Universidad Nacional de Asunción
Facultad de Ingeniería

Apuntes de Álgebra Moderna

En proceso de elaboración

Clases de teoría

Fredy Gabriel Ramírez Villanueva

versión 0.1.0-alpha

18 de agosto de 2024

Índice general

Capítulo 1

Conjuntos y funciones

1.1. Conjuntos

1.1.1. Definición intuitiva de conjunto

Un conjunto es una colección o agrupación de objetos o elementos que comparten una característica común. Estos objetos pueden ser números, letras, personas, animales, o cualquier otra cosa que deseemos considerar juntos. En otras palabras, un conjunto es como una "caja" que contiene elementos relacionados.

Ejemplos de conjuntos

- Conjunto de números naturales ($\mathbb{N}$):

  El conjunto de todos los números naturales es un ejemplo fundamental. Se denota como $\mathbb{N}$ y contiene los números $\{1, 2, 3, 4, 5, \ldots\}$.

- Conjunto de vocales: $\{a, e, i, o, u\}$.

- Conjunto de días de la semana:

  $\{\text{lunes}, \text{martes}, \text{miércoles}, \text{jueves}, \text{viernes}, \text{sábado}, \text{domingo}\}$

- Conjunto de números pares: $\{2, 4, 6, 8, 10, \ldots\}$

- Conjunto de colores primarios: $\{\text{rojo}, \text{azul}, \text{amarillo}\}$.

En un conjunto, los elementos no se repiten, y el orden no importa. Notar que los elementos de un conjunto se escriben entre llaves {}.

Notación

Para denotar conjuntos utilizaremos generalmente letras mayúsculas ($A, B, C, \ldots$), y para especificar elementos se usarán letras minúsculas ($a, b, c, \ldots$), a menos que dichos elementos sean, a su vez, conjuntos.

Conjuntos numéricos

Las notaciones usuales para caracterizar conjuntos numéricos son las siguientes:

- $\mathbb{N}$: conjunto de números naturales;
- $\mathbb{Z}$: conjunto de números enteros;
- $\mathbb{Q}$: conjunto de números racionales;
- $\mathbb{R}$: conjunto de números reales;
- $\mathbb{C}$: conjunto de números complejos;

Conjuntos especiales

- El **conjunto universal**, denotado como U, es el que contiene todos los elementos posibles que estamos considerando en un contexto particular. Es el conjunto más grande en ese contexto y actúa como un marco de referencia para otros conjuntos más pequeños.

  Por ejemplo, si estamos trabajando con números naturales, el conjunto universal sería $\mathbb{N}$, que incluye todos los números positivos enteros: $\{1, 2, 3, 4, \ldots\}$.

- El **conjunto vacío**, denotado como $\emptyset$, es aquel que no contiene ningún elemento. El conjunto vacío es único, es decir todos los conjuntos vacíos son iguales.

  Por ejemplo, el conjunto vacío puede representar el conjunto de números reales que son mayores que 10 y menores que 5. Dado que no hay números que cumplan esta condición, el conjunto resultante es vacío: $\emptyset$.

- Un **conjunto unitario** está formado por un único elemento. Ejemplo $A = \{a\}$.

1.1.2. Relaciones de pertenencia e inclusión

Pertenencia

Para indicar la pertenencia de un elemento a un conjunto será utilizado el símbolo $\in$.

La proposición $a \in A$ se lee "*a pertenece* a A", o bien "el elemento *a pertenece* al conjunto A". Su negación es $a \notin A$, que se lee "*a no pertenece* a A"

Notación por extensión

En la notación por extensión, enumeramos todos los elementos de un conjunto de manera explícita, es decir, listamos cada elemento individualmente. Algunos ejemplos:

1. Conjunto de números pares menores que 10: $E = \{2, 4, 6, 8\}$
2. Conjunto de vocales: $V = \{a, e, i, o, u\}$
3. Conjunto de meses del año: $M = \{\text{enero}, \text{febrero}, \ldots, \text{diciembre}\}$

Notación por comprensión

En la notación por comprensión, describimos las propiedades o características que deben cumplir los elementos del conjunto, luego, utilizamos una condición lógica para definir el conjunto.

En general su estructura tiene la forma:

$$A = \{x \in U \mid P(x)\}$$

es decir, el conjunto cuyos elementos verifican la propiedad $P(x)$, o más brevemente, si U está sobreentendido:

$$A = \{x \mid P(x)\}$$

se lee: "A es el conjunto formado por los elementos x, tales que $P(x)$", en donde $P(x)$ es un función proposicional.

Un objeto a del universal pertenece al conjunto A, si y sólo si verifica la propiedad $P(x)$, es decir:

$$a \in A \iff P(a)$$

en consecuencia:

$$a \notin A \iff \neg P(a)$$

Ejemplo 1.1

1. Conjunto de números pares: $P = \{x \in \mathbb{N} \mid x = 2k \wedge k \in \mathbb{N}\}$

   "Son todos los números naturales x tal que cada x es igual al doble de un número natural k".

2. Conjunto de números primos menores que 20:

   $$N = \{x \in \mathbb{N} \mid (x \text{ es un número primo}) \wedge (x < 20)\}$$

   "Son todos los números naturales que son a la vez primos y menores que 20"

3. Conjunto de letras del alfabeto: $L = \{x \mid x \text{ es una letra del alfabeto}\}$

   "El conjunto de elementos x tal que x es una letra del alfabeto"

4. El conjunto vacío puede definirse simbólicamente como: $\emptyset = \{x \mid x \neq x\}$

   "Los elementos x tal que cada x es distinto de sí mismo" (no existen tales elementos).

   En este caso la propiedad relativa a x es $P(x) : x \neq x$, la cual resulta falsa cualquiera sea x.

5. Si A es un conjunto unitario cuyo único elemento es a, escribiremos:

   $$A = \{a\} = \{x \mid x = a\}$$

Inclusión

Definición 1.1. Inclusión

Sean A y B dos conjuntos, si ocurre que todo elemento de A pertenece a B, diremos que A está incluido en B, o que A es parte de B, o que A es un subconjunto de B.

Notación:

$$A \subset B$$

Formalmente:

$$A \subset B \iff \forall x : x \in A \implies x \in B$$

Esta definición tiene el siguiente significado: si sabemos que $A \subset B$, entonces la proposición $\forall x : x \in A \implies x \in B$ es verdadera; recíprocamente, si esta proposición es verdadera, entonces se verifica que $A \subset B$.

- Ejemplos:

  1. Consideremos los conjuntos: $A = \{1, 2\}$ y $B = \{1, 2, 3\}$.

     En este caso, $A \subset B$, ya que todos los elementos de A (1 y 2) también pertenecen a B.

  2. Consideremos los conjuntos:

     - $C = \{x \mid x \text{ es un número par}\}$
     - $D = \{x \mid x \text{ es un número entero}\}$

       Aquí, $C \subset D$, ya que todo número par es también entero.

- Propiedades de la inclusión

  I) **Reflexibidad**: Todo conjunto es parte de sí mismo.

  $$A \subset A$$

  II) **Transitividad**: Si un conjunto es parte de otro y este es parte de un tercero, el primero está incluido en el tercero:

  $$A \subset B \text{ y } B \subset C \implies A \subset C$$

  III) **Antisimetría**: Si un conjunto es parte de otro y éste es parte del primero, entonces son iguales.

  $$A \subset B \text{ y } B \subset A \implies A = B$$

- Observaciones:

  1. En repetidas ocasiones se necesitará demostrar que un conjunto es parte de otro; entonces, de acuerdo con la definición, será suficiente demostrar que cualquier elemento del primero pertenece al segundo, es decir, en la inclusión no puede darse que haya un elemento de A que no pertenezca a B.

  $$A \subset B \implies x \in A \implies x \in B$$

2. El conjunto vacío es subconjunto de cualquier conjunto.

$$\emptyset \subset A$$

Diagrama de Venn

Existe una representación visual de los conjuntos dados por diagramas llamados de Venn. En este sentido, el conjunto universal suele representarse por un rectángulo y los conjuntos por recintos cerrados. Es claro que todo elemento de A pertenece a U, es decir, $A \subset U$. A, B y C subconjuntos de U, como indica el diagrama de la fig. 1.1.

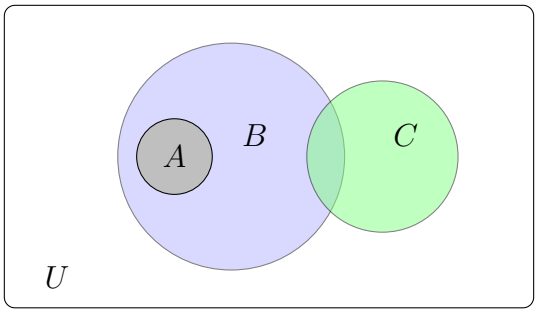


Figura 1.1. Diagrama de Venn

1.1.3. Operaciones con conjuntos

Unión $\cup$

Definición 1.2. Unión

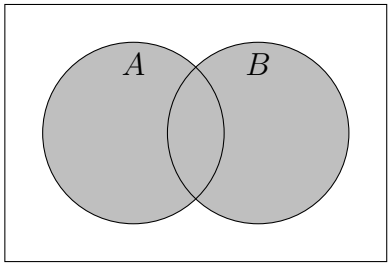
La unión de dos conjuntos A y B consiste en todos los elementos que pertenecen a A, a B, o a ambos conjuntos.

Notación: $A \cup B$

Formalmente:

$$A \cup B = \{x \mid x \in A \text{ o } x \in B\}$$

- Diagrama de Venn



$A \cup B$

- Ejemplo: Si $A = \{1, 2, 3\}$ y $B = \{3, 4, 5\}$, entonces $A \cup B = \{1, 2, 3, 4, 5\}$.
- Propiedades:

i) Idempotencia[1]: $A \cup A = A$

ii) Asociatividad: $(A \cup B) \cup C = A \cup (B \cup C)$

iii) Conmutatividad: $A \cup B = B \cup A$

Intersección $\cap$

Definición 1.3. Intersección

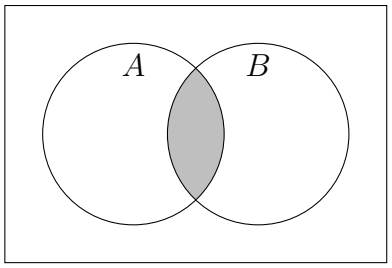
La intersección de dos conjuntos A y B contiene los elementos que pertenecen tanto a A como a B.

Notación: $A \cap B$

Formalmente:

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

- Diagrama de Venn



$A \cap B$

- Ejemplo: Si $A = \{1, 2, 3\}$ y $B = \{3, 4, 5\}$, entonces $A \cap B = \{3\}$.
- Propiedades:

i) Idempotencia: $A \cap A = A$

ii) Asociatividad: $(A \cap B) \cap C = A \cap (B \cap C)$

iii) Conmutatividad: $A \cap B = B \cap A$

Complemento (A^c)

Definición 1.4. Complemento

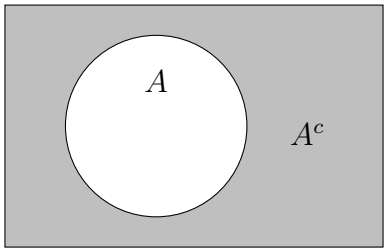
El complemento de un conjunto A con respecto a un conjunto universal U contiene todos los elementos que no están en A. Notación: A^c o $\overline{A}$ o A'

Formalmente:

$$A^c = \{x \mid x \in U \text{ y } x \notin A\}$$

[1]La idempotencia se define en la pág. 76, definición 3.4.

- Diagrama de Venn



A^c

- Ejemplo: Si U es el conjunto de números naturales y A el conjunto de números pares, $A = \{2, 4, 6, \ldots\}$, entonces A^c es el conjunto de números impares, $A^c = \{1, 3, 5, 7, \ldots\}$.
- Propiedades:
  1. Involución $(A^c)^c = A$.

     De donde: Si $A^c = B$ entonces $B^c = A$
  2. $A \subset B \implies B^c \subset A^c$
  3. El complemento del vacío es el universal: $\emptyset^c = U$
  4. El complemento del universal es el vacío: $U^c = \emptyset$

Diferencia $(-, \setminus)$

Definición 1.5. Diferencia

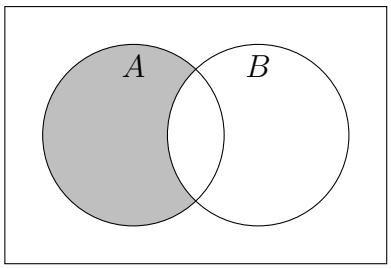
La diferencia entre dos conjuntos A y B contiene los elementos que están en A pero no en B.

Notación: $A - B$ o $A \setminus B$

Formalmente:

$$A \setminus B = \{x \mid x \in A \text{ y } x \notin B\}$$

- Diagrama de Venn



$A \setminus B$

- Ejemplo: Si $A = \{1, 2, 3\}$ y $B = \{3, 4, 5\}$, entonces $A - B = \{1, 2\}$.

- Propiedades:

    1) La diferencia entre dos conjuntos es igual a la intersección del primero con el complemento del segundo: $A \setminus B = A \cap B^c$

Diferencia simétrica $\triangle$

Definición 1.6. Diferencia simétrica

La diferencia simétrica de dos conjuntos A y B, es el conjunto que contiene los elementos que pertenecen a A o a B, pero no a ambos.

Notación: $A \triangle B$

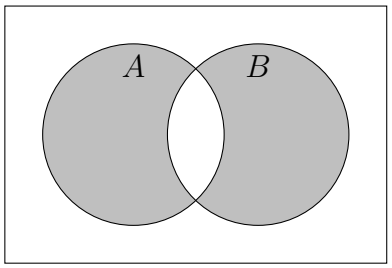
Formalmente:

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

La diferencia simétrica es el conjunto de elementos que están en uno de los conjuntos, pero no en ambos. Es como si "excluyéramos" la intersección de los dos conjuntos, por lo tanto también podemos escribir:

$$A \triangle B = (A \cup B) \setminus (A \cap B)$$

- Diagrama de Venn



$A \triangle B$

- Ejemplos:

    1. Consideremos los conjuntos: $A = \{1, 2, 3, 4\}$ y $B = \{3, 4, 5, 6\}$. Entonces, la diferencia simétrica es:

    $$A \triangle B = \{1, 2, 5, 6\}$$

    Los elementos 1 y 2 están solo en A, 5 y 6 están solo en B, y los elementos 3 y 4 se excluyen porque están en ambos conjuntos.

    2. Consideremos los conjuntos:

        - $C = \{x \mid x \text{ es un número par}\}$
        - $D = \{x \mid x \text{ es un número primo}\}$

La diferencia simétrica es:

$$C \triangle D = \{x \mid x \text{ es par y no es 2, o } x \text{ es primo y no es 2}\}$$

El número 2 se excluye porque es el único par que también es primo.

