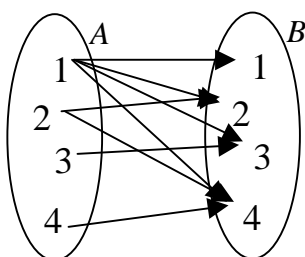
$$\mathfrak{R} \subseteq A \times A$$

- *Ejemplo:*

$$A = \{1,2,3,4\}$$

$$\mathfrak{R} \subseteq A \times A$$

$a\mathfrak{R}b$ si a es divisor de b



Para cada conjunto A se define la relación identidad como:

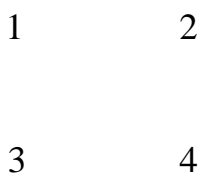
$$a\mathfrak{I}_A b \Leftrightarrow a = b$$

- *Ejemplo:*

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

$$\mathfrak{I}_A = \{(a,a), (b,b), (c,c)\}$$

- *Ejemplo:* (mismo conjunto que el anterior)



Propiedades que pueden presentar las funciones binarias

Reflexiva: $\forall a \in A \quad a \mathcal{R} a$

Antirreflexiva: $\forall a \in A \quad a \not\mathcal{R} a$

Simétrica: $\forall a, b \in A \quad a \mathcal{R} b \Rightarrow b \mathcal{R} a$

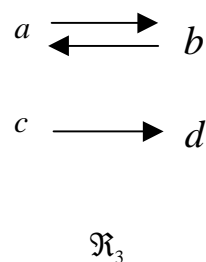
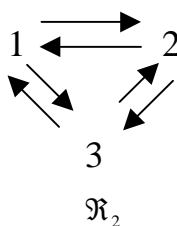
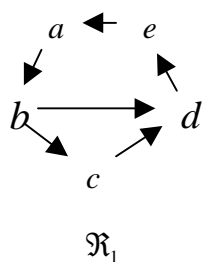
(las reflexivas son también simétricas)

Antisimétrica: $\forall a, b \in A \quad \left. \begin{array}{l} a \mathcal{R} b \\ b \mathcal{R} a \end{array} \right\} \Rightarrow a = b$

(las reflexivas son también antisimétricas)

Transitiva: $\forall a, b, c \in A \quad \left. \begin{array}{l} a \mathcal{R} b \\ b \mathcal{R} c \end{array} \right\} \Rightarrow a \mathcal{R} c$

• Ejemplos:



Reflexiva: \mathcal{R}_3
 Antirreflexiva: ninguna
 Simétrica: \mathcal{R}_2
 Antisimétrica: \mathcal{R}_1
 Transitiva: \mathcal{R}_3

Relaciones de equivalencia. Particiones de conjuntos

Una relación binaria \mathcal{R} en un conjunto A se dice que es *de equivalencia* si es **reflexiva, simétrica y transitiva**.

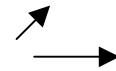
Ejercicio: En \mathbb{Z} se define la relación de congruencia módulo 2 de la siguiente forma: $a \equiv b \pmod{2} \Leftrightarrow b - a$ es múltiplo de 2. Demuestra que es una relación de equivalencia.

$$b - a = 2k \text{ para algún } k \in \mathbb{Z}$$

$$b = a + 2k \text{ para algún } k \in \mathbb{Z}$$

$$a = 0 \quad \dots, -4, -2, 0, 2, 4, 6, 8, \dots \quad [0]$$

$$a = 1 \quad \dots, -3, -1, 1, 2, 3, 4, 5, \dots \quad [1]$$



Dado un conjunto $A \neq \emptyset$, llamaremos *partición de A* a una familia de subconjuntos $\{A_i, i \in I\}$ no vacíos de A , tales que:

- $\bigcup_{i \in I} A_i = A$
- $A_i \cap A_j = \emptyset \quad \forall i, j \in I \text{ con } i \neq j$

• *Ejemplo:*

$$A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$A_i = \{2i, 2i + 1\} \text{ con } i \in \{0, 1, 2, 3, 4\}$$

0	2	4	6	8
1	3	5	7	9

Sea \mathfrak{R} una relación de equivalencia en A y $a \in A$. Llamamos *clase de equivalencia de a*, $[a]$, al subconjunto de todos los elementos relacionados con a .

$$[a] = \{x \in A \mid x \mathfrak{R} a\}$$

Teorema: Sea \mathfrak{R} una relación de equivalencia en A y $a, b \in A$.

- $a \in [a]$ (propiedad reflexiva)
- $a \mathfrak{R} b \Leftrightarrow [a] = [b]$
- Si $[a] \neq [b]$ entonces $[a] \cap [b] = \emptyset$

Corolario: Las clases de equivalencia de una relación \mathfrak{R} en A establecen una partición de A .

Demostración de que $a \mathfrak{R} b \Leftrightarrow [a] = [b]$

- $a \mathfrak{R} b \Rightarrow [a] = [b]$

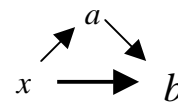
Partimos de: $a \mathfrak{R} b$.

Queremos demostrar: $x \in [a] \Leftrightarrow x \in [b]$

$$x \in [a] \Leftrightarrow x \mathfrak{R} a \text{ (definición de clase de } a)$$

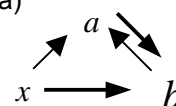
$$x \in [a] \Leftrightarrow x \mathfrak{R} a \Rightarrow x \mathfrak{R} b \text{ (propiedad transitiva)}$$

$$x \in [a] \Leftrightarrow x \mathfrak{R} a \Rightarrow x \mathfrak{R} b \Leftrightarrow x \in [b]$$



$x \in [b] \Leftrightarrow x \mathcal{R} b \Rightarrow x \mathcal{R} a$ (propiedad simétrica y transitiva)

$x \in [b] \Leftrightarrow x \mathcal{R} b \Rightarrow x \mathcal{R} a \Leftrightarrow x \in [a]$



- $[a] = [b] \Rightarrow a \mathcal{R} b$

Partimos de: $[a] = [b]$

Queremos demostrar: $a \mathcal{R} b$

$a \in [a] \Rightarrow a \in [b]$ (primera de las propiedades del teorema)

$a \in [a] \Rightarrow a \in [b] \Rightarrow a \mathcal{R} b$ (definición de clase de b)

Ejercicio: Demostrar la tercera propiedad del teorema.