- Propiedades:
  - I) Conmutatividad: $A \triangle B = B \triangle A$
  - II) Asociatividad: $(A \triangle B) \triangle C = A \triangle (B \triangle C)$
  - III) Existencia del neutro: $A \triangle \emptyset = \emptyset \triangle A = A$
  - IV) Existencia de inversas: $A \triangle A = \emptyset$

Conjunto potencia o conjunto de partes $\mathcal{P}(A)$

Definición 1.7. Conjunto potencia

Dado un conjunto A, el conjunto potencia o conjunto de partes de A, denotado por $\mathcal{P}(A)$ o 2^A, es el conjunto de todos los subconjuntos de A.

Formalmente:

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}$$

Es decir, el conjunto potencia de un conjunto A es una colección que contiene a todos los posibles subconjuntos de A, incluyendo el conjunto vacío ($\emptyset$) y el propio conjunto A.

- Ejemplos:
  1. Consideremos el conjunto: $A = \{1, 2\}$

     Entonces, el conjunto potencia es:

     $$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$$

     Observe que hay $2^2 = 4$ elementos en el conjunto potencia, ya que cada elemento de A tiene dos opciones: estar o no estar en un subconjunto particular.

  2. Consideremos el conjunto: $B = \{a, b, c\}$

     El conjunto potencia es:

     $$\mathcal{P}(B) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

     En este caso, hay $2^3 = 8$ elementos en el conjunto potencia.

  En general, si un conjunto A tiene n elementos, entonces su conjunto potencia $\mathcal{P}(A)$ tiene 2^n elementos.

Producto cartesiano

Definición 1.8. Producto cartesiano

El producto cartesiano de dos conjuntos A y B, es el conjunto de todos los pares ordenados (a, b) donde el primer elemento a pertenece al conjunto A y el segundo elemento b pertenece al conjunto B.

Notación: $A \times B$

Formalmente:

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

Esto es, el producto cartesiano combina cada elemento de un conjunto con cada elemento del otro conjunto, formando pares ordenados donde el orden de los elementos es importante.

- Ejemplos:
  1. Consideremos los conjuntos: $A = \{1, 2\}$ y $B = \{x, y\}$, entonces, el producto cartesiano es:
  $$A \times B = \{(1, x), (1, y), (2, x), (2, y)\}$$
  2. Consideremos los conjuntos: $C = \{a, b\}$ y $D = \{1, 2, 3\}$, el producto cartesiano es:
  $$C \times D = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$$
- Observaciones:
  1. El producto cartesiano no es conmutativo, es decir, en general, $A \times B \neq B \times A$.
  2. Si A tiene m elementos y B tiene n elementos, entonces $A \times B$ tiene $m \cdot n$ elementos.
  3. El producto cartesiano se puede extender a más de dos conjuntos. Por ejemplo, el producto cartesiano de tres conjuntos A, B y C es:
  $$A \times B \times C = \{(a, b, c) \mid a \in A, b \in B, c \in C\}$$
  4. Si los elementos son del mismo conjunto A:
  $$A \times A \times A = A^3 = \{(a, b, c) \mid a, b, c \in A\}$$
- Propiedades:

  ı) El producto cartesiano es **distributivo** respecto de la unión:
  $$(A \cup B) \times C = (A \times C) \cup (B \times C)$$

1.1.4. Álgebra de conjuntos

Propiedades fundamentales

- **Idempotencia**:
  - $A \cup A = A$
  - $A \cap A = A$
- **Conmutatividad**:
  - $A \cup B = B \cup A$
  - $A \cap B = B \cap A$
- **Asociatividad**:
  - $(A \cup B) \cup C = A \cup (B \cup C)$
  - $(A \cap B) \cap C = A \cap (B \cap C)$
- **Distributividad**:
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- **Leyes de De Morgan**:

  1) El complemento de la unión de dos conjuntos es igual a la intersección de los complementos de dichos conjuntos.

  $$(A \cup B)^c = A^c \cap B^c$$

  2) El complemento de la intersección de dos conjuntos es igual a la unión de los complementos de dichos conjuntos.

  $$(A \cap B)^c = A^c \cup B^c$$

- **Elemento neutro**[2]:
  - De la unión es el conjunto vacío: $A \cup \emptyset = A$
  - De la intersección es el universal: $A \cap U = A$
  - De la diferencia simétrica es el conjunto vacío: $A \triangle \emptyset = \emptyset \triangle A = A$
- **Existencia de inversas**[3]:
  - Para la diferencia simétrica, A es su propia inversa: $A \triangle A = \emptyset$
- **Otras propiedades**:
  - $A \cup A^c = U$
  - $A \cap A^c = \emptyset$

[2] El concepto de elemento neutro se presenta en detalle en la sección 3.1.1, pág. 74
[3] ibid.

Operaciones generalizadas

- **Unión generalizada**

  Dada una colección finita de conjuntos $\{A_1, A_2, \ldots, A_n\}$ la unión generalizada de estos conjuntos se denota por:

  $$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$$

  Se define como el conjunto que contiene todos los elementos que pertenecen a *al menos uno* de los conjuntos A_i.

  Formalmente:

  Si definimos el conjunto de índices $I_n = \{1, 2, \ldots, n\}$ (conjunto de los n primeros números naturales):

  $$\bigcup_{i=1}^{n} A_i = \{x \mid x \in A_i \text{ para algún } i \in I_n\}$$

  Si el conjunto I_n se identifica con $\mathbb{N}$ (conjunto de números naturales):

  $$\bigcup_{i=1}^{\infty} A_i = \{x \mid x \in A_i \text{ para algún } i \in \mathbb{N}\}$$

- **Intersección generalizada**

  Dada una colección finita de conjuntos $\{A_1, A_2, \ldots, A_n\}$ la intersección generalizada de estos conjuntos se denota por:

  $$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$$

  Se define como el conjunto que contiene todos los elementos que pertenecen a *todos* los conjuntos A_i.

  Formalmente:

  $$\bigcap_{i=1}^{n} A_i = \{x \mid x \in A_i \ \forall i \in I_n\}$$

  Si el conjunto I_n se identifica con $\mathbb{N}$:

  $$\bigcap_{i=1}^{\infty} A_i = \{x \mid x \in A_i \ \forall i \in \mathbb{N}\}$$

- **Leyes de De Morgan generalizadas**

  1. El complemento de la unión es igual a la intersección de los complementos.

  $$\left(\bigcup_{i \in I} A_i\right)^c = \bigcap_{i \in I} A_i^c$$

2. El complemento de la intersección es igual a la unión de los complementos.

$$\left(\bigcap_{i\in I} A_i\right)^c = \bigcup_{i\in I} A_i^c$$

Ejemplo 1.2. Unión e intersección generalizadas

Consideremos los conjuntos:

- $A_1 = \{1, 2, 3\}$
- $A_2 = \{2, 3, 4\}$
- $A_3 = \{3, 4, 5\}$

Entonces:

$$\bigcup_{i=1}^{3} A_i = \{1, 2, 3, 4, 5\}$$

$$\bigcap_{i=1}^{3} A_i = \{3\}$$

Uniones disjuntas

Definición 1.9. Uniones disjuntas

Se dice que una colección de conjuntos tiene *uniones disjuntas* si los conjuntos son mutuamente excluyentes, es decir, si la intersección de cualquier par de conjuntos de la colección es el conjunto vacío.

Formalmente, una colección de conjuntos $\{A_i\}_{i\in I}$ es una colección de uniones disjuntas si:

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

Es decir, los conjuntos en una unión disjunta no comparten ningún elemento[a].

Notación:

Para dos conjuntos disjuntos A y B, es usual escribir:

$$A + B$$

en lugar de $A \cup B$ para el caso $A \cap B = \emptyset$.

[a] La noción de uniones disjuntas se puede generalizar a un número infinito de conjuntos.

Algunas aplicaciones:

1. *Partición de un conjunto*[4]: Una partición de un conjunto A es una colección de subconjuntos no vacíos de A que son disjuntos dos a dos y cuya unión es igual a

[4] Las particiones se estudian en la sección 1.2.2, pág. 18

A. Las particiones son útiles en diversas áreas, como la teoría de probabilidades y estadística.

2. *Clasificación*: En muchas situaciones, es necesario clasificar objetos en diferentes categorías. Estas pueden ser representadas como conjuntos disjuntos, donde cada objeto pertenece a una y solo una categoría. Por ejemplo, en biología, los organismos se clasifican en diferentes especies, que son conjuntos disjuntos.

Ejemplo 1.3. Uniones disjuntas

Consideremos los siguientes conjuntos: $A_1 = \{1, 2, 3\}$, $A_2 = \{4, 5\}$, $A_3 = \{6\}$

La colección $\{A_1, A_2, A_3\}$ es una colección de uniones disjuntas, ya que:

- $A_1 \cap A_2 = \emptyset$
- $A_1 \cap A_3 = \emptyset$
- $A_2 \cap A_3 = \emptyset$

1.2. Relaciones y particiones

Una *relación* es un vínculo o una correspondencia. Se trata de la correspondencia que existe entre dos conjuntos: a cada elemento del primer conjunto le corresponde al menos un elemento del segundo conjunto.

Cuando a cada elemento de un conjunto le corresponde solo uno del otro, se habla de *función*. Esto quiere decir que las funciones siempre son, a su vez, relaciones, pero que las relaciones no siempre son funciones.

Definición 1.10. Relaciones

Dados dos conjuntos A y B, una **relación** entre ellos es un subconjunto $\mathcal{R} \subset A \times B$, en el que el par ordenado $(a, b) \in \mathcal{R}$ con $a \in A$ y $b \in B$, así decimos que a está relacionado con b y se denota:

$$a\mathcal{R}b$$

1.2.1. Relaciones de equivalencia

Definición 1.11. Relación de equivalencia

La relación $\mathcal{R} \subset A^2$ es de equivalencia en A si y sólo si es reflexiva, simétrica y transitiva

Se suele utilizar el símbolo "$\equiv$" o "$\sim$". La notación $a \sim b$ o $a \equiv b$ se lee "a es equivalente a b".

Conforme a la definición, las relaciones de equivalencia satisfacen:

I) **Reflexividad**: Todo elemento en A es equivalente a sí mismo.

$$\forall x \in A : \Longrightarrow \ x \equiv x$$

II) **Simetría**: Si un elemento es equivalente a otro, entonces este es equivalente al primero.

$$\forall x, y \in A : x \equiv y \implies y \equiv x$$

III) **Transitividad**: Si un elemento es equivalente a otro y éste es equivalente a un tercero, entonces el primero es equivalente al tercero.

$$\forall x, y, z \in A : x \equiv y \wedge y \equiv z \implies x \equiv z$$

Clases de equivalencia y conjunto cociente

Definición 1.12. Clase de equivalencia

Sea A un conjunto y $\mathcal{R}$ una relación de equivalencia en A. Para cada elemento $a \in A$, la **clase de equivalencia** de a, que se denota $[a]$ o $\bar{a}$, es el conjunto de todos los elementos $x \in A$ tales que x está relacionado con a en $\mathcal{R}$.

$$[a] = \bar{a} = \{x \in A / x \mathcal{R} a\}$$

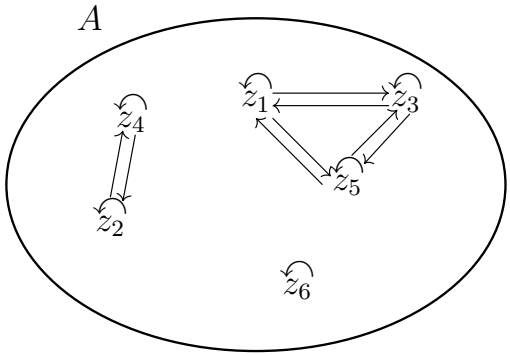
Ejemplo 1.4. Clases de equivalencia

Sea $A = \{z_1, z_2, z_3, z_4, z_5, z_6\}$ y la relación:

$$\mathcal{R} = \{(z_1, z_1), (z_1, z_3), (z_1, z_5), (z_2, z_2), (z_2, z_4), (z_3, z_1), (z_3, z_3), (z_3, z_5), (z_4, z_2), (z_4, z_4), (z_5, z_1), (z_5, z_3), (z_5, z_5), (z_6, z_6)\}$$

Las clases de equivalencia son:

$$\begin{aligned}
[z_1] &= \{z_1, z_3, z_5\} \\
[z_2] &= \{z_2, z_4\} \\
[z_3] &= \{z_1, z_3, z_5\} = [z_1] \\
[z_4] &= \{z_2, z_4\} = [z_2] \\
[z_5] &= \{z_1, z_3, z_5\} = [z_1] \\
[z_6] &= \{z_6\}
\end{aligned}$$



En la fig. se muestra, en un diagrama, las relaciones.

Definición 1.13. Conjunto cociente

Sea A un conjunto y $\mathcal{R}$ (o $\sim$)una relación de equivalencia en A. El **conjunto cociente** se define por:

$$A/\mathcal{R} = \frac{A}{\sim} = \{[a]/a \in A\}$$

Ejemplo 1.5. Conjunto cociente

Del ejemplo 1.4, el conjunto cociente es:

$$A/\mathcal{R} = \frac{A}{\sim} = \{[z_1], [z_2], [z_6]\} = \{\{z_1, z_3, z_5\}, \{z_2, z_4\}, \{z_6\}\}$$

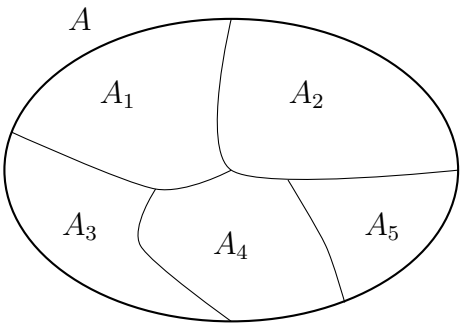
1.2.2. Particiones

Definición 1.14. Partición

Dado un conjunto no vacío A, una **partición** de A es una colección finita o infinita de conjuntos de A que cumplen:

$$A_i \cap A_j = \emptyset \; \forall \, i \neq j \quad \wedge \quad \cup_{i=1}^{n} A_i = A$$

En la fig. 1.2 se muestra en un diagrama, una partición de A.



$A_i \cap A_j = \emptyset$, siempre que $i \neq j$
$A_1 \cup A_2 \cup \cdots \cup A_5 = A$

Figura 1.2

Teorema fundamental de las relaciones de equivalencia

Toda relación de equivalencia definida en un conjunto no vacío determina una partición de éste en clases de equivalencia.

Teorema 1.1. Fundamental de las relaciones de equivalencia

Si $\sim$ es una relación de equivalencia definida en el conjunto $A \neq \emptyset$, entonces existe un subconjunto $I \subset \mathbb{N}$, tal que cualquiera sea $i \in I$, existe $A_i \subset A$, de modo que se verifican las siguientes proposiciones:

I) $i \in I \implies A_i \neq \emptyset$;

II) $a \sim b \iff a$ y b pertenecen al mismo A_i;

III) $A_i \cap A_j \neq \emptyset \implies A_i = A_j$;

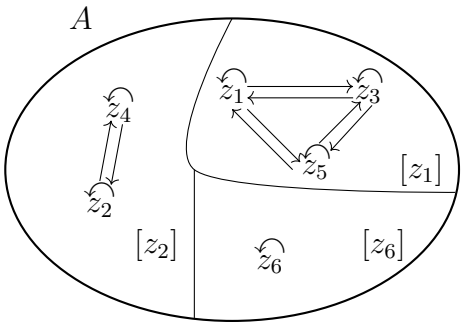
IV) $i \neq j \implies A_i \cap A_j = \emptyset$;

V) $\forall a \in A, \exists i \in I / a \in A_i$

Las clases de equivalencia conforman una partición del conjunto A.

Ejemplo 1.6. Particiones

Del ejemplo 1.4:



$$A/\mathcal{R} = \{[z_1], [z_2], [z_3]\}$$
$$[z_1] \cap [z_2] = \emptyset,\ [z_1] \cap [z_6] = \emptyset,$$
$$[z_2] \cap [z_6] = \emptyset$$
$$[z_1] \cup [z_2] \cup [z_6] = A$$

1.3. Funciones

Esta sección está basada en [1] cap. 4.

1.3.1. Relaciones funcionales

Sean A y B dos conjuntos no vacíos, que llamaremos *dominio* y *codominio* respectivamente.

Una **función** de A en B es toda regla que hace corresponder a cada elemento de A un único elemento de B.

Para denotar que f (o g, h, etc.) es una función de A en B, se escribe:

$$f : A \to B$$

se lee: *f es una función o aplicación de A en B*, o bien *f es una función con dominio A y codominio B*.

Ejemplo 1.7. Función

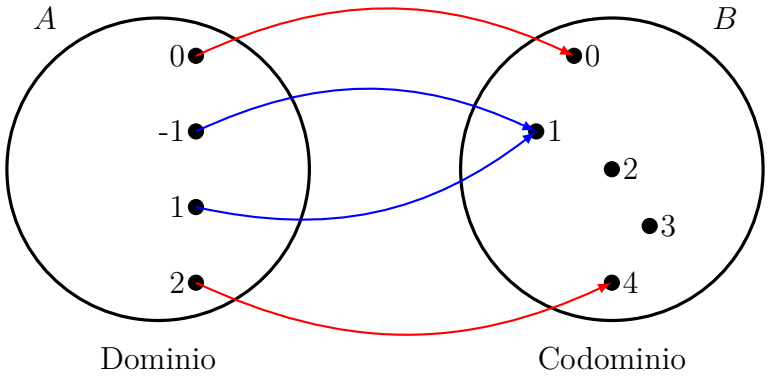
En particular, si $A = \{-1, 0, 1, 2\}$, $B = \{0, 1, 2, 3, 4\}$ y f es la relación

$$(x, y) \in f \iff y = x^2$$

se tiene (cada 2da. componente es el cuadrado de la 1ra.):

$$f = \{(-1, 1), (0, 0), (1, 1), (2, 4)\}$$

El diagrama de Venn correspondiente es:



Definición 1.15. Función

f es una función o aplicación de A en B si y sólo si f es una relación entre A y B, tal que todo elemento de A tiene un único correspondiente en B.

o bien:

Definición 1.16 (Función)**.** f es una función o aplicación de A en B si y sólo si f es un subconjunto de $A \times B$ que satisface las siguientes condiciones de existencia y unicidad:

1. $\forall a \in A,\ \exists\, b \in B / (a, b) \in f$
2. $(a, b) \in f \wedge (a, c) \in f \implies b = c$

Observaciones:

- Si $(a, b) \in f$ decimos que b es el correspondiente o *imagen* de a, por f, y suele escribirse $b = f(a)$, es decir, b es el transformado de a por la función f.
- Si f es como arriba, una aplicación o un *mapeo* de A a B a menudo se escribe $x \mapsto f(x)$ para denotar la imagen de x por f. Por ejemplo: Si $A = \mathbb{R}$ y $B = \mathbb{R}^+$, sea $f : \mathbb{R} \to \mathbb{R}^+$ la aplicación $f(x) = x^2$, es decir, el mapeo cuyo valor en x es x^2. Podemos también decir: f es la aplicación tal que $x \mapsto x^2$ (x se mapea a x^2 o x se transforma en x^2 o x se aplica a x^2). En este caso la imagen de f es el conjunto de números reales no negativos.
- Una función queda especificada si se da el dominio A, el codominio B, y además la relación $f \subset A \times B$, que satisface las condiciones 1 y 2 de la definición.

- Por ser un conjunto, f puede estar dado por *extensión*, es decir, como conjunto de pares ordenados, o bien por *comprensión*, mediante una fórmula o ley de correspondencia que permita asignar a cada objeto del dominio su imagen en el codominio.

Ejemplo 1.8. Funciones

Determinamos si las siguientes relaciones son funciones.

1. Sean $A = \{a, b, c, d\}, B = \{1, 2, 3\}$ y la relación:

$$f = \{(a, 1), (b, 2), (c, 3), (d, 1)\}$$

   Se cumplen las condiciones de la definición, y resulta f una función tal que:

$$f(a) = 1, \quad f(b) = 2, \quad f(c) = 2, \quad f(d) = 1$$

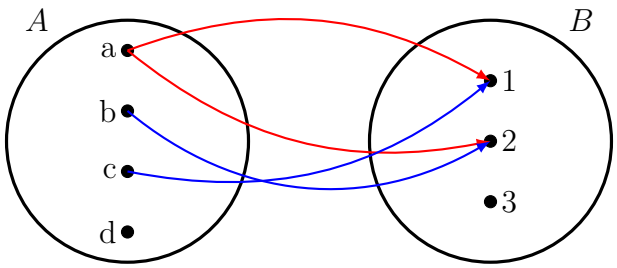
2. Con los mismos A y B la relación

$$\{(a, 1), (a, 2), (b, 2), (c, 1)\}$$

   No es una función.

   - No todo elemento en A (d) tiene imagen en B;
   - Un mismo elemento en A (a) tiene dos imágenes en B (1 y 2).

   El diagrama de la relación es:



3. Si A es el conjunto de las personas y f es la relación en A definida por:

$$(x, y) \in f \iff x \text{ es hijo de } y$$

   entonces f es una función de A en A, ya que toda persona tiene padre y este es único.

En cambio la relación definida en el mismo A mediante:

$$(x, y) \in f \iff x \text{ es padre de } y$$

no es una función de A en A, ya que existen en A personas que no son padres, es decir, elementos del dominio que carecen de imagen en el codominio, por otra parte, tampoco se verifica la unicidad pues existen personas que son padres de más de un hijo.

Nota: Si una relación es función, la relación inversa no lo es necesariamente

1.3.2. Representación cartesiana de funciones

Las funciones pueden representarse mediante un sistema de coordenadas cartesianas en el plano o en el espacio, según el dominio sea unidimensional o bidimensional respectivamente. En el caso del plano, el dominio es un subconjunto del eje horizontal, y el codominio, del eje vertical.

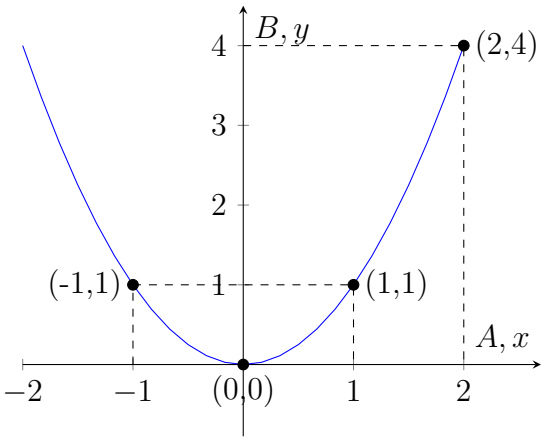
Ejemplo 1.9

Representación cartesiana de la función del ejemplo 1.7.

$$A = \{-1, 0, 1, 2\} \quad B = \{0, 1, 2, 3, 4\}$$

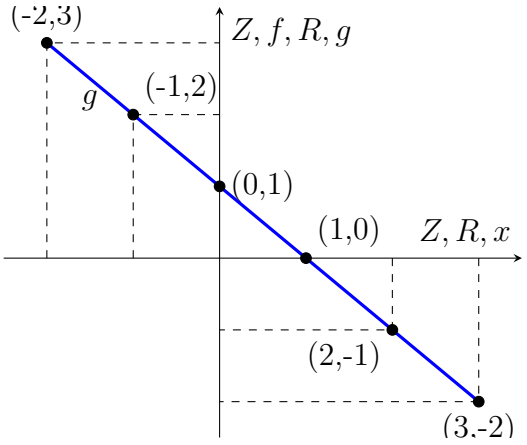
$$f(x) = y = x^2$$

Si $g : \mathbb{R} \to \mathbb{R}_0^+ / g(x) = y = x^2$, resulta la parábola de la figura.



Ejemplo 1.10

Sea $f : \mathbb{Z} \to \mathbb{Z}$ tal que la imagen de cada entero es su opuesto aumentado en 1, es decir: $f(x) = -x + 1$.



Si $g : \mathbb{R} \to \mathbb{R}$ es tal que $g(x) = -x + 1$. Su representación es un conjunto continuo de

(x, y)	$f(x, y) = x + y$
$(1, 1)$	2
$(1, 2)$	3
$(2, 1)$	3
$(2, 2)$	4

f	1	2
1	2	3
2	3	4

$\mathbb{R}^2$, consistente en una recta del plano.

Notar que $f \neq g$ aunque $f \subset g$.

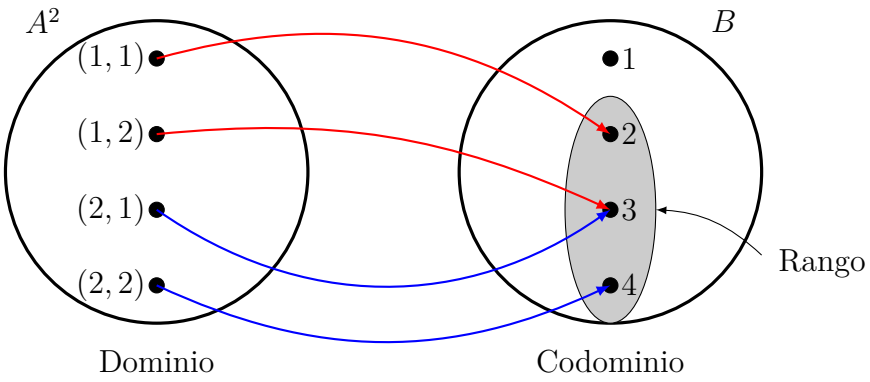
Ejemplo 1.11. Consideremos $A = \{1, 2\}$, $B = \{1, 2, 3, 4\}$ y la función:

$$f : A^2 \to B$$

que asigna a cada elemento del dominio A^2, la suma de sus componentes, es decir:

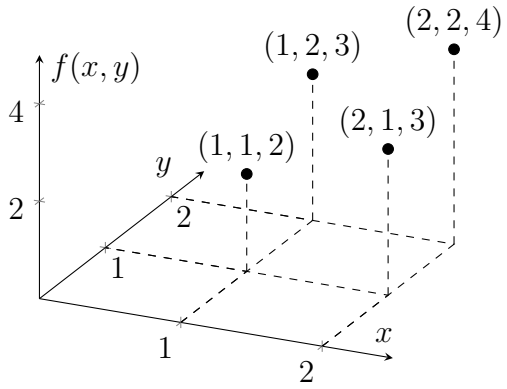
$$f(x, y) = x + y$$

1. Representación en una tabla de simple entrada. El elemento 1 de B carece de antecedente o *preimagen*[5] en A.
2. Representación en una tabla de doble entrada.
3. El diagrama de Venn es:

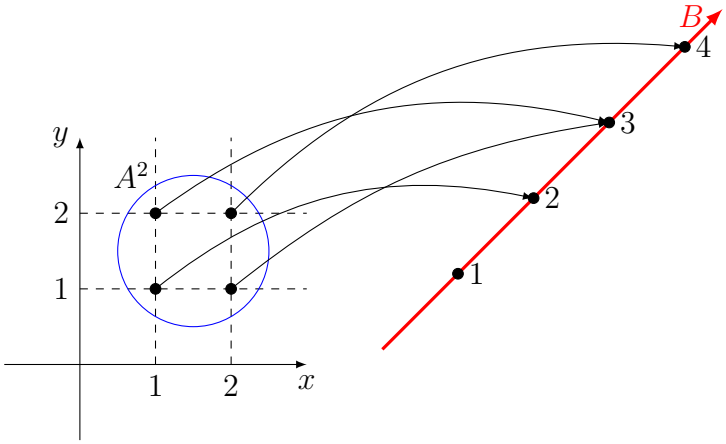


4. Representación cartesiana en el espacio.

[5]Ver definición 1.25, pág. 41.



5. La misma función puede representarse de la siguiente manera, desconectando el dominio del codominio.



1.3.3. Clasificación de funciones

Sea una función $f : A \to B$

- Si ocurre que elementos distintos del dominio tienen imágenes distintas en el codominio, entonces f se llama función *inyectiva* o uno a uno.
- Por otra parte, si todo elemento del codominio es imagen de algún elemento del dominio, la función se llama *sobreyectiva*.
- Cuando se presentan ambas situaciones simultáneamente, la función se llama *biyectiva* o correspondencia biunívoca.

Función inyectiva

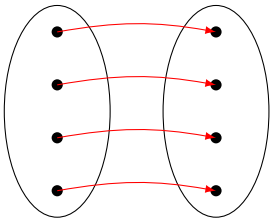
Definición 1.17. Función inyectiva

Una función $f : A \to B$ es inyectiva si, y solo si, para cualquier par de elementos distintos x' y x'' en el conjunto A, sus imágenes bajo la función f también son distintas.

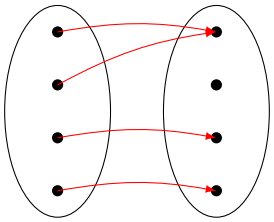
O, de forma equivalente:

Una función $f : A \to B$ es inyectiva si, y solo si, cuando dos elementos cualesquiera $x', x'' \in A$ tienen la misma imagen, $f(x') = f(x'')$ entonces esos dos elementos deben ser el mismo elemento ($x' = x''$).

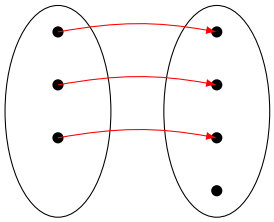
- En la inyectividad no puede darse que elementos distintos del dominio den la misma imagen.
- En el diagrama de Venn no puede presentarse ninguna bifurcación de elementos del dominio hacia el codominio.
- En la representación plana cartesiana no puede ocurrir que una ordenada corresponda a más de una abscisa.



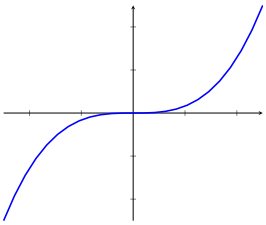
Sí es inyectiva



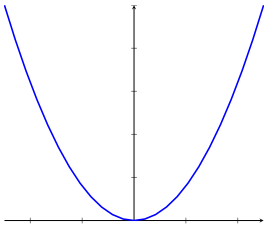
No es inyectiva



Sí es inyectiva



$f : \mathbb{R} \to \mathbb{R} / f(x) = x^3$
Sí es inyectiva



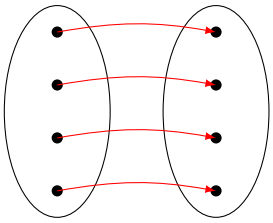
$f : \mathbb{R} \to \mathbb{R}_0^+ / f(x) = x^2$
No es inyectiva

Función sobreyectiva

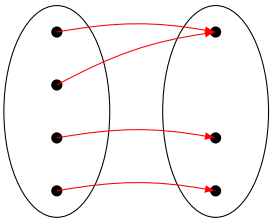
Definición 1.18. Función sobreyectiva

Una función $f : A \to B$ es *sobreyectiva* si, y solo si, para cada elemento $y \in B$, existe al menos un elemento $x \in A$ tal que $y = f(x)$.