- *Ejemplo:* Para la relación de congruencia módulo 2 en \mathbb{Z} , las clases forman los pares por un lado y los impares por otro.

Dada una relación de equivalencia \mathcal{R} en un conjunto A , se llama *conjunto cociente de A con la relación \mathcal{R}* , y se representa A/\mathcal{R} , al conjunto formado por las clases de equivalencia.

- *Ejemplo:*

$$\mathbb{Z}/\equiv (\text{mod}.2) = \{[0], [1]\} = \{[2], [3]\} = \dots$$

$$\mathbb{Z}/\equiv (\text{mod}.2) = \mathbb{Z}_2$$

Ejercicio: Escribir las diferentes clases de equivalencia que definen la relación congruencia módulo 5 en los enteros, y el conjunto \mathbb{Z}_5 .

Relaciones de orden

Una relación \mathcal{R} en un conjunto A : $\mathcal{R} \subseteq A \times A$.

Se dice que es una relación de orden si es **reflexiva**, **antisimétrica** y **transitiva**.

- *Ejemplo:*

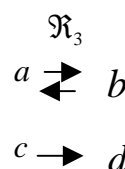
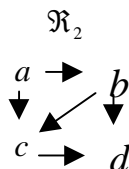
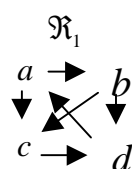
$$A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$a \mathcal{R} b \Leftrightarrow a \text{ divide a } b$$

Sea A un conjunto, \mathcal{R} una relación de orden en A , y $a, b \in A$, decimos que a y b son *comparables* si $a \mathcal{R} b$ o $b \mathcal{R} a$.

Se dice que \mathfrak{R} es una relación de *orden total* si todos los elementos de A son comparables entre sí. En caso contrario se dice que \mathfrak{R} es una relación de *orden parcial*.

- Ejemplo: $A = \{a, b, c, d\}$



Relación de orden total: \mathfrak{R}_1
 Relación de orden parcial: \mathfrak{R}_2
 No es relación de orden: \mathfrak{R}_3 (es simétrica)

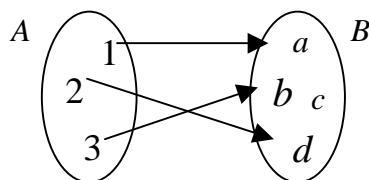
4. FUNCIONES

Sean A y B dos conjuntos y $f \subseteq A \times B$. Decimos que f es una función o aplicación si:

- $\text{Dom}(f) = A$
- Si $(a, b) \in f$ y $(a, c) \in f$ entonces $b = c$.

(todo elemento del conjunto original tiene imagen, y esta imagen es única)

- Ejemplos:



$$f : \mathbb{R} \rightarrow \mathbb{R}$$

$$f(x) = 2x + 1$$

Al conjunto A lo llamaremos *conjunto inicial* y al conjunto B conjunto final.

Si $(a, b) \in f$, diremos que b es imagen de a o que a es origen de b y lo denotaremos por $f(a) = b$.

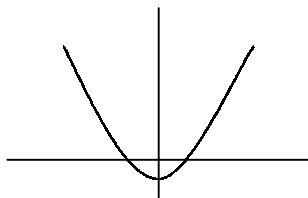
Para expresar que f es una función de A en B , en vez de $f \subseteq A \times B$, escribiremos $f: A \rightarrow B$.

- Ejemplo:

$$f: \mathbb{R} \rightarrow \mathbb{R}$$

$$f(x) = x^2 - 1$$

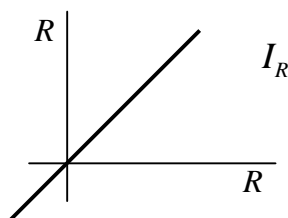
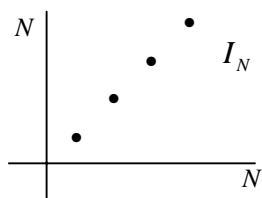
$$f = \{(x, x^2 - 1) \mid x \in \mathbb{R}\} = \{(x, y) \mid x \in \mathbb{R}, y = x^2 - 1\}$$



• *Ejemplo:*

La relación de identidad en un conjunto A es una función: $I_A = A \rightarrow A$, $f(x) = x$

Las representaciones de I_N y de I_R son:



Dada una función $f: A \rightarrow B$ podemos relacionar subconjuntos de A con subconjuntos de B de la siguiente forma:

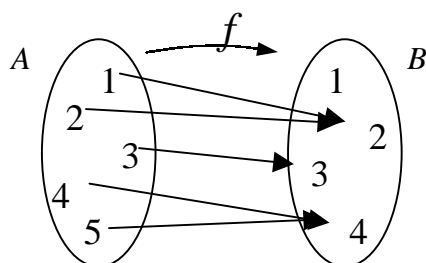
- Sea $X \subseteq A$, llamamos *imagen de X* al conjunto:

$$f(X) = \{y \in B \mid \exists x \in X \text{ con } f(x) = y\} = \{f(x) \mid x \in X\}$$

- Sea $Y \subseteq B$, llamamos *imagen inversa o preimagen de Y* al siguiente conjunto:

$$f^{-1}(Y) = \{x \in A \mid f(x) \in Y\}$$

• *Ejemplo:*



$$f(\{1, 2, 3, 4\}) = \{2, 3\}$$

$$f^{-1}(\{1, 3\}) = \{3\}$$

Ejercicio: Dada la función $f: R \rightarrow R$, $f(x) = \sin x$, calcular la preimagen del intervalo $(0,1)$ y la imagen del intervalo $[3\pi/2, 2\pi]$.