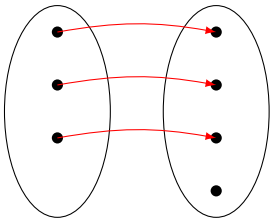
- El conjunto de las imágenes (*rango* o *recorrido*) se identifica con el codominio de la función. Es decir, no hay elementos del codominio que no sea la imagen de *al menos un* elemento del dominio, en otras palabras, el rango y el codominio coinciden.
- El ejemplo 3 corresponde a funciones sobreyectivas.
- Es usual nombrar a las funciones sobreyectivas como “sobre” o “suryectiva”



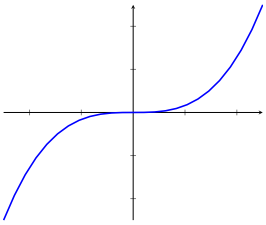
Sí es sobreyectiva



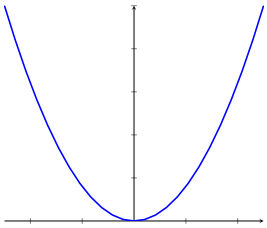
Sí es sobreyectiva



No es sobreyectiva



$f : \mathbb{R} \to \mathbb{R} / f(x) = x^3$
Sí es sobreyectiva



$f : \mathbb{R} \to \mathbb{R}_0^+ / f(x) = x^2$
Sí es sobreyectiva

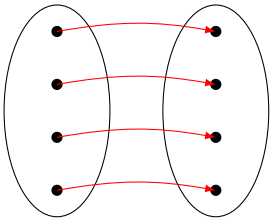
Función biyectiva

Definición 1.19. Función biyectiva

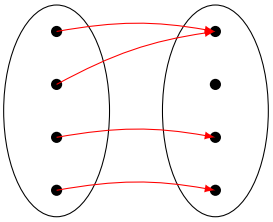
$f : A \to B$ es biyectiva si f es inyectiva y sobreyectiva.

- Las funciones del ejemplo 3 son biyectivas.

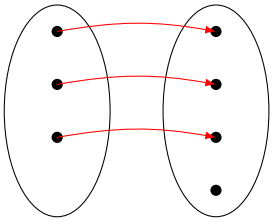
Notar que si $f : A \to B$ no es biyectiva, entonces no es inyectiva o no es sobreyectiva.



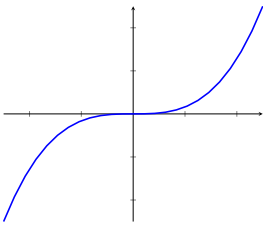
Sí es biyectiva



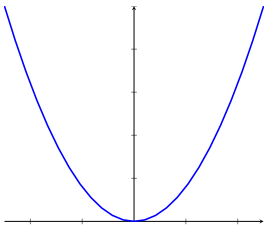
No es biyectiva



No es biyectiva



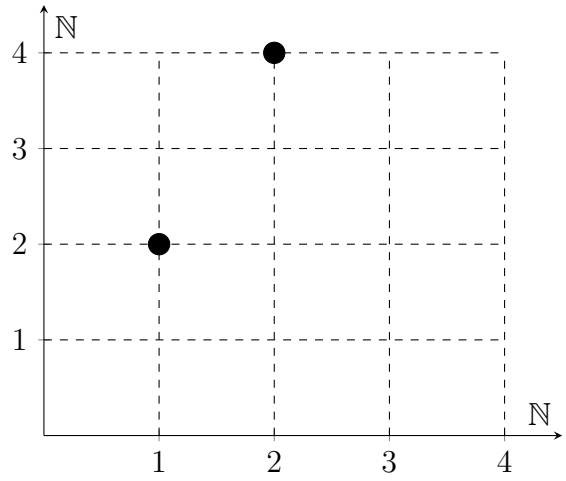
$f : \mathbb{R} \to \mathbb{R} / f(x) = x^3$
Sí es biyectiva



$f : \mathbb{R} \to \mathbb{R}_0^+ / f(x) = x^2$
No es biyectiva

Ejemplo 1.12

Probar la inyectividad de f, siendo $f : \mathbb{N} \to \mathbb{N}$ tal que $f(x) = 2x$



- Sean x' y x'' en $\mathbb{N}$ tales que $f(x') = f(x'')$, entonces $2x' = 2x''$, en consecuencia $x' = x''$. De modo que f es inyectiva uno a uno.
- f no es sobreyectiva, pues los elementos impares del codominio, carecen de antecedente. Resulta que f no es biyectiva.

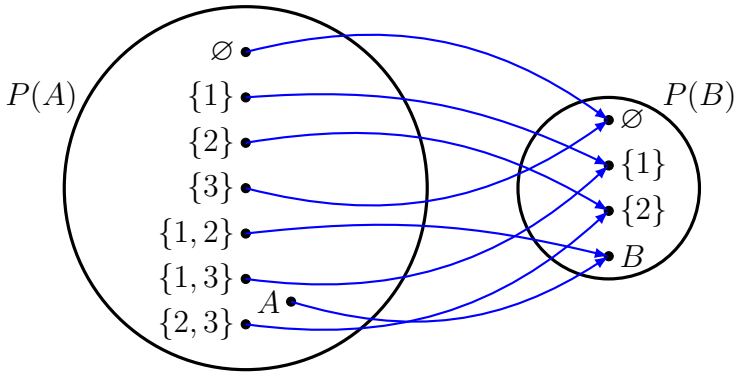
Si se utiliza el conjunto P de los números naturales pares y $f : \mathbb{N} \to \mathbb{P}$ tal que $f(x) = 2x$, f resulta biyectiva.

Ejemplo 1.13

Sean $A = \{1, 2, 3\}$ y $B = \{1, 2\}$.

Definimos $f : P(A) \to P(B)$ mediante $f(X) = X \cap B$, es decir, la imagen de todo subconjunto de A es su intersección con B.

El diagrama muestra que f es sobreyectiva pero no inyectiva.



Ejemplo 1.14. Función biyectiva

Sea $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^3$.

1. f es 1-1. En efecto, sean x_1 y x_2 en $\mathbb{R}$ tales que $f(x_1) = f(x_2)$, es decir, $x_1^3 = x_2^3$, o $x_1^3 - x_2^3 = 0$, factorizando:

$$(x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2) = 0$$

$$x_1 - x_2 = 0 \implies x_1 = x_2$$

de $x_1^2 + x_1x_2 + x_2^2 = 0$ se tiene:

$$x_1 = \frac{-x_2 \pm \sqrt{x_2^2 - 4x_2}}{2} = \frac{-x_2 \pm \sqrt{-3x_2^2}}{2}$$

Es decir:

$$x_1 = \left(-\frac{1}{2} \pm i\frac{\sqrt{3}}{2}\right) x_2 \tag{1.1}$$

Si $x_2 = 0$ entonces $x_1 = 0$ y resulta $x_1 = x_2$, los cuales son los únicos valores reales que satisfacen (1.1), en consecuencia f **es inyectiva**.

2. f **es sobreyectiva**, pues

$$\forall y \in \mathbb{R}, \exists\ x = \sqrt[3]{y} \text{ tal que } f(x) = f(\sqrt[3]{y}) = (\sqrt[3]{y})^3 = y$$

Ocurre entonces que f **es biyectiva**.

1.3.4. Funciones especiales

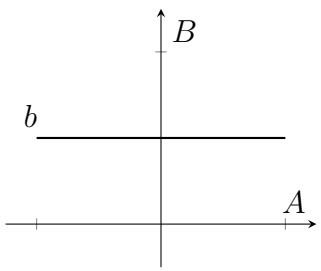
- **Función constante**

  La función $f : A \to B$, que asigna a todos los elementos del dominio el elemento $b \in B$, se llama constante.

  Está definida por $f(x) = b$ para todo $x \in A$, se tiene:

$$f = \{(x, b)/x \in A\}$$

  A menos que A sea unitario, la función constante **no es inyectiva**, y **es sobreyectiva** si B se reduce a un único elemento.



- **Función identidad**

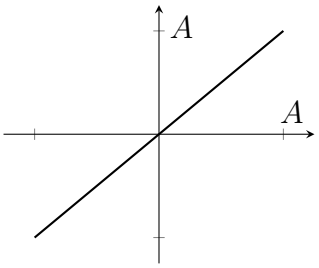
  Identidad en A es la aplicación que asigna a cada elemento de A el mismo elemento. $i_A : A \to A$ tal que $i_A(x) = x$.

A veces se utiliza el símbolo $\mathbf{1}_A$.

Se tiene: $i_A = \{(x, x)/x \in A\}$

Es decir, la identidad en A es la diagonal de A^2. Como relación es reflexiva, simétrica y transitiva, o sea, de equivalencia en A; además es antisimétrica.

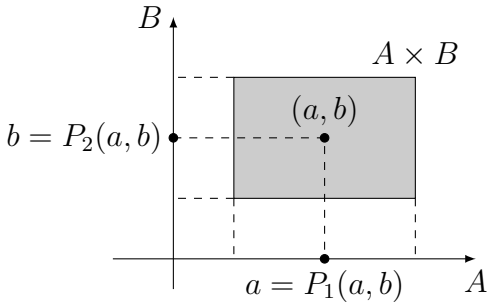
La función i_A es obviamente **biyectiva**.



- **Función proyección**

  Consideremos $A \times B$, y las funciones $P_1 : A \times B \to A$; $P_2 : A \times B \to B$ definidas por $P_1(a, b) = a \quad \text{y} \quad P_2(a, b) = b$

  Tales funciones se llaman *primera y segunda proyección del producto cartesiano*, y asignan a cada par ordenado la primera y la segunda componentes, respectivamente. En un gráfico cartesiano se tiene:



- **Función canónica**

  Sea $\sim$ o $\mathcal{R}$ una relación de equivalencia definida en el conjunto *no vacío* A. Por el teorema fundamental de las relaciones de equivalencia, queda determinado el conjunto cociente $\dfrac{A}{\sim} = A/\mathcal{R}$, cuyos elementos son las clases de equivalencia.

Definición 1.20. Función canónica

Aplicación canónica es la función:

$$\varphi : A \to A/\mathcal{R}$$

que asigna a cada elemento de A, su clase de equivalencia, es decir, tal que

$$\varphi(x) = K_x = [x]$$

Dos elementos equivalentes pertenecen a la misma clase y en consecuencia admiten la misma imagen, es decir, la aplicación canónica **no es inyectiva**, salvo en caso de clases unitarias.

Como cada clase es no vacía, ocurre que siempre **es sobreyectiva**, es decir:

$$\forall\, [u] \in A/\mathcal{R}, \exists\ x \in A/\varphi(x) = [u]$$

Vale la siguiente proposición:

$$a \equiv b \iff \varphi(a) = \varphi(b)$$

En el caso de congruencia módulo 3, definida en $\mathbb{Z}$ es $\varphi : \mathbb{Z} \to \mathbb{Z}_3$ tal que $\varphi(x) = [u]$, siendo u el resto de la división de x por 3.

Ejemplo 1.15

Sea en $\mathbb{R}^2$ dos pares ordenados de reales que están relacionados si y sólo si tienen la misma primera componente.

$$\mathcal{R}:\ (a,b) \equiv (a',b') \iff a = a'$$

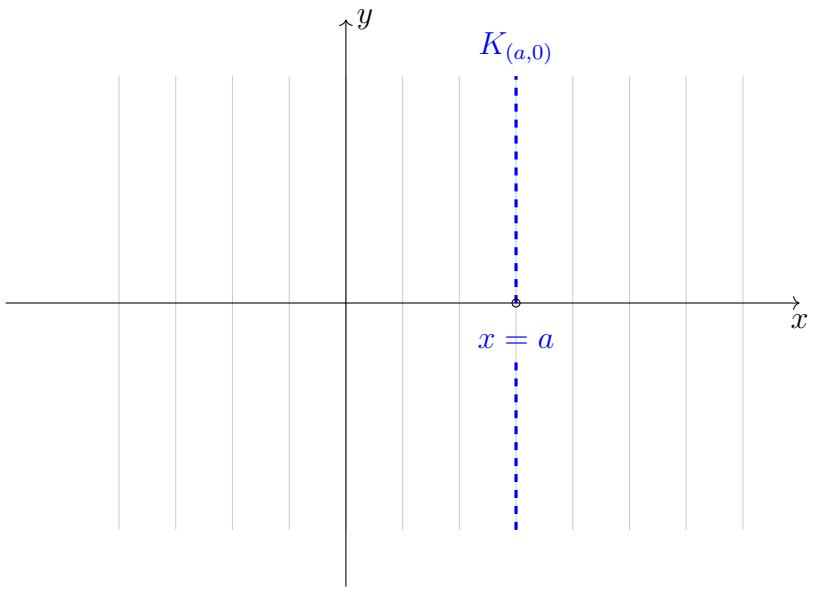
La relación es de equivalencia, y el propósito es caracterizar la aplicación canónica.

Las clases de equivalencia son del tipo: $K_{(a,b)} = \{(x,y)/x = a\}$ (rectas paralelas al eje de ordenadas)

Definir el conjunto cociente requiere un conjunto de índices, y al elegir un único elemento en cada clase, lo tomamos sobre el eje de abscisas, de modo que:

$$\mathbb{R}^2/\mathcal{R} = \{K_{(u,0)}/u \in \mathbb{R}\}$$

Así la función canónica es $\phi : \mathbb{R}^2 \to \mathbb{R}^2/\mathcal{R}$ tal que $\phi(a,b) = K_{(u,0)}$ si $u = a$



La recta vertical por $x = a$ representa a la clase de equivalencia $K_{(a,0)}$, de todos los puntos del plano con la misma primera componente $x = a$.

1.3.5. Composición de funciones

Sean $f : A \to B$ y $g : B \to C$

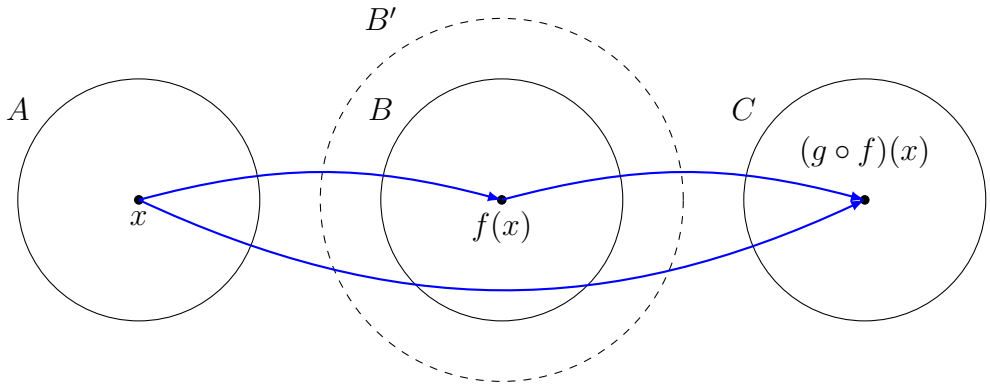


Figura 1.3

El codominio de f es dominio de g, pero es suficiente que el codominio de la primera sea parte del dominio de la segunda, es decir: $B \subset B'$. En la fig. 1.3 se ve gráficamente esta afirmación.

Definición 1.21. Composición de funciones

Composición de las funciones $f : A \to B$ y $g : B \to C$ es la función $g \circ f : A \to C$, tal que: $(g \circ f)(x) = g\,[f(x)] \;\; \forall x \in A$

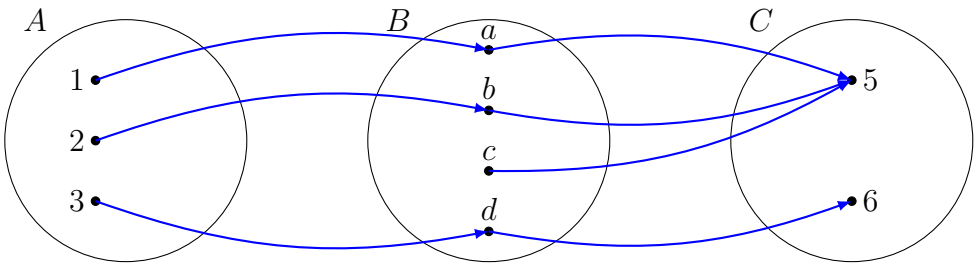
Ejemplo 1.16. Composición de funciones discretas

Sean $A = \{1, 2, 3\}$, $B = \{a, b, c, d\}$, $C = \{5, 6\}$ y las funciones $f : A \to B$ y $g : B \to C$

definidas así:

$$f : \{(1, a), (2, b), (3, d)\}; \quad g = \{(a, 5), (b, 5), (c, 5), (d, 6)\}$$

Resulta: $g \circ f = \{(1, 5), (2, 5), (3, 6)\}$. Ver figura.



Nótese que no coexisten $g \circ f$ y $f \circ g$ ya que, en este caso, el codominio de g es C y el dominio de f es A. Ambas composiciones existen si $C \subset A$.

Ejemplo 1.17. Composición de funciones continuas

Sean:

$$\begin{cases} f : \mathbb{R} \to \mathbb{R} & \text{tal que } f(x) = 2x \\ g : \mathbb{R} \to \mathbb{R} & \text{tal que } g(x) = x^2 \end{cases}$$

1. $g \circ f : \mathbb{R} \to \mathbb{R}$ es: $(g \circ f)(x) = g\left[f(x)\right] = g(2x) = (2x)^2 = 4x^2$
2. $f \circ g : \mathbb{R} \to \mathbb{R}$ es: $(f \circ g)\,(x) = f\left[g(x)\right] = f(x^2) = 2x^2$

Ambas funciones compuestas, a pesar de tener el mismo dominio y codominio, son distintas, por diferir en la ley de asignación.

Definición 1.22 (Funciones iguales)**.** Dos funciones $f : A \to B$ y $g : A \to B$ son iguales si y sólo si para todo x de A se verifica $f(x) = g(x)$

Con relación al ejemplo 1.17 $g \circ f \neq f \circ g$.

Asociatividad de la composición

Si $f : A \to B$, $g : B \to C$ y $h : C \to D$, entonces: $(h \circ g) \circ f = h \circ (g \circ f)$

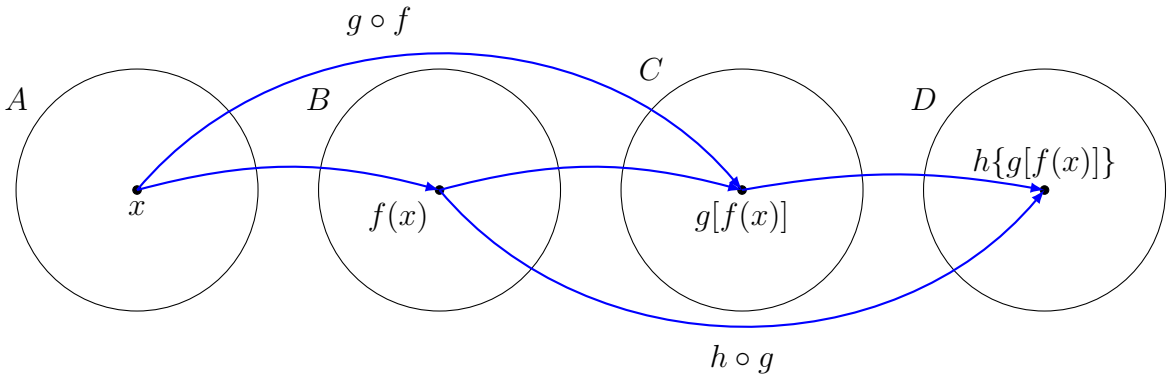


Figura 1.4

En efecto, $\forall x \in A$:

$$\begin{cases} ((h \circ g) \circ f)(x) & = (h \circ g)(f(x)) = h\{g[f(x)]\} \\ (h \circ (g \circ f))(x) & = h((g \circ f)(x)) = h\{g[f(x)]\} \end{cases}$$

De donde resulta la igualdad buscada. Ver fig. 1.4.

Composición de funciones inyectivas

Proposición 1.2

Si $f : A \to B$ y $g : B \to C$ son inyectivas, entonces $g \circ f : A \to C$ es inyectiva.

Prueba 1.2.1

Debemos probar: H) $\forall\, x', x'' \in A$ con $(g \circ f)(x') = (g \circ f)(x'')$, entonces T) $x' = x''$

Por hipótesis y por definición de composición:

$$g[f(x')] = g[f(x'')]$$

por ser g inyectiva:

$$f(x') = f(x'')$$

por ser f inyectiva:

$$x' = x''$$

La composición de funciones inyectivas es inyectiva.

Composición de funciones sobreyectivas

Proposición 1.3

Si $f : A \to B$ y $g : B \to C$ son sobreyectivas, entonces $g \circ f : A \to C$ es sobreyectiva.

Prueba 1.3.1

Hay que probar que $\forall\, z \in C\, \exists\, x \in A$ tal que $(g \circ f)(x) = z$.

Por ser g sobreyectiva: $\forall\, z \in C$, $\exists\, y \in B / g(y) = z$

Ahora bien, dado que $y \in B$, por ser f sobreyectiva $\exists\, x \in A / f(x) = y$

De aquí se deduce que:

$$g[f(x)] = g(y) = z$$

La composición de funciones sobreyectivas es sobreyectiva.

Se sigue de los casos anteriores que, si $f : A \to B$ y $g : B \to C$ son biyectivas, entonces $g \circ f : A \to C$ es biyectiva.

Ejemplo 1.18

Demostrar que si $f : A \to B$ y $g : B \to C$ son tales que $g \circ f : A \to C$ es inyectiva, entonces f es inyectiva.
Prueba 1.3.2. Sean $x', x'' \in A$ tales que $f(x') = f(x'')$, la imagen de este elemento de B por g, es:

$$g[f(x')] = g[f(x'')]$$

ya que cada elemento del dominio B tiene imagen única en C, por definición de función. Por definición de composición

$$(g \circ f)(x') = (g \circ f)(x'')$$

y por ser $g \circ f$ inyectiva, resulta $x' = x''$, en consecuencia f es inyectiva.

Análogamente se demuestra que si la composición de dos aplicaciones es sobreyectiva, la segunda es sobreyectiva.

1.3.6. Funciones inversas

Cabe preguntarse si, para la función $f : A \to B$, la relación inversa es una función. En general la respuesta es negativa, como se ve a través del ejemplo 2, diapositiva 1.9, donde $A = \{-1, 0, 1, 2\}$, $B = \{0, 1, 2, 3, 4\}$ y $f(x) = x^2$

$$f = \{(-1, 1), (0, 0), (1, 1), (2, 4)\}$$

la inversa de esta relación es el subconjunto $B \times A$

$$\{(1, -1), (0, 0), (1, 1), (4, 2)\}$$

se ve que esta relación no es una función de B en A, pues los elementos 2 y 3 del eventual dominio carecen de imágenes en A y además no se cumple la condición de unicidad, ya que 1 tiene dos correspondientes en A.

Sea, en cambio, el siguiente caso $A = \{1, 2, 3\}$, $B = \{a, b, c\}$ y $f(x) = \{(1, a), (2, c), (3, b)\}$. La relación inversa es:

$$g = \{(a, 1), (b, 3), (c, 2)\}$$

es claramente una función de B en A, llamada función inversa de f. La composición

$$g \circ f = \{(1,1),(2,2),(3,3)\} = i_A$$

en donde g es la *inversa izquierda* de f y

$$f \circ g = \{(a,a),(b,b),(c,c)\} = i_B$$

En este caso g es la *inversa derecha* de f

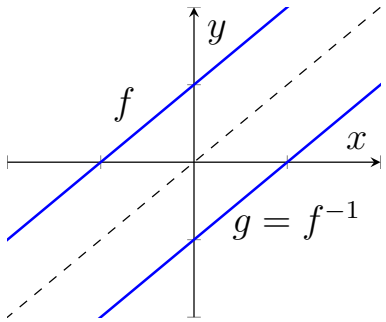
La función $f : A \to B$ admite inversa si y sólo si existe $g : B \to A$ tal que $g \circ f = i_A$ y $f \circ g = i_B$

Ejemplo 1.19. Función inversa

La función $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x + 2$ admite inversa $g : \mathbb{R} \to \mathbb{R}$ tal que $g(x) = x - 2$, pues

$$\begin{cases} (g \circ f)(x) & = g[f(x)] = g(x+2) = x + 2 - 2 = x = i_{\mathbf{R}}(x) \\ (f \circ g)(x) & = f[g(x)] = f(x-2) = x - 2 + 2 = x = i_{\mathbf{R}}(x) \end{cases}$$

La representación cartesiana de dos funciones inversas conduce a gráficos simétricos respecto de la recta a 45°.



Teorema 1.4

Una función admite inversa si y sólo si es biyectiva.

1. Si una función admite inversa, entonces es biyectiva.

   H) $f : A \to B$ es tal que $\exists\, g : B \to A$ siendo $g \circ f = i_A$ y $f \circ g = i_B$

   T) f es biyectiva.

   Prueba 1.4.1. En dos partes.

   a) Inyectividad de f

   Sean $x', x'' \in A / f(x') = f(x'') \in B$.

   La imagen por g es $g[f(x')] = g[f(x'')]$, o, $(g \circ f)(x') = (g \circ f)(x'')$

   siendo $g \circ f = i_A$, se tiene $i_A(x') = i_A(x'')$, es decir $x' = x''$.

Por tanto f es 1-1.

b) f es sobreyectiva

Según definición, hay que probar $\forall\, y \in B, \exists\, x \in A / f(x) = y$

Sea $y \in B$, entonces $y = i_B(y)$, y como $i_B = f \circ g$, se tiene

$$y = (f \circ f)(y), \text{ es decir } y = f[g(x)]$$

por tanto, a expensas de $y \in B$, hemos determinado $x = g(y)$ en A, tal que $f(x) = y$

Siendo f inyectiva y sobreyectiva resulta biyectiva.

2. Si una función es biyectiva, entonces admite inversa.

H) $f : A \to B$ es biyectiva.

T) $\exists\, g : B \to A$ tal que $g \circ f = i_A$ y $f \circ g = i_B$

Prueba 1.4.2. Necesitamos proceder en tres etapas.

a) Definimos $g : B \to A$ mediante $g(y) = x$ si $f(x) = y \quad (1)$

que satisface la definición de función, pues:

I) Todo $y \in B$ proviene de algún $x \in A$

II) La x asociada a y es única, por ser f inyectiva.

En efecto, si x y x' fueran antecedentes distintos de y por f se tendría $x \neq x' \wedge f(x) = f(x') = y$, lo que es absurdo por la inyectividad de f.

b) Hay que probar que $g \circ f = i_A$.

$\forall x \in A$, se tiene, por definición de composición, por (1), y por definición de identidad en A:

$$(g \circ f)(x) = g[f(x)] = g(y) = x = i_A(x)$$

Entonces, por definición de funciones iguales:

$$g \circ f = i_A$$

c) Finalmente, demostramos que $f \circ g = i_B$

Como $f \circ g : B \to B\ \forall\, y \in B$, tenemos, por definición de composición, por (1) y por identidad en B.

$$(f \circ g)(y) = f[g(y)] = f(x) = y = i_B(y)$$

Es decir:

$$f \circ g = i_B$$

Consecuencia

Si $f : A \to B$ es biyectiva, entonces la función $g : B \to A$ a que se refiere el teorema anterior, es única y, además, biyectiva.

Prueba 1.4.3. Si existieran dos funciones g y g' se tendría:

$$g' = g' \circ i_B = g' \circ (f \circ g) = (g' \circ f) \circ g = i_A \circ g = g$$

Por otra parte, como una función que admite inversa es biyectiva, se tiene que $g : B \to A$ es tal que $\exists\, f : A \to B$, siendo $f \circ g = i_B$ y $g \circ f = i_A$. En consecuencia, g es biyectiva

La función g se llama inversa y se denota por f^{-1}.

Ejemplo 1.20

Probar que $f : \mathbb{R} \to (-1, 1)$ definida por $f(x) = \dfrac{x}{1 + |x|}$ admite inversa.

a) f es inyectiva

Sean $x', x'' \in A / f(x') = f(x'')$

$$\frac{x'}{1 + |x'|} = \frac{x''}{1 + |x''|} \implies x' + x'|x''| = x'' + x''|x'| \implies x' = x''$$

O sea, f es 1-1.

b) f es sobreyectiva

Sea $y \in (-1, 1)$. Si $\exists\, x \in \mathbb{R} / f(x) = y$, entonces $\dfrac{x}{1 + |x|} = y$, notar que x y y tienen signos iguales, es decir $\operatorname{sg}(x) = \operatorname{sg}(y)$.

Operando (siendo $|y| < 1$):

$$x = y + y|x| \to x = y + y\, x \operatorname{sg}(x) \to x = y + x\, y \operatorname{sg}(y) \to x - x\, y \operatorname{sg}(y) = y$$

$$\to x(1 - |y|) = y \to x = \frac{y}{1 - |y|}$$

Es decir: $\forall\, y \in (-1, 1), \exists\, x = \dfrac{y}{1 - |y|}$ tal que:

$$f(x) = f\left(\frac{y}{1 - |y|}\right) = \frac{\dfrac{y}{1 - |y|}}{1 - \left|\dfrac{y}{1 - |y|}\right|} = \frac{\dfrac{y}{1 - |y|}}{1 - \dfrac{|y|}{1 - |y|}} = y$$

lo que prueba que f es sobreyectiva.