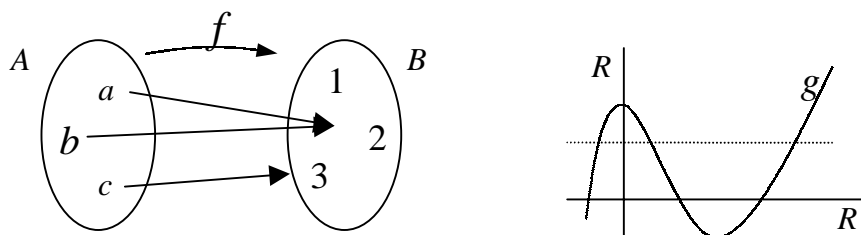
Tipos especiales de funciones

Una función $f: A \rightarrow B$ se dice **inyectiva** si:

$$\forall x, x' \in A \quad x \neq x' \quad \text{se tiene} \quad f(x) \neq f(x')$$

$$(\text{si } f(x) = f(x') \text{ entonces } x = x')$$

- *Ejemplo:*



No son inyectivas ni f ni g .

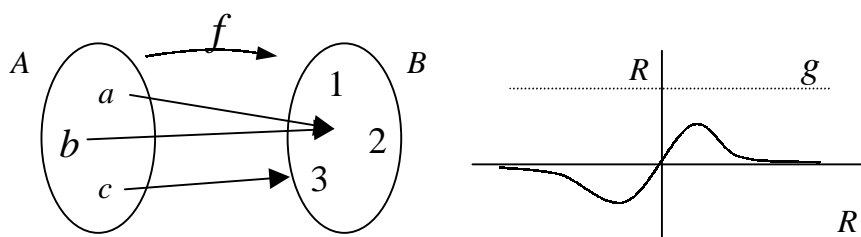
$$h: \mathbb{Z} - \{1\} \rightarrow \mathbb{Q}$$

$$h(x) = \frac{x}{x-1} \quad (\text{sí es inyectiva})$$

$$h(x) = h(x') \Rightarrow \frac{x}{x-1} = \frac{x'}{x'-1} \Rightarrow x = x'$$

Una función $f: A \rightarrow B$ es **sobreyectiva** si: $\text{Im}(f) = B$

- *Ejemplos:*



No son sobreyectivas ni f ni g .

$$h: \mathbb{R} \rightarrow \mathbb{R}$$

$$h(x) = 1 + 2x \quad (\text{sí es sobreyectiva})$$

Una función $f: A \rightarrow B$ es **biyectiva** si es inyectiva y sobreyectiva.

Ejercicio: Condiciones que han de cumplir dos conjuntos para poder definir funciones biyectivas entre ellos.

Composición de funciones. Función inversa

Dadas dos funciones $f: A \rightarrow B$ y $g: B \rightarrow C$, se define f compuesto con g como:

$$g \circ f: A \rightarrow C \quad (g \circ f)(x) = g(f(x))$$

En conjuntos:

$$\mathfrak{R}_1 \subseteq A \times B$$

$$\mathfrak{R}_2 \subseteq B \times C$$

$$\mathfrak{R}_1 \circ \mathfrak{R}_2 \subseteq A \times C$$

$$a(\mathfrak{R}_1 \circ \mathfrak{R}_2)c \Leftrightarrow \exists b \in B / a\mathfrak{R}_1b \text{ y } b\mathfrak{R}_2c$$

En funciones:

$$f: A \rightarrow B$$

$$g: B \rightarrow C$$

$$g \circ f: A \rightarrow C$$

$$(g \circ f)(a) = c \Leftrightarrow \exists b \in B / f(a) = b \text{ y } g(b) = c$$

$$\Leftrightarrow g(f(a)) = c$$

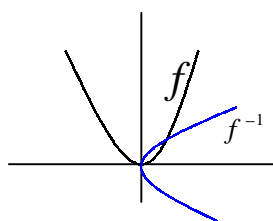
Diremos que una función $f: A \rightarrow B$ es *invertible* si la relación inversa $f^{-1}: B \rightarrow A$ es una función.

Teorema: Una función $f: A \rightarrow B$ es invertible si, y sólo si, la función es biyectiva.

• *Ejemplos:*

$$f: \mathbb{R} \rightarrow \mathbb{R}$$

$$f(x) = x^2$$

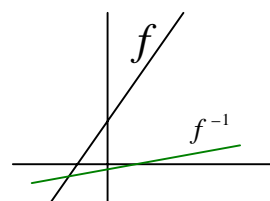


No es invertible

$$f: \mathbb{R} \rightarrow \mathbb{R}$$

$$f(x) = 2x + 1$$

$$f^{-1}(x) = \frac{x-1}{2}$$



Sí es invertible

Teorema: Sea $f: A \rightarrow B$ una función invertible, entonces:

$$f \circ f^{-1} = I_B \quad \text{y} \quad f^{-1} \circ f = I_A$$

Y, además, f^{-1} es la única función que cumple estas condiciones para f .

5. LEYES DE COMPOSICIÓN

Dado un conjunto A , llamamos *operación binaria interna* o *ley de composición interna* a cualquier función de $A \times A$ en A .

$$*: A \times A \rightarrow A$$

$$*(a, b) = c \quad a * b = c$$

• *Ejemplos:*

$*: Z \times Z \rightarrow Z \quad a * b = a + b - ab$ es una ley de composición interna.

$\Delta: Z \times Z \rightarrow Z \quad a \Delta b = \sqrt{a^2 + b^2}$ no es una ley de composición interna.

$$A = \{a, b, c\} \quad \begin{array}{c|ccc} \square & a & b & c \\ \hline a & a & b & c \\ b & b & a & b \\ c & c & b & a \end{array} \quad \text{es una ley de composición interna.}$$

Dado un conjunto A , $X \subseteq A$ y $*$ una ley de composición interna en A . Decimos que X es *parte estable de A respecto $*$* si $*$ es ley de composición interna en X .

• *Ejemplo:*

$X = \{a, b\}$ es parte estable de A respecto \square (del ejemplo anterior).

Dados dos conjuntos A y B llamaremos *ley de composición externa en A* a cualquier función del tipo $*: A \times B \rightarrow A$.