Por a) y b) resulta que f es biyectiva y en consecuencia admite inversa. La inversa es:

$$f^{-1} : (-1, 1) \to \mathbb{R} / f^{-1}(x) = \frac{x}{1 - |x|}$$

Se puede verificar que $g \circ f = i_{\mathbb{R}}$ y que $f \circ g = i_{(-1,1)}$.

Ejemplo 1.21

La función $f : A \to B$ es inyectiva si y sólo si existe $g : B \to A$ tal que $g \circ f = i_A$.

H) $f : A \to B$ es 1-1;

T) $\exists\, g : B \to A / g \circ f = i_A$

La función f no es necesariamente sobreyectiva. Nos apoyamos en el diagrama de la fig: 1.5.

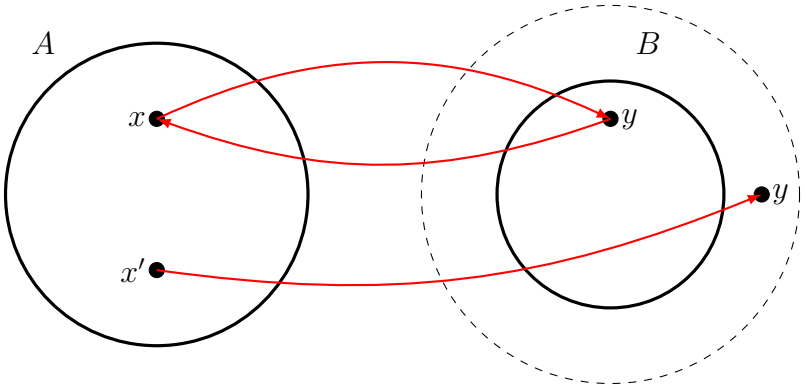


Figura 1.5

Prueba 1.4.4. Definimos una función $g : B \to A$:

$$g(y) \begin{cases} x & \text{si } f(x) = y \\ x' & \text{(cualquier elemento fijo de } A\text{) si } \nexists\, x \in A / f(x) = y \end{cases}$$

De este modo, todo elemento de B tiene su correspondiente en A, y es único por ser f inyectiva. Ahora bien:

$$(g \circ f)(x) = g[f(x)] = g(y) = x = i_A(x)$$

es decir:

$$g \circ f = i_A$$

2. H) $f : A \to B$ es tal que existe $g : B \to A$ de modo que $g \circ f = i_A$;

   T) f es inyectiva.

   Prueba 1.4.5. Sean $x', x'' \in A / f(x') = f(x'')$, entonces

   $$g[f(x')] = g[f(x'')] \implies (g \circ f)(x') = (g \circ f)(x'')$$

   por hipótesis:

   $$i_A(x') = i_A(x'') \implies x' = x''$$

en consecuencia f es 1-1

Resumen de funciones inversas

Definición 1.23. Función inversa

Sea f una función biyectiva con dominio X y rango Y. La **inversa** de f es la función f^{-1} cuyo dominio es Y y rango es X, para los cuales

$$f \circ f^{-1} = f[f^{-1}(x)] = x \quad \forall x \in Y$$

y

$$f^{-1} \circ f = f^{-1}[f(x)] = x \quad \forall x \in X$$

Propiedades:

i) Dominio f^{-1} = rango f;

ii) Rango f^{-1} = dominio f;

iii) $y = f(x)$ equivale a $x = f^{-1}(y)$;

iv) f^{-1} es biyectiva;

v) $(f^{-1})^{-1} = f$;

vi) La inversa de f es única.

1.3.7. Imágenes de subconjuntos del dominio

Sean $f : X \to Y$ y $A \subset X$

Definición 1.24. Imagen de subconjuntos

Imagen del subconjunto $A \subset X$ es el conjunto cuyos elementos son las imágenes de los elementos de A.

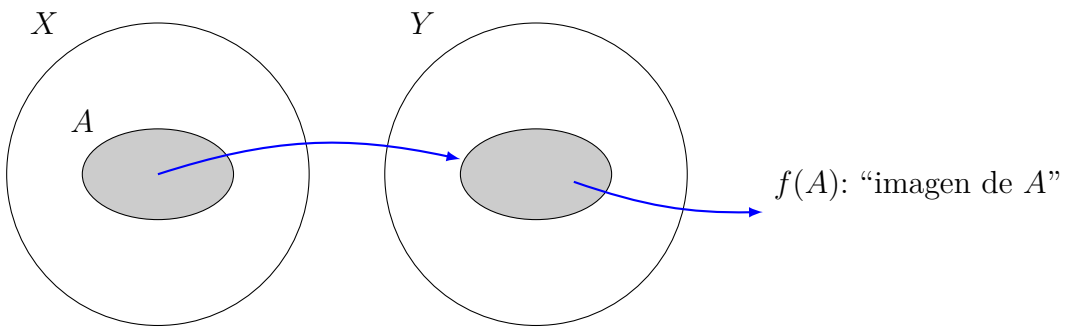


Figura 1.6

$$f(A) = \{f(x)/x \in A\} \text{ o bien } f(A) = \{y \in Y/\exists\, x \in A \wedge f(x) = y\}$$

De acuerdo con la definición: $y \in f(A) \iff \exists\, x \in A/y = f(x)$

Si $A = X$, entonces $f(X)$ es la imagen del dominio por f. Además $f(\varnothing) = \varnothing$. f es sobreyectiva si y sólo si $f(X) = Y$.

Propiedades de la imagen

Sean $f : X \to Y$ y A y B subconjuntos del dominio.

a) Si un subconjunto del dominio es parte de otro, entonces la misma relación vale para sus imágenes. Es decir:

$$f : X \to Y, A \subset B, B \subset X \text{ y } A \subset B \implies f(A) \subset f(B)$$

En efecto, sea

$$z \in f(A) \to \exists\, x \in A / f(x) = z \to \exists\, x \in B / f(x) = z \to z \in f(B)$$

b) La imagen de la unión de dos subconjuntos del dominio, es igual a la unión de sus imágenes. Es decir:

$$f : X \to Y, A \subset X \wedge B \subset X \implies f(A \cup B) = f(A) \cup f(B)$$

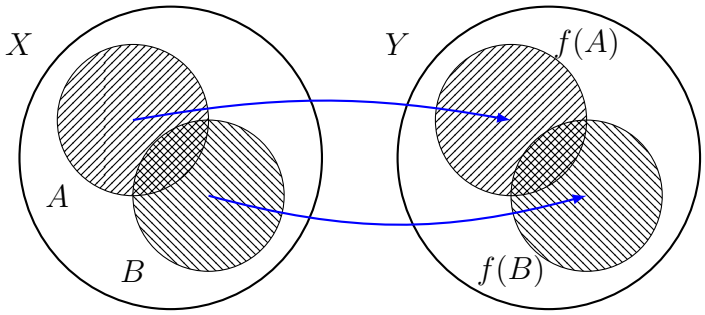


Figura 1.7

c) La imagen de la intersección de dos subconjuntos del dominio está incluida en la intersección de sus imágenes.

$$f : X \to Y, A \subset X \wedge B \subset X \implies f(A \cap B) \subset f(A) \cap f(B)$$

El siguiente ejemplo prueba que no es válida la inclusión en el otro sentido.

Sean $f : \mathbb{Z} \to \mathbb{N} / f(x) = x^2$ y los subconjuntos de $\mathbb{Z}$

$$A = \{-2, -3, 4\} \text{ y } B = \{2, 3, 4, 5\}$$

Se tiene $A \cap B = \{4\}$, $f(A \cap B) = \{16\}$, $f(A) \cap f(B) = \{4, 9, 16\}$

Resulta

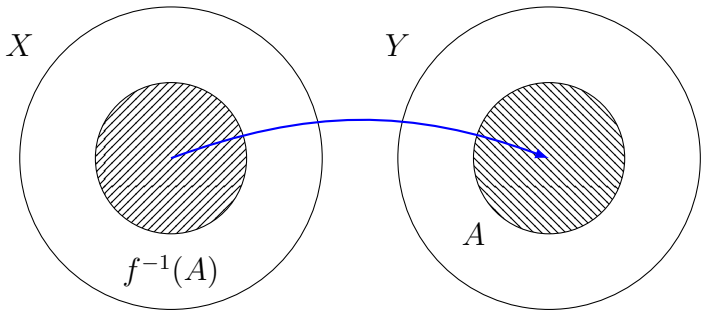
$$f(A \cap B) \subsetneq f(A) \cap f(B)$$

1.3.8. Imágenes inversas de subconjuntos del codominio

Sean $f : X \to Y$ y $A \subset Y$.

Definición 1.25. Preimagen

Imagen inversa o preimagen del subconjunto $A \subset Y$, es el conjunto de los elementos del dominio cuyas imágenes pertenecen a A.



$$f^{-1}(A) = \{x \in X / f(x) \in A\}$$

Es claro que: $x \in f^{-1}(A)$ si, y solo si $f(x) \in A$, es decir, un elemento del dominio pertenece a la preimagen de A si y sólo si su imagen pertenece a A.

Ejemplo 1.22. Preimagen

Sea $f : \mathbb{R} \to \mathbb{R} / f(x) = x^2$. Determinamos las preimágenes de los siguientes subconjuntos del codominio

$$(-\infty, -1], (-1, 1], (-1, 1), [4, 9]$$

I) $f^{-1}(-\infty, -1] = \{x \in \mathbb{R} / f(x) \in (-\infty, -1]\}$

Ahora bien

$$f(x) \in (-\infty, -1) \iff x^2 \leq -1 \iff x \in \varnothing$$

Resulta

$$f^{-1}(-\infty, -1] = \varnothing$$

II) En el segundo caso:

$$x \in f^{-1}(-1, 1] \to f(x) \in (-1, 1] \to x^2 \in (-1, 1] \to -1 < x \leq 1$$

$$\to x^2 \leq 1 \to |x|^2 \leq 1 \to -1 \leq x \leq 1 \to x \in [-1, 1]$$

Entonces $f^{-1}(-1, 1] = [-1, 1]$

III) Se tiene

$$x \in f^{-1}(-1, 1) \to f(x) \in (-1, 1) \to x^2 \in (-1, 1) \to x^2 < 1$$

$$\to |x| < 1 \to -1 < x < 1 \to x \in (-1, 1)$$

Luego $f^{-1}(-1,1) = (-1,1)$

IV) Finalmente

$$x \in f^{-1}[4,9] \to f(x) \in [4,9] \to x^2 \in [4,9] \to 4 \leq x^2 \leq 9$$

$$\to x^2 \geq 4 \wedge x^2 \leq 9 \to |x| \geq 2 \wedge |x| \leq 3$$

$$\to x \in [-3,-2] \vee x \in [2,3] \to x \in [-3,-2] \cup [2,3]$$

Entonces:

$$f^{-1}[4,9] = [-3,-2] \cup [2,3]$$

Propiedades de la preimagen

Sean $f : X \to Y$ y los subconjuntos $A \subset Y$, $B \subset Y$.

a) La preimagen de la unión es la unión de las preimágenes.

$$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$$

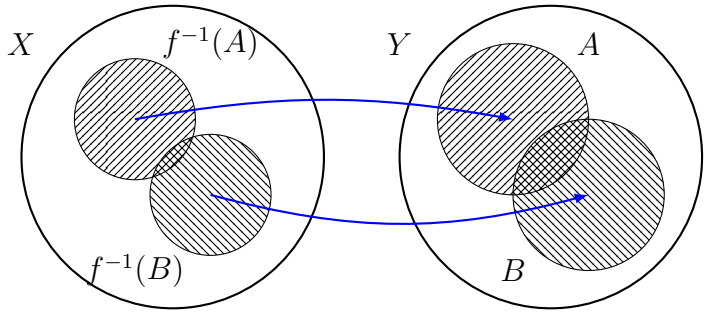


Figura 1.8

$$x \in f^{-1}(A \cup B) \to f(x) \in A \cup B \to f(x) \in A \vee f(x) \in B$$

$$\to x \in f^{-1}(A) \vee x \in f^{-1}(B) \to x \in f^{-1}(A) \cup f^{-1}(B)$$

b) La preimagen de la intersección es igual a la intersección de las preimágenes.

$$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$$

Se tiene

$$x \in f^{-1}(A \cap B) \iff f(x) \in A \cap B \iff f(x) \in A \wedge f(x) \in B$$

$$\iff x \in f^{-1}(A) \wedge x \in f^{-1}(B) \iff x \in f^{-1}(A) \cap f^{-1}(B)$$

b) La imagen inversa del complemento de un subconjunto del codominio es igual al complemento de su preimagen.

$$f^{-1}(A^c) = \left[f^{-1}(A)\right]^c$$

En efecto:

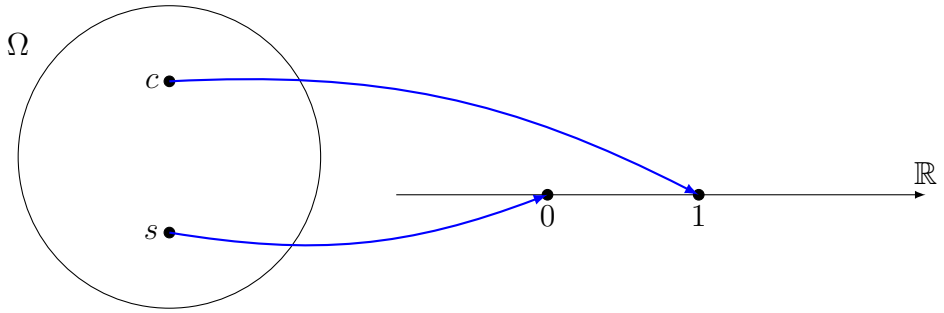
$$x \in f^{-1}(A^c) \iff f(x) \in A^c \iff f(x) \notin A \iff \sim [f(x) \in A]$$

$$\iff \sim \left[x \in f^{-1}(A)\right] \iff x \notin f^{-1}(A) \iff x \in \left[f^{-1}(A)\right]^c$$

Ejemplo 1.23

El conjunto Ω consiste en los posibles resultados que se obtienen al lanzar una moneda, es decir: $\Omega = \{c, s\}$.

Se define $f : \Omega \to \mathbb{R}$ mediante $f(c) = 1,\ f(s) = 0$. El diagrama es:



Determinar $f^{-1}(-\infty, x], \forall\, x \in \mathbb{R}$

Por definición de preimagen $f^{-1}(-\infty, x] = \{w \in \Omega\ f(w) \leq x\}$, entonces

$$f^{-1}(-\infty, x] = \begin{cases} \varnothing & \text{si } x < 0 \\ \{s\} & \text{si } 0 \leq x < 1 \\ \{c, s\} & \text{si } 1 \leq x \end{cases}$$

1.3.9. Restricción y extensión de una función

Definición 1.26. Restricción de una función

Sean $f : X \to Y$, $A \subset X$ y la función $g : A \to Y \mid g(x) = f(x)\, \forall\, x \in A$.

Decimos que g es la restricción de la aplicación f al subconjunto A, y la denotamos $g : f \mid A$.

Definición 1.27. Extensión de una función

Si g es la restricción de f al subconjunto A, entonces $f : X \to Y$ es una extensión de la función g sobre el conjunto X.