Propiedades

Asociativa: Sea $*$ una ley de composición interna en un conjunto A . Decimos que $*$ tiene propiedad asociativa si:

$$\forall x, y, z \in A \quad x * (y * z) = (x * y) * z$$

Proposición: Sea $*$ una ley de composición interna en A , con propiedad asociativa, y $X \subseteq A$. Si X es parte estable de A respecto $*$, entonces $*$ tiene propiedad asociativa en X .

Conmutativa: Sea $*$ una ley de composición interna en un conjunto A . Decimos que $*$ tiene propiedad conmutativa si:

$$\forall x, y \in A \quad x * y = y * x$$

Proposición: Sea $*$ una ley de composición interna en A , con propiedad conmutativa y $X \subseteq A$. Si X es parte estable de A respecto $*$, entonces $*$ tiene propiedad asociativa en X .

• *Ejemplo:*

$A = \{0,1,2,3\}$	\triangle	0	1	2	3
	0	0	1	2	3
	1	1	2	3	0
	2	2	3	0	1
	3	3	0	1	2

\triangle tiene propiedad conmutativa.
 $\{0,2\}$ es parte estable de A .

\triangle en $\{0,2\}$ tiene también	\triangle	0	2
propiedad conmutativa.	0	0	2
	2	2	0

Dada una ley de composición interna en un conjunto A , un elemento $c \in A$ se dice *central* si:

$$\forall x \in A \quad x * c = c * x$$

Llamamos *centro* al conjunto de todos los elementos centrales.

Distributiva: Sean $*$ y Δ dos leyes de composición interna en un conjunto A .

Δ es distributiva por la izquierda respecto de $*$ si:

$$\forall x, y, z \in A \quad x \Delta (y * z) = (x \Delta y) * (x \Delta z)$$

Δ es distributiva por la derecha respecto de $*$ si:

$$\forall x, y, z \in A \quad (y * z) \Delta x = (y \Delta x) * (z \Delta x)$$

Δ es distributiva respecto de $*$ si lo es por la izquierda y por la derecha.

Elementos particulares

Elemento neutro: Un elemento $e \in A$ es neutro para $*$ si:

$$\forall x \in A \quad x * e = e * x = x$$

Proposición: El elemento neutro, si existe, es único.

Demostración: Suponiendo que hay dos elementos neutros: e y e'

$$\left. \begin{array}{l} e * e' = e' \\ e' * e = e \end{array} \right\} \Rightarrow e * e' = e' * e \rightarrow e = e'$$

Simétrico de un elemento: Sea e el elemento neutro para una ley de composición interna $*$ en un conjunto A .

Dado $x \in A$, $x' \in A$ es el simétrico de x si:

$$x * x' = x' * x = e$$

Si un elemento $x \in A$ tiene simétrico se dice que es *simetrizable*.

• *Ejemplos:*

$$(Z, +) \quad a = 2; a' = -2 \qquad (Z, \cdot) \quad a = 2; a' = \text{no hay}$$

Proposición: El simétrico del simétrico de un elemento es el mismo elemento: $(a')' = a$.

Proposición: Si $*$ tiene propiedad asociativa en A y $a \in A$ es simetrizable, su simétrico es único.

Demostración: Suponiendo que hay dos simétricos: a' y a''

$$\left. \begin{array}{l} a'' * a * a' = a'' * (a * a') = a'' * e = a'' \\ a'' * a * a' = (a'' * a) * a' = e * a' = a' \end{array} \right\} \Rightarrow a' = a''$$

Proposición: Si $*$ es asociativa en A , tiene elemento neutro y $a \in A$ es simetrizable, las siguientes ecuaciones tienen solución única:

$$a * x = b$$

$$x * a = b$$

Demostración:

$$\left. \begin{array}{l} a * x = b \rightarrow (a' * a) * x = a' * b \rightarrow e * x = a' * b \rightarrow x = a' * b \\ x * a = b \rightarrow x * (a * a') = b * a' \rightarrow x * e = b * a' \rightarrow x = b * a' \end{array} \right\} \Rightarrow a' * b = b * a'$$

Proposición: Si $*$ es asociativa y a y b son simetrizables entonces $a * b$ también lo es y:

$$(a * b)' = b' * a'$$

Demostración:

$$(a * b) * (b' * a') = a * (b * b') * a' = a * e * a' = a * a' = e$$

Elementos simplificables o regulares: Sea $*$ una ley de composición interna en un conjunto A .

$c \in A$ es regular por la derecha si:

$$a * c = b * c \Rightarrow a = b$$

$c \in A$ es regular por la izquierda si:

$$c * a = c * b \Rightarrow a = b$$

$c \in A$ es *regular* si lo es por la izquierda y por la derecha.

Si todos los elementos de A son regulares, se dice que $*$ satisface la *ley de simplificación*.

Proposición: Si $*$ es asociativa, todo elemento simetrizable es regular.

Ejercicio: Buscar un ejemplo con elementos no simetrizables.

Elemento absorbente: Sea $*$ una ley de composición interna en A , y sea $c \in A$.

c es *absorbente* si $\forall a \in A, a * c = c * a = c$

Elemento idempotente: Sea $*$ una ley de composición interna en A , y sea $a \in A$.

a es *idempotente* si $a * a = a$

Si todos los elementos de A son idempotentes diremos que A con $*$ es idempotente.

6. ESTRUCTURAS ALGEBRAICAS

$(A, *)$ es **semigrupo** si:

$*$ es **ley de composición interna** en A

Cumple la **propiedad asociativa**

Opcionales:

Propiedad conmutativa (semigrupo *Abeliano*)

Elemento neutro (con *elemento neutro*)

$(A, *)$ es **grupo** si:

$*$ es **ley de composición interna** en A

Cumple la **propiedad asociativa**

Posee **elemento neutro**

Todos los elementos son **simetrizables**

Opcional:

Propiedad conmutativa (*Abeliano*)

$(A, *, \Delta)$ es **semianillo** si:

$*$ es ley de composición interna en A	Δ es ley de composición interna en A
Cumple la propiedad asociativa	Cumple la propiedad asociativa
Cumple la propiedad conmutativa	Propiedad conmutativa (opcional, <i>Abeliano</i>)
Posee elemento neutro	Elemento neutro (opcional, <i>con elemento unidad</i>)

Cumple que Δ es **distributiva** respecto $*$

$(A, *, \Delta)$ es **anillo** si:

$*$ es ley de composición interna en A	Δ es ley de composición interna en A
Cumple la propiedad asociativa	Cumple la propiedad asociativa
Cumple la propiedad conmutativa	Propiedad conmutativa (opcional, <i>Abeliano</i>)
Posee elemento neutro	Elemento neutro (opcional, <i>con elemento unidad</i>)
Todos los elementos son simetrizables	

Cumple que Δ es **distributiva** respecto $*$

$(A, *, \Delta)$ es **cuerpo** si:

$*$ es ley de composición interna en A	Δ es ley de composición interna en A
Cumple la propiedad asociativa	Cumple la propiedad asociativa
Cumple la propiedad conmutativa	Posee elemento neutro
Posee elemento neutro	Todos sus elementos son simetrizables (menos el 0)
Todos los elementos son simetrizables	Propiedad conmutativa (opcional, <i>Abeliano</i>)

Cumple que Δ es **distributiva** respecto $*$

• **Ejemplos:**

Dado el conjunto $Z_4 = \{[0], [1], [2], [3]\}$, llamado convergencia en módulo cuatro, y formado por las siguientes clases:

$[0] = \{\dots, -4, 0, 4, 8, 12, \dots\}$	Se define una operación como:	+	[0]	[1]	[2]	[3]
$[1] = \{\dots, -3, 1, 5, 9, \dots\}$		[0]	[0]	[1]	[2]	[3]
$[2] = \{\dots, -2, 2, 6, 10, \dots\}$		[1]	[1]	[2]	[3]	[0]
$[3] = \{\dots, -1, 3, 7, 11, \dots\}$		[2]	[2]	[3]	[0]	[1]
		[3]	[3]	[0]	[1]	[2]

- Es una ley de composición interna (todos los elementos pertenecen al conjunto original)
- Tiene propiedad asociativa (por ser la suma la operación)
- Tiene propiedad conmutativa (puede verse a ambos lados de la diagonal principal)
- Tiene elemento neutro (la clase del cero, $[0]$)
- Cada elemento tiene simétrico (si en todas las columnas y filas aparece el elemento neutro, en este caso, la clase del cero).

Por lo tanto, se trata de un **grupo abeliano**.

Dado el conjunto formado por las siguientes permutaciones:

$$S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\} \quad |S_3| = 3! = 6$$

Se define la operación de composición como:

\circ	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_2	μ_3	μ_1
ρ_2	ρ_2	ρ_0	ρ_1	μ_3	μ_1	μ_2
μ_1	μ_1	μ_3	μ_2	ρ_0	ρ_2	ρ_1
μ_2	μ_2	μ_1	μ_3	ρ_1	ρ_0	ρ_2
μ_3	μ_3	μ_2	μ_1	ρ_2	ρ_1	ρ_0

- Es una ley de composición interna (todos los elementos pertenecen al conjunto)
- Tiene propiedad asociativa (definida con la composición de conjuntos)
- No es conmutativa (puede verse en la diagonal principal)
- Tiene elemento neutro (la permutación ρ_0)
- Es simetrizable (esta permutación aparece en todas las filas y columnas).

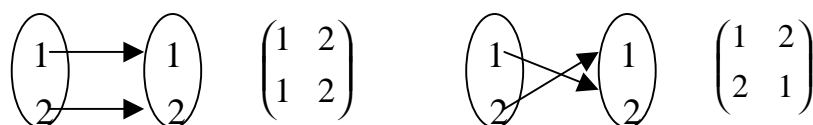
Por lo tanto, se trata de un **grupo**.

Nota sobre las permutaciones

Las permutaciones se definen como funciones biyectivas de un conjunto sobre sí mismo. En la práctica representan las distintas ordenaciones posibles entre dos conjuntos iguales.

- *Ejemplos:*

Dado el conjunto $\{1,2\}$, hay dos permutaciones posibles:



En el ejemplo del apartado anterior, las permutaciones resultantes serían:

$$\begin{aligned} \rho_0 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & \rho_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} & \rho_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \\ \mu_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & \mu_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} & \mu_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \end{aligned}$$

Propiedades de los grupos

Si $(G, *)$ es un grupo:

1. El elemento neutro es único.
2. Cualquier elemento tiene un único simétrico,
3. $(a * b)' = b' * a'$
4. Todos los elementos son regulares (se pueden simplificar).
5. Las ecuaciones $a * x = b$ y $x * a = b$ tienen solución única.

Dado un grupo $(G, *)$ y $H \subseteq G$, se dice que H es un **subgrupo** de G si $(H, *)$ es también grupo. Para ello, ha de cumplir:

- H ha de ser **parte estable** de G ①
 $\forall x, y \in H \quad x * y \in H$
- $*$ debe cumplir la **propiedad asociativa**
 (no hace falta demostrarla)
- Ha de poseer **elemento neutro** ②
 $e \in H$
- Todo elemento ha de ser **simetrizable** ③
 $\forall a \in H \quad a' \in H$

Teorema (de caracterización): Sea $(G, *)$ un grupo y $H \subseteq G$. H es subgrupo de G si $(H, *)$ es también grupo. Se ha de cumplir que:

- i) $H \neq \emptyset$
- ii) $\forall x, y \in H \quad x * y' \in H$

Demostración (aplicando las propiedades anteriores y el teorema) de lo siguiente:

$$H \text{ es subgrupo} \Leftrightarrow H \neq \emptyset \text{ y } \forall x, y \in H \quad x * y' \in H$$

La demostración \Rightarrow es la más sencilla. Usarla como **Ejercicio**.