Es claro que la restricción es única y la extensión no necesariamente, en efecto si $g : A \to Y$ y $A \subset X$ entonces podemos definir una extensión de g al conjunto X de la siguiente manera:

Sea $y_0 \in Y$, definimos:

$$f : X \to Y \text{ mediante } f(x) = \begin{cases} g(x) & \text{si } x \in A \\ y_0 & \text{si } x \in X - A \end{cases}$$

Capítulo 2

Lógica matemática

La lógica matemática es una disciplina que se ocupa del estudio de los principios y reglas que rigen el razonamiento válido. A través de símbolos y estructuras formales, la lógica nos permite analizar argumentos, deducir conclusiones y establecer conexiones entre proposiciones. A continuación, exploraremos los conceptos básicos de la lógica.

2.1. Lógica proposicional

2.1.1. Proposiciones

Definición 2.1. Proposición

Una *proposición* es una oración que puede ser verdadera o falsa.

Ejemplo 2.1

- Proposiciones verdaderas
  - El sol sale por el este.
  - $2 + 2 = 4$
  - La Tierra gira alrededor del Sol.
- Proposiciones falsas
  - Los unicornios existen
  - $1 + 1 = 3$
  - La luna está hecha de queso verde

Ahora, veamos ejemplos de oraciones que **no son proposiciones**:

Ejemplo 2.2

- Preguntas:

- ¿Cómo estás hoy?
- ¿Qué hora es?
- ¿Dónde está mi libro?

- Mandatos u Órdenes:
  - ¡Cerrá la puerta!
  - Estudiá para el examen.
  - Limpiá tu habitación.
- Expresiones abiertas o incompletas:
  - $x + 3 = 7$ (no es una proposición completa sin asignar un valor a x).
  - "Alguien ganará el premio" (no especifica quién ganará el premio).

Las proposiciones se representan mediante letras (como p, q, r) y se combinan para formar argumentos más complejos.

2.1.2. Operadores lógicos

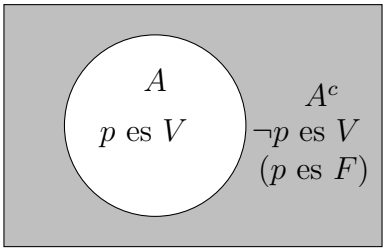
A continuación presentamos varios operadores lógicos y sus correspondientes *tablas de verdad*. En una tabla de verdad se evalúan todos los posibles valores de verdad de las proposiciones componentes y se determina el valor de verdad resultante de la proposición completa.

Negación $\neg$

La negación de una proposición p se denota como $\neg p$ o $\sim p$. Representa la idea de que algo no es verdadero. Por ejemplo, si p es "llueve", entonces $\neg p$ sería "no llueve". Su tabla de verdad es la siguiente:

p	$\neg p$
V	F
F	V

La operación de negación ($\neg$) es análoga a la complementación (^{c}) de la teoría de conjuntos. El paralelismo se construye al considerar la pertenencia de un conjunto como una proposición p, si un elemento pertenece a A, p es verdadero. El complemento A^c contiene todos los elementos que no pertenecen a A, entonces p es falso, es decir $\neg p$ es verdadero.



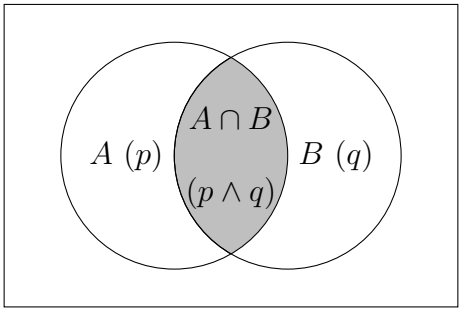
A^c es equivalente a $\neg p$

Conjunción $\wedge$

La conjunción de dos proposiciones p y q se denota como $p \wedge q$. Representa la idea de que ambas proposiciones son verdaderas. Por ejemplo, si p es "es lunes" y q es "tengo una reunión", entonces $p \wedge q$ sería "es lunes y tengo una reunión". Su tabla de verdad es:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

La operación lógica de conjunción es análoga a la intersección de la teoría de conjuntos. La intersección $A \cap B$ contiene solo los elementos que pertenecen a A y a B ($p \wedge q$ es V).



$A \cap B$ equivalente a $p \wedge q$

Disyunción inclusiva $\vee$

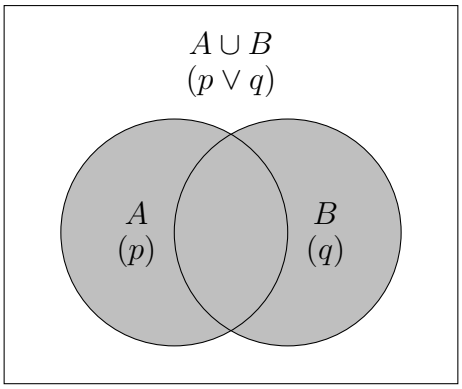
La disyunción de dos proposiciones p y q se denota como $p \vee q$. Representa la idea de que al menos una de las proposiciones es verdadera. Por ejemplo, si p es "estudiaré" y q es "veré una película", entonces $p \vee q$ sería "estudiaré o veré una película". La tabla de verdad correspondiente es:

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

La operación lógica de disyunción es análoga a la unión de la teoría de conjuntos. La unión $A \cup B$ contiene los elementos que pertenecen a A o a B o a ambos, es decir, siempre y cuando un elemento pertenezca a A o a B o a ambos $p \vee q$ será V.

Diferencia simétrica o disyunción excluyente $\oplus$

La diferencia simétrica o disyunción excluyente es verdadera cuando *exactamente una* de las dos proposiciones es verdadera, por ejemplo "p o q pero no ambos". Se denota por $p \oplus q$ o $p \nleftrightarrow q$ o $p \underline{\vee} q$. La tabla de verdad correspondiente es:



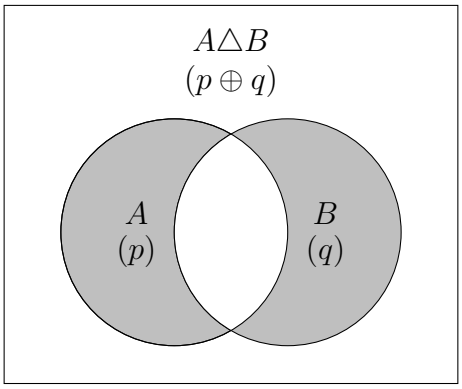
$A \cup B$ equivalente a $p \vee q$

p	q	$p \oplus q$
V	V	F
V	F	V
F	V	V
F	F	F

Ejemplo 2.3. Disyunción excluyente

- "Podés elegir té (p) o café (q)" (implícitamente excluyente, ya que normalmente no se consumen ambas bebidas al mismo tiempo).
- "El interruptor está encendido (p) o apagado (q)" (excluyente, ya que un interruptor solo puede estar en uno de esos dos estados).
- "Ganará la final el equipo local (p) o el equipo visitante (q)" (excluyente, ya que solo uno de los dos equipos puede ganar la final).

Esta operación es análoga a la diferencia simétrica de la teoría de conjuntos. $A \triangle B$ contiene los elementos que pertenecen a A o a B pero no a ambos.



$A \triangle B$ equivalente a $p \oplus q$

Implicación o condicional $\implies$

Si se combinan dos proposiciones por medio de las palabras *"si..., entonces..."* se obtiene un *implicación* o *proposición condicional*. La implicación de una proposición p a otra q se denota como $p \implies q$. Representa la idea de que si p es verdadero, entonces q también debe serlo. Por ejemplo, si p es "estudiaré", entonces q es "aprobaré el examen". La tabla de verdad es:

p	q	$p \implies q$
V	V	V
V	F	F
F	V	V
F	F	V

Tabla 2.1. Tabla de verdad de la implicación

Se observa que $p \implies q$ es verdadero si y sólo si no se da el caso de que p sea verdadero y q falso.

En teoría de conjuntos la inclusión $A \subset B$ es verdadero si y sólo si no existe un elemento que esté en A pero no en B. La conexión entre la implicación lógica y la inclusión de conjuntos se visualiza en la fig. 2.1.

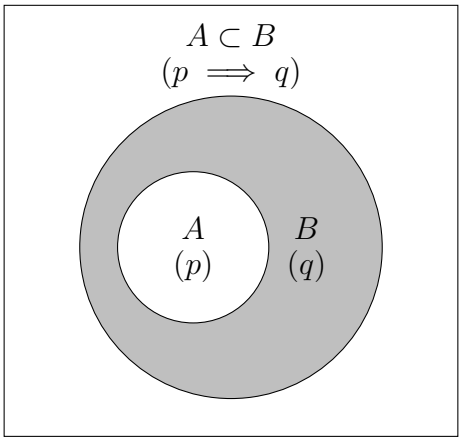


Figura 2.1. $A \subset B$ equivalente a $p \implies q$

Proposiciones. Para algún $x \in U$:

- $p : x \in A$.
- $q : x \in B$.
- La implicación $p \implies q$ se interpreta como: Si x está en A, entonces x está en B.

Paralelismo con la tabla de verdad:

- $p = V$, $q = V$ $(x \in A \land x \in B)$: Corresponde a elementos que están tanto en A como en B, lo cual es consistente con $A \subset B$, la implicación es verdadera.
- $p = V$, $q = F$, $(x \in A \land x \notin B)$: Este caso viola la inclusión $A \subset B$ ya que hay un elemento en A que no está en B, la implicación es falsa.

- $p = F$, $q = V$ ($x \notin A \land x \in B$): Esto es consistente con $A \subset B$, ya que elementos fuera de A pueden estar en B sin violar la inclusión, la implicación es verdadera.
- $p = F, q = F$ ($x \notin A \land x \notin B$): También es consistente con $A \subset B$, ya que elementos que no están en A ni tampoco en B no afectan la inclusión, la implicación es verdadera.

Doble implicación o bicondicional $\iff$

La doble implicación o proposición "si y solo si" se denota como $p \iff q$. Representa la idea de que p es verdadero si y solo si q también lo es. Puede verse, si es verdadera, como cumplimiento en ambos sentidos las implicaciones $p \implies q$ y $q \implies b$. Su tabla de verdad es la siguiente:

p	q	$p \iff q$
V	V	V
V	F	F
F	V	F
F	F	V

Tabla 2.2. Tabla de verdad de la bicondicional

Ejemplo 2.4

Si p es "Es fin de semana" y q es "No tengo clases".

- La implicación $p \implies q$ sería: "Es un fin de semana entonces no tengo clases".
- La implicación recíproca $q \implies p$ sería: "No tengo clases entonces es un fin de semana"
- La bicondicional $p \iff q$ sería: "Es fin de semana si y solo si no tengo clases"

En la teoría de conjuntos, su equivalente es la **igualdad de conjuntos**. Si definimos, igual que antes, p: pertenencia al conjunto A y q: pertenencia al conjunto B, la doble implicación $p \iff q$ se interpreta como: un elemento está en A si y solo si está en B.

2.1.3. Condiciones necesarias y suficientes

Condición necesaria y condición suficiente

Consideremos la tabla de verdad de la implicación, tabla 2.1, que, reescribimos a continuación:

p	q	$p \implies q$
V	V	V
V	F	F
F	V	V
F	F	V

Hay tres casos en que $p \implies q$ es V, y entre ellos hay uno en que p es V, en el cual resulta q verdadera. Es obvio que nos referimos al primer renglón de la tabla, y se tiene que si $p \implies q$ es V y p es V, entonces q es V. Se dice entonces que en antecedente p es *condición suficiente* para el consecuente q.

En cambio, si p es F, nada podemos decir de q, puesto que puede ser V o F, por otra parte, cuando $p \implies q$ es V, si q es V, entonces p puede ser V o F; mas, para que p sea V se necesita que q lo sea. Se dice entonces que q es *condición necesaria* para p.

Resumiendo, si $p \implies q$ es V, entonces p es condición suficiente para q y q es condición necesaria para p, suele expresarse así:

- q si p: condición suficiente;
- p sólo si q: condición necesaria.

Ejemplo 2.5

"Si T es equilátero, entonces T es isósceles"

En este caso:

- p: T es equilátero;
- q: T es isósceles.

p es condición suficiente para q, es decir, que un triángulo sea equilátero es suficiente para asegurar que sea isósceles. Por otra parte, T es equilátero sólo si es isósceles; es decir, que un triángulo sea isósceles es necesario para que sea equilátero.

Condición necesaria y suficiente

Sea ahora la doble implicación $p \iff q$, es decir $(p \implies q) \wedge (q \implies p)$. Si $p \iff q$ es V, entonces $p \implies q$ es V y $q \implies p$, es V. Se tiene, atendiendo a la primera, que p es condición suficiente para q; y, teniendo en cuenta la segunda implicación, ocurre que p es condición necesaria para q.

Es decir, si $p \implies q$ es V, entonces el antecedente p es condición necesaria y suficiente para el consecuente q.

Análogamente, en el caso de la doble implicación verdadera, el consecuente q es también condición necesaria y suficiente para el antecedente p.

Ejemplo 2.6

"T es equilátero si y sólo si T es equiángulo"

Es la doble implicación de las proposiciones:

- p: T es equilátero;
- q: T es equiángulo.

Aquella es V, y cualquiera de las dos proposiciones es condición necesaria y suficiente de la otra.

2.1.4. Tautología y contradicción

Tautología

Definición 2.2. Tautología

Cuando una proposición compuesta, como por ejemplo $(p \implies q) \wedge p \implies q$ es verdadera, independientemente de los valores de verdad de las proposiciones componentes, se dice que tal proposición es una *tautología* o *ley lógica*, es decir, una tautología es una proposición lógica que siempre es verdadera.

En el cálculo proposicional se utilizan las siguientes leyes o tautologías cuyas demostraciones se reduce a la confección de las correspondientes tablas de verdad.

- Identidad

$$p \implies p; \qquad p \iff p$$

$$p \wedge \text{verdadero} = p \quad \text{y} \quad p \vee \text{falso} = p$$

- Ley del tercero excluido

$$p \vee \neg p = V$$

  Una proposición es verdadera o su negación es verdadera.

- No contradicción

$$p \wedge \neg p = F$$

- Involución o doble negación

$$\neg(\neg p) \iff p$$

  La doble negación es equivalente a una afirmación, es decir: "no, no p, equivale a p"

- Idempotencia

$$(p \wedge p) \iff p \quad y \quad (p \vee p) \iff p$$

- Conmutatividad

  a) De la conjunción: $p \wedge q \iff q \wedge p$.

  b) De la disyunción: $p \vee q \iff q \vee p$.

- Asociatividad

  a) De la conjunción: $(p \wedge q) \wedge r \iff p \wedge (q \wedge r)$,

  b) De la disyunción: $(p \vee q) \vee r \iff p \vee (q \vee r)$

- Distributividad

  a) De la conjunción respecto de la disyunción:

$$p \vee (q \wedge r) \iff (p \wedge r) \vee (q \wedge r)$$

b) De la disyunción respecto de la conjunción:

$$(p \wedge (q \vee r)) \iff (p \vee r) \wedge (q \vee r)$$

c) De la implicación respecto de la disyunción

$$(p \implies q \vee r) \iff ((p \implies q) \vee (p \implies r))$$

d) De la implicación respecto de la conjunción

$$(p \implies q \wedge r) \iff ((p \implies q) \wedge (p \implies r))$$

- Leyes de De Morgan

a) La negación de una disyunción es equivalente a la conjunción de las negaciones:

$$\neg(p \vee q) \iff \neg p \wedge \neg q$$

b) La negación de una conjunción es equivalente a la disyunción de las negaciones.

$$\neg(p \wedge q) \iff \neg p \vee \neg q$$

- Leyes de absorción total

1. Primera forma:
$$p \vee (p \wedge q) \iff p$$
2. Segunda forma:
$$p \wedge (p \vee q) \iff p$$

Si p es verdadero (o falso) ambos miembros son verdaderos (o falsos) independientemente de q.