Para demostrar \Leftarrow :

$$\begin{array}{c} \exists a \in H \Rightarrow a * a' \in H \Rightarrow e \in H \quad ② \\ \text{i)} \quad \text{ii} \\ \quad \quad \quad \setminus \end{array}$$

$$\text{Si } a \in H \Rightarrow a' \in H$$

$$\left. \begin{array}{l} a \in H \\ e \in H \end{array} \right\} \Rightarrow e * a' \in H \Rightarrow a' \in H \quad ③$$

$$\left. \begin{array}{l} x \in H \\ y \in H \end{array} \right\} \quad \left. \begin{array}{l} x \in H \\ y' \in H \end{array} \right\} \xrightarrow[\text{ii}]{\text{③}} x * (y')' \in H \Rightarrow x * y \in H \quad ①$$

Observación: Para cualquier grupo $(G, *)$, $\{e\}$ y G son subgrupos que llamaremos **impropios**. A los demás los llamaremos subgrupos **propios**.

Si $(G, *)$ es un grupo finito, llamamos **orden del grupo** al número de elementos que tiene G .

Teorema de Lagrange: Sea $(G, *)$ un grupo finito de orden n . Si H es un subgrupo de G de orden m , entonces m debe ser un divisor de n .

Ejercicio: Encontrar todos los subgrupos de $(Z_6, +)$.

Subgrupos normales: Dado un grupo $(G, *)$ y un subgrupo de éste H , se dice que H es **subgrupo normal** si:

$$\forall a \in G \quad a * H = H * a$$

donde
$$\begin{cases} a * H = \{a * h / h \in H\} \\ H * a = \{h * a / h \in H\} \end{cases}$$

Teorema (de caracterización): Dado un subgrupo H de $(G, *)$

$$H \text{ es subgrupo normal} \Leftrightarrow \begin{cases} \forall a \in G \\ \forall h \in H \end{cases} a * h * a' \in H$$

- *Ejemplo:* (usando el mismo ejemplo de las permutaciones de tres elementos)

$$\text{Sea } H = \{\rho_0, \rho_1, \rho_2\}$$

$$\begin{array}{ll} \rho_0 \circ H = \{\rho_0, \rho_1, \rho_2\} & = H \circ \rho_0 = \{\rho_0, \rho_1, \rho_2\} \\ \dots & \dots \\ \dots & \dots \\ \mu_1 \circ H = \{\mu_1, \mu_3, \mu_2\} & = H \circ \mu_1 = \{\mu_1, \mu_2, \mu_3\} \\ \dots & \dots \\ \dots & \dots \end{array}$$

Por lo tanto, es un **subgrupo normal**.

Si un grupo es conmutativo, todos sus subgrupos serán normales.
Si un subgrupo es normal, el grupo no tiene por qué ser conmutativo.

Ejercicio: Según el ejemplo anterior, dado el conjunto $H = \{\rho_0, \mu_1\}$, comprobar si es un subgrupo de G y, si lo es, si es un subgrupo normal.

Propiedades de los anillos

$(A, *, \Delta)$ es anillo si:

1. $(A, *)$ es **grupo abeliano**
2. (A, Δ) es **semigrupo** (y cumple, por tanto, la propiedad asociativa)
3. Δ es **distributiva** respecto $*$

Para hablar de los anillos se empleará una **notación y terminología** determinada, para poder diferenciar los elementos neutros, simétricos, etc. de ambos conjuntos.

Notación aditiva			Notación multiplicativa		
$*$	$+$		Δ	\cdot	
e_*	0	"cero"	e_Δ	1	"uno", "unidad"
a'	$-a$	"opuesto"	a'	$a^{-1}, \frac{1}{a}$	"inverso"
$a \overset{n}{*} \dots * a$	$n \cdot a$	$(n \in \mathbb{N})$	$a \overset{n}{\Delta} \dots \Delta a$	a^n	$(n \in \mathbb{N})$

Esta notación no significa que las operaciones que se vayan a utilizar sean únicamente la suma y la multiplicación, sino que se simbolizarán de esta forma.

Por ello, la siguiente igualdad no siempre es cierta: $(a+b)^2 = a^2 + b^2 + 2ab$. Sólo lo es en el caso de tratarse de anillos conmutativos:

$$\begin{aligned} (a+b)^2 &= (a+b) \cdot (a+b) = [a \cdot (a+b)] + [b \cdot (a+b)] = (a \cdot a + a \cdot b) + (b \cdot a + b \cdot b) = \\ &= a \cdot a + a \cdot b + b \cdot a + b \cdot b = a^2 + a \cdot b + b \cdot a + b^2 \neq a^2 + b^2 + 2ab \end{aligned}$$

• *Ejemplos:*

$$Z_5 = \{[0], [1], [2], [3], [4]\}$$

$+$	[0]	[1]	[2]	[3]	[4]	\cdot	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[1]	[2]	[3]	[4]	[0]	[1]	[0]	[1]	[2]	[3]	[4]
[2]	[2]	[3]	[4]	[0]	[1]	[2]	[0]	[2]	[4]	[1]	[3]
[3]	[3]	[4]	[0]	[1]	[2]	[3]	[0]	[3]	[1]	[4]	[2]
[4]	[4]	[0]	[1]	[2]	[3]	[4]	[0]	[4]	[3]	[2]	[1]

$(Z_5, +, \cdot)$ es un anillo abeliano con elemento unidad, y por lo tanto, es un cuerpo abeliano. En la segunda tabla, se ignora la columna y fila del cero para establecer si es o no simetrizable.

$$Z_6 = \{[0], [1], [2], [3], [4], [5]\}$$

+	[0]	[1]	[2]	[3]	[4]	[5]	·	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[1]	[2]	[3]	[4]	[5]	[0]	[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[2]	[3]	[4]	[5]	[0]	[1]	[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[3]	[4]	[5]	[0]	[1]	[2]	[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[4]	[5]	[0]	[1]	[2]	[3]	[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[5]	[0]	[1]	[2]	[3]	[4]	[5]	[0]	[5]	[4]	[3]	[2]	[1]

No es cuerpo (no es simetrizable) pero sí anillo conmutativo con elemento unidad.

Teorema (regla de los signos). Sea $(A, +, \cdot)$ un anillo. $\forall a, b \in A$

- i) $0 \cdot a = a \cdot 0 = 0$
- ii) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
- iii) $a \cdot b = (-a) \cdot (-b)$

Demostración de i):

$$0 + 0 = 0$$

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

(se demuestra de forma análoga para $0 \cdot a = 0$)

Anillo de integridad: Dado $(A, +, \cdot)$ un anillo. Un elemento $a \in A$ ($a \neq 0$) se dice que es **divisor de cero** si:

$$\exists b \in A \ (b \neq 0) / a \cdot b = 0 \text{ ó } b \cdot a = 0$$

Si en un anillo no hay divisores de 0 diremos que es un anillo de integridad. Si además tiene elemento unidad y es abeliano, diremos que es un **dominio de integridad**.

Proposición: Sea $(A, +, \cdot)$ un anillo y $a \in A$.

$$a \text{ es simplificable} \Leftrightarrow a \text{ no es } 0 \text{ ni divisor de } 0$$

Corolario: Si $(A, +, \cdot)$ es un anillo de integridad, todos los elementos son simplificables salvo el 0.

Subanillos: Dado un anillo $(A, +, \cdot)$ y un subconjunto $B \subseteq A$. B es un subanillo de A si $(B, +, \cdot)$ es un anillo.

$$\Leftrightarrow \begin{cases} (B,+) \text{ es subgrupo de } (A,+) \\ (B,\cdot) \text{ es parte estable de } (A,\cdot) \end{cases}$$

$$\Leftrightarrow \{B \neq \emptyset, \quad \forall a,b \in B \quad a+(-b) \in B \quad \text{y} \quad a \cdot b \in B\}$$

$\{0\}$ y A son subanillos impropios de $(A,+,\cdot)$.

Ideales: Dado un anillo $(A,+,\cdot)$ se dice que un subconjunto $I \subseteq A$ no vacío es un ideal del anillo si satisface:

- Si $i, j \in I$ entonces $i + (-j) \in I$
- Si $i \in I$ y $a \in A$ entonces $i \cdot a \in I$
 $a \cdot i \in I$

Si I es un ideal de $(A,+,\cdot)$, entonces es un subanillo de $(A,+,\cdot)$.

- *Ejemplo:* $\{[0],[2]\}$ es un ideal de $(Z_4,+,\cdot)$ (ver un ejemplo anterior)

Propiedades de los cuerpos

$(K,+,\cdot)$ es un cuerpo si:

- $(K,+)$ es un grupo abeliano
- $(K - \{0\}, \cdot)$ es un grupo (no es obligatorio que sea abeliano)
- \cdot es distributiva respecto $+$.

1. Todo cuerpo abeliano es **dominio de integridad**.
2. Todo dominio de integridad finito es cuerpo.

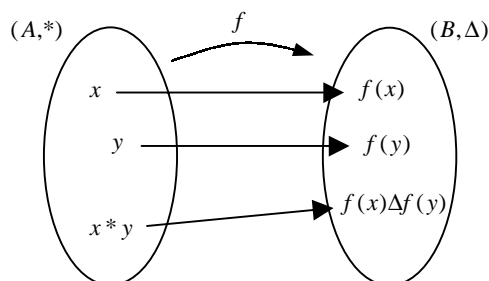
Ejercicio: Justificar por qué $(Z_n,+,\cdot)$ es cuerpo $\Leftrightarrow n$ es primo.

3. Los únicos **ideales** de un cuerpo $(K,+,\cdot)$ son $\{0\}$ y K .
4. En un cuerpo K , la **ecuación** $a = bx$ ($b \neq 0$) tiene solución única.

4. HOMOMORFISMOS

Sean A y B dos conjuntos y $*$ y Δ leyes de composición interna en ellos, respectivamente. Una función $f: A \rightarrow B$ se dice *homomorfismo* si:

$$\forall x, y \in A \quad f(x * y) = f(x) \Delta f(y)$$



• *Ejemplo:*

Sea $A = (0, \infty)$, y consideramos (A, \cdot) y $(\mathbb{R}, +)$. La función $f: A \rightarrow \mathbb{R} \quad f(x) = \log x$ es un homomorfismo.

$$\begin{aligned} f(x) &= \log x \\ f(y) &= \log y \end{aligned} \qquad f(x \cdot y) = \log(x \cdot y) = \log x + \log y$$

Composición de homomorfismos

Consideramos los conjuntos con sus leyes de composición interna:

$$(A, *) \qquad (B, \Delta) \qquad (C, \perp)$$

Si $f: A \rightarrow B$ y $g: B \rightarrow C$ son homomorfismos, entonces $(g \circ f): A \rightarrow C$ es un homomorfismo.

$$\begin{aligned} f: A \rightarrow B \quad f(x * y) &= f(x) \Delta f(y) \quad \forall x, y \in A \\ g: B \rightarrow C \quad g(x \Delta y) &= g(x) \perp g(y) \quad \forall x, y \in B \end{aligned}$$

$$\begin{aligned} g \circ f: A \rightarrow C \quad \forall x, y \in A \quad (g \circ f)(x * y) &= g(f(x * y)) = g(f(x) \Delta f(y)) = \\ &= g(f(x)) \perp g(f(y)) = (g \circ f)(x) \perp (g \circ f)(y) \end{aligned}$$

Imagen de un homomorfismo

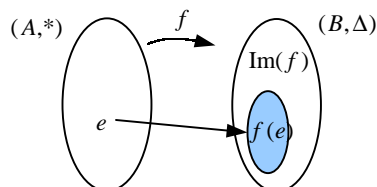
Sean $(A, *)$ y (B, Δ) dos estructuras y $f: A \rightarrow B$ un homomorfismo. El conjunto $\text{Im}(f) \subseteq B$ es parte estable de (B, Δ) .

$$\begin{aligned} \text{Im}(f) \text{ es parte estable} &\Rightarrow \forall x, y \in \text{Im}(f) \rightarrow \exists a, b \in A \quad \begin{aligned} f(a) &= x \\ f(b) &= y \end{aligned} \\ f(a) \Delta f(b) &= f(a * b) \Rightarrow x \Delta y \in \text{Im}(f) \end{aligned}$$

Propiedades del conjunto imagen

Sea $f: A \rightarrow B$ un homomorfismo de $(A, *)$ en (B, Δ) .

1. Si $*$ es **asociativa** en A , entonces Δ es asociativa en $\text{Im}(f)$.
2. Si $*$ es **conmutativa** en A , entonces Δ es conmutativa en $\text{Im}(f)$.
3. Si e es el **elemento neutro** de $*$ en A , entonces $f(e)$ es el elemento neutro de Δ en B .



Demostración:

Partiendo de: $\forall x, y \in A \quad x * e = e * x = x$

Hay que demostrar: $\forall y \in \text{Im}(f) \quad y \Delta f(e) = f(e) \Delta y = y$

Si $f(x) = y$

$$\begin{aligned} f(x * e) &= f(e * x) = f(x) \\ &= f(x) \Delta f(e) = f(e) \Delta f(x) = f(x) = y \end{aligned}$$

4. Si a y a' son **simétricos** en $(A, *)$, entonces $f(a)$ y $f(a')$ son simétricos en $(\text{Im}(f), \Delta)$.

Conclusión: El conjunto imagen tiene las mismas propiedades que el conjunto original. Por eso se le llama homomorfismo.

Tipos de homomorfismos

Sean $(A, *)$ y (B, Δ) dos estructuras y $f: A \rightarrow B$ un homomorfismo.

f es **monomorfismo** $\Leftrightarrow f$ es inyectiva

f es **epimorfismo** $\Leftrightarrow f$ es sobreyectiva

f es **isomorfismo** $\Leftrightarrow f$ es biyectiva

(cuando todas las propiedades son iguales en dos conjuntos, se habla de conjuntos *isomorfos*)

Si f es un homomorfismo de $(A, *)$ en $(A, *)$, lo llamaremos **endomorfismo**, y si además es biyectivo, **automorfismo**.

Ejercicio: ¿Por qué no aparecen ahora funciones sobreyectivas o inyectivas (en los endomorfismos)?

Homomorfismos de grupos

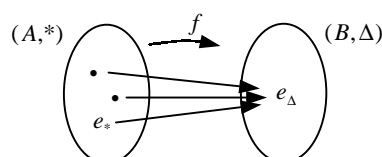
Sean $(A, *)$ y (B, Δ) dos grupos y $f: A \rightarrow B$ un homomorfismo.

- Si X es un subgrupo de $A \Rightarrow f(X)$ es subgrupo de B .
- Si Y es un subgrupo de $B \Rightarrow f^{-1}(Y)$ es un subgrupo de A .

Núcleo de un homomorfismo

Sean $(A, *)$ y (B, Δ) dos grupos y $f: A \rightarrow B$ un homomorfismo. Sea e_Δ el elemento neutro de (B, Δ) . Se define el núcleo de f como:

$$\text{Ker}(f) = \{x \in A \mid f(x) = e_\Delta\}$$



$\text{Ker}(f)$ es un **subgrupo normal** de $(A, *)$.

- Subgrupo: Si $\text{Ker}(f) = \emptyset$
 $\forall x, y \in \text{Ker}(f) \quad x * y' \in \text{Ker}(f)$
- Normal: $\left. \begin{array}{l} \forall x \in \text{Ker}(f) \\ \forall a \in A \end{array} \right\} a * x * a' \in \text{Ker}(f)$

El elemento neutro e_* siempre pertenece a $\text{Ker}(f)$.

Teorema: Sea f un homomorfismo de grupos de $(A, *)$ en (B, Δ) .

$$f \text{ es inyectiva} \Leftrightarrow \text{Ker}(f) = \{e_*\}$$

(siendo e_* el elemento neutro de $(A, *)$)

Demostración:

a) Si $\text{Ker}(f) = \{e_*\} \Rightarrow f$ es inyectiva.

$$f(a) = f(b) \Rightarrow a = b \quad \forall a, b \in A$$

$$f(a) = f(b) \rightarrow f(a) \Delta f(b)' = f(b) \Delta f(b)' = e_\Delta$$

$$\text{Por ser homomorfismo: } f(a * b') = e_\Delta$$

$$\text{Como } f(a * b') = e_\Delta, a * b' \in \text{Ker}(f).$$

Como en el núcleo sólo está el elemento neutro: $a * b' = e_*$

Concluyéndose que $a = b$.

b) Si f es inyectiva $\Rightarrow \text{Ker}(f) = \{e_*\}$

$e_* \in \text{Ker}(f)$ (trivial)

Suponiendo $x \in \text{Ker}(f)$ con $x \neq e_*$

$\left. \begin{array}{l} f(x) = e_\Delta \\ f(e_*) = e_\Delta \end{array} \right\}$ por ser inyectiva, $f(x) = f(e_*) \Rightarrow x = e_* \rightarrow$ contradicción

Homomorfismos de anillos

Dados dos anillos $(A, +, \cdot)$ y $(B, *, \Delta)$, una función $f: A \rightarrow B$ es un homomorfismo si $\forall x, y \in A$:

$$f(x + y) = f(x) * f(y) \quad f(x \cdot y) = f(x) \Delta f(y)$$

Núcleo de un homomorfismo entre anillos

Sean $(A, +, \cdot)$ y $(B, *, \Delta)$ dos anillos y $f: A \rightarrow B$ un homomorfismo de anillos. Sea 0_A el neutro para $+$ en A y 0_B el neutro para $*$ en B .

Se define el núcleo de f como:

$$\text{Ker}(f) = \{x \in A \mid f(x) = 0_B\}$$

Teorema: f es inyectiva $\Leftrightarrow \text{Ker}(f) = \{0_A\}$

Homomorfismos de cuerpos

Sean $(A, +, \cdot)$ y $(B, *, \Delta)$ dos cuerpos y $f: A \rightarrow B$ un homomorfismo.

$$\text{Ker}(f) = \{0_A\} \text{ (inyectivo)}$$

ó

$$\text{Ker}(f) = \{A\} \text{ (homomorfismo nulo, } \forall x \in A \quad f(x) = 0_B)$$