- Leyes de absorción parcial

1. $p \vee (\neg p \wedge q) \iff p \vee q$
2. $p \wedge (\neg p \vee q) \iff p \wedge q$

La mayoría de estas leyes lógicas tienen sus análogas en teoría de conjuntos, algunas de las cuales se listan en la tabla 2.3.

Contradicción

Una contradicción es una proposición lógica que siempre es falsa, sin importar los valores de verdad de sus componentes. Es decir, es una fórmula que es falsa en todas las interpretaciones posibles.

Ejemplos de contradicciones:

- Conjunción de una proposición y su negación:

$$p \wedge \neg p$$

- Negación de una tautología:

$$\neg\,(p \vee \neg p)$$

N°	Ley	Lógica	Conjuntos
1	Identidad	$p \implies p$ $p \iff p$ $p \wedge \mathrm{V} = p$ $p \vee \mathrm{F} = p$	$A = A$ $A \cap U = A$ $A \cup \emptyset = A$
2	Tercero excluido	$p \vee \neg p = \mathrm{V}$	$A \cup A^c = U$
3	No contradicción	$p \wedge \neg p = \mathrm{F}$	$A \cap A^c = \emptyset$
4	Involución	$\neg(\neg p) \iff p$	$(A^c)^c = A$
5	Idempotencia	$p \wedge p \iff p$ $p \vee p \iff p$	$A \cap A = A$ $A \cup A = A$
6	Conmutatividad	$p \wedge q \iff q \wedge p$ $p \vee q \iff q \vee p$	$A \cap B = B \cap A$ $A \cup B = B \cup A$
7	Asociatividad	$(p \wedge q) \wedge r \iff p \wedge (q \wedge r)$ $(p \vee q) \vee r \iff p \vee (q \vee r)$	$(A \cap B) \cap C = A \cap (B \cap C)$ $(A \cup B) \cup C = A \cup (B \cup C)$
8	Distributividad	$p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
9	Leyes de De Morgan	$\neg(p \vee q) \iff \neg p \wedge \neg q$ $\neg(p \wedge q) \iff \neg p \vee \neg q$	$(A \cup B)^c = A^c \cap B^c$ $(A \cap B)^c = A^c \cup B^c$
10	Ley de absorción	$p \vee (p \wedge q) \iff p$ $p \wedge (p \vee q) \iff p$	$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$

Tabla 2.3. Paralelismo entre las leyes lógicas y las de conjuntos.

2.1.5. Funciones booleanas

En lógica simbólica, las *funciones booleanas* son aquellas que toman uno o más valores de verdad (verdadero o falso) como entrada y producen un único valor de verdad como salida. Estas funciones se construyen utilizando operadores lógicos homónimos, que son:

- **Conjunción** (AND): Representada por $\wedge$ o $\cdot$. Es verdadera solo si ambas proposiciones de entrada son verdaderas.
- **Disyunción** (OR): Representada por $\vee$ o $+$. Es verdadera si al menos una de las proposiciones de entrada es verdadera.
- **Negación** (NOT): Representada por $\neg$ o una barra sobre la proposición. Invierte el valor de verdad de la proposición.

A partir de estos operadores básicos, podemos construir funciones booleanas más complejas. Algunas de las funciones booleanas más comunes son:

1. **Función Identidad**:
   - Definición: La salida es igual a la entrada.
   - Expresión: $f(p) = p$
   - Ejemplos:
     a) Si p es verdadero, entonces $f(p)$ es verdadero.
     b) Si p es falso, entonces $f(p)$ es falso.
2. **Función Constante**:

- Definición: La salida siempre es el mismo valor de verdad, independientemente de la entrada.
- Expresión:
  - $f(p) = 1$ (Función constante verdadera)
  - $f(p) = 0$ (Función constante falsa)
- Ejemplos:
  a) Si p es verdadero, $f(p)$ sigue siendo verdadero (para la función constante verdadera) o falso (para la función constante falsa).
  b) Si p es falso, $f(p)$ sigue siendo verdadero (para la función constante verdadera) o falso (para la función constante falsa).

3. **Función Negación**:
   - Definición: La salida es la negación de la entrada.
   - Expresión: $f(p) = \neg p$
   - Ejemplos:
     a) Si p es verdadero, entonces $f(p)$ es falso.
     b) Si p es falso, entonces $f(p)$ es verdadero.
4. **Función Conjunción**:
   - Definición: La salida es verdadera solo si todas las entradas son verdaderas.
   - Expresión: $f(p, q) = p \wedge q$
   - Ejemplos:
     a) Si p es verdadero y q es verdadero, entonces $f(p, q)$ es verdadero.
     b) Si p es verdadero y q es falso, o viceversa, o ambos son falsos, entonces $f(p, q)$ es falso.
5. **Función Disyunción**:
   - Definición: La salida es verdadera si al menos una de las entradas es verdadera.
   - Expresión: $f(p, q) = p \vee q$
   - Ejemplos:
     a) Si p es verdadero o q es verdadero, o ambos son verdaderos, entonces $f(p, q)$ es verdadero.
     b) Si p es falso y q es falso, entonces $f(p, q)$ es falso.
6. **Función Implicación**:
   - Definición: La salida es falsa solo si la primera entrada es verdadera y la segunda es falsa
   - Expresión: $f(p, q) = p \implies q$

- Ejemplos:
  a) Si p es verdadero y q es verdadero, entonces $f(p, q)$ es verdadero.
  b) Si p es verdadero y q es falso, entonces $f(p, q)$ es falso.
  c) Si p es falso, independientemente del valor de q, $f(p, q)$ es verdadero

7. **Función Equivalencia** (Bicondicional):
   - Definición: La salida es verdadera si ambas entradas tienen el mismo valor de verdad
   - Expresión: $f(p, q) = p \iff q$
   - Ejemplos:
     a) Si p es verdadero y q es verdadero, o si p es falso y q es falso, entonces $f(p, q)$ es verdadero.
     b) Si p es verdadero y q es falso, o viceversa, entonces $f(p, q)$ es falso.

2.1.6. Proposiciones equivalentes

Al unir dos proposiciones cualesquiera por medio de la frase *"si y sólo si"*, (cuyo símbolo es $\iff$) se obtiene una proposición compuesta que se llama *equivalencia*. Las proposiciones conectadas de esta manera reciben los nombres de *miembro izquierdo* y *miembro derecho* de la equivalencia. Al afirmar la equivalencia de las proposiciones, se excluye la posibilidad de que una sea verdadera y la otra falsa; por lo tanto, una equivalencia es verdadera si sus miembros izquierdo y derecho son o bien ambos verdaderos o bien ambos falsos; en caso contrario la equivalencia es falsa.

Dos proposiciones son *equivalentes* si y solo si tienen el mismo valor de verdad en todas las posibles combinaciones de valores de verdad de sus proposiciones componentes. Es decir, sus tablas de verdad son idénticas.

La equivalencia lógica captura la idea de que dos proposiciones, aunque expresadas de manera diferente, representan la misma información desde el punto de vista lógico. Si dos proposiciones son equivalentes, podemos sustituir una por la otra en cualquier contexto lógico sin alterar el significado o la validez del razonamiento.

Ejemplo 2.7. Proposiciones equivalentes

Dada la proposición compuesta:

"x es un número positivo si, y solo si, $3x$ es un número positivo"

De x *es un número positivo* (p) se sigue que $3x$ *es un número positivo* (q), (en símbolos $p \implies q$) y, recíprocamente, de $3x$ *es un número positivo* se sigue que x *es un número positivo* ($q \implies p$). Las condiciones de que x sea un número positivo y que $3x$ sea un número positivo son equivalentes entre sí ($p \iff q$).

La condición de ser x un número positivo es *necesaria y suficiente* para que $3x$ sea un número positivo, recíprocamente, para que x sea un número positivo es necesario y suficiente que $3x$ lo sea, es decir, cada una de las proposiciones representa una

condición necesaria y suficiente para la otra.

Verificación de equivalencia

La forma más directa de comprobar si dos proposiciones son equivalentes es construir sus tablas de verdad y compararlas. Si las columnas de resultados finales son idénticas, entonces las proposiciones son equivalentes. Utilizaremos el símbolo de equivalencia "≡"

Ejemplo 2.8

Probar la ley de De Morgan: $\neg\,(p \wedge q) \equiv \neg p \vee \neg q$

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
V	V	V	F	F	F	F
V	F	F	V	F	V	V
F	V	F	V	V	F	V
F	F	F	V	V	V	V

Se observa que la cuarta columna, de $\neg\,(p \wedge q)$, y la última columna, de $\neg p \vee \neg q$ son idénticas, por lo tanto estas proposiciones son equivalentes.

Ejemplo 2.9. Implicación material

Probar que: $p \implies q \equiv \neg p \vee q$

p	q	$p \implies q$	$\neg p$	$\neg p \vee q$
V	V	V	F	V
V	F	F	F	F
F	V	V	V	V
F	F	V	V	V

Se observa que la tercera columna, de $p \implies q$, y la última columna, de $\neg p \vee q$ son idénticas, por lo tanto estas proposiciones son equivalentes. Esta equivalencia se conoce como *ley de implicación material*.

El concepto de equivalencia lógica es fundamental en la simplificación de expresiones lógicas, en la demostración de teoremas y en la resolución de problemas lógicos. Nos permite manipular y transformar proposiciones manteniendo su significado original, lo que facilita el análisis y la comprensión de argumentos lógicos complejos.

2.1.7. Álgebra de proposiciones

El álgebra de proposiciones nos proporciona un marco formal para combinar y manipular proposiciones utilizando operadores lógicos, lo que nos permite analizar y razonar sobre argumentos y demostraciones de manera rigurosa.

Ejemplo 2.10. Simplificación de expresiones lógicas

Simplifica la siguiente expresión lógica utilizando las leyes del álgebra de proposiciones:

$$(\neg p \land q) \lor (p \land \neg q) \lor (p \land q)$$

Solución

$$\begin{array}{ll}
(\neg p \land q) \lor (p \land \neg q) \lor (p \land q) & \\
\equiv (\neg p \land q) \lor [(p \land \neg q) \lor (p \land q)] & \text{agrupando términos} \\
\equiv (\neg p \land q) \lor [p \land (\neg q \lor q)] & \text{distributividad} \\
\equiv (\neg p \land q) \lor p & \text{ley del tercero excluido} \\
\equiv p \lor (\neg p \land q) & \text{conmutatividad de la disyunción} \\
\equiv p \lor q & \text{ley de absorción}
\end{array}$$

$$(\neg p \land q) \lor (p \land \neg q) \lor (p \land q) \equiv p \lor q$$

Ejemplo 2.11. Demostración de equivalencia

Demuestra que las siguientes expresiones son equivalentes:

$$p \implies (q \lor r) \equiv (p \land \neg q) \implies r$$

Solución

$$\begin{array}{ll}
p \implies (q \lor r) & \\
\equiv \neg p \lor (q \lor r) & \text{implicación material} \\
\equiv (\neg p \lor q) \lor r & \text{asociatividad} \\
\equiv \neg\,(p \land \neg q) \lor r & \text{De Morgan} \\
\equiv (p \land \neg q) \implies r & \text{implicación material}
\end{array}$$

2.1.8. Proposiciones condicionales

Cuando tenemos una proposición en forma de implicación (como $p \implies q$, "si p, entonces q"), podemos derivar tres proposiciones adicionales, estas son la recíproca, la proposición contraria (o la negación de la proposición original) y la proposición contrarrecíproca.

1. **Proposición recíproca** ($q \implies p$): Se forma al *invertir la implicación* de una proposición dada. Ejemplo con el teorema de Pitágoras:
   - Este teorema establece que: "en un triángulo rectángulo, la suma de los cuadrados de los catetos es igual al cuadrado de la hipotenusa" ($p \implies q$).
   - La proposición recíproca afirmaría que: "si la suma de los cuadrados de los catetos es igual al cuadrado de la hipotenusa, entonces el triángulo es rectángulo" ($q \implies q$).
2. **Proposición Contraria** ($\neg p \implies \neg q$): Se obtiene al reemplazar tanto el antecedente como el consecuente de la proposición original por sus negaciones. Por ejemplo:

- Proposición original: “Si llueve, entonces la calle estará mojada” ($p \implies q$)
- Contraria:“Si no llueve, entonces la calle no estará mojada” ($\neg p \implies \neg q$).

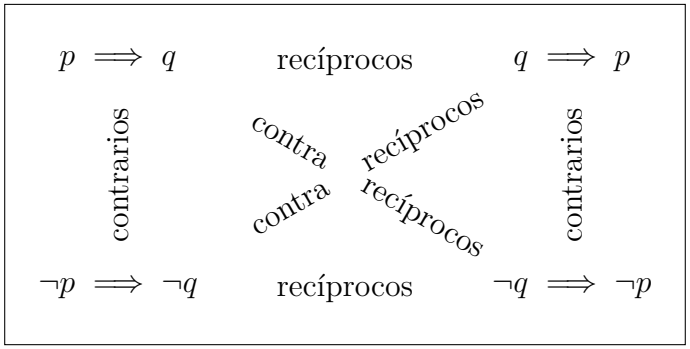
3. **Proposición Contrarrecíproca** ($\neg q \implies \neg p$): La contrarrecíproca es el resultado de intercambiar el antecedente y el consecuente en la proposición contraria. Por ejemplo:
   - Proposición original: “Si estudio, entonces saco buenas notas” ($p \implies q$)
   - Proposición contraria: “Si no estudio, entonces no saco buenas notas” ($\neg p \implies \neg q$).
   - Contrarrecíproca: “Si no saco buenas notas, entonces no estoy estudiando” ($\neg q \implies \neg p$).

Estas tres proposiciones están relacionadas entre sí y nos ayudan a explorar diferentes aspectos de una implicación. Es importante entenderlas para razonar correctamente en lógica y matemáticas.

Resumen, en símbolos:

- Implicación: $p \implies q$
- Recíproca: $q \implies p$
- Contraria: $\neg p \implies \neg q$
- Contrarrecíproca: $\neg q \implies \neg p$

Las cuatro implicaciones anteriores se llaman conjugadas, y cualquiera de ellas puede tomarse como directa. El siguiente esquema nos proporciona una relación que las vincula:



Es fácil verificar que las implicaciones contrarrecíprocas son equivalentes, es decir, las siguientes bicondicionales son tautologías:

$$(p \implies q) \iff (\neg q \implies \neg p)$$

$$(q \implies p) \iff (\neg p \implies \neg q)$$

Si la implicación directa es V, también lo es la contrarrecíproca, y no podemos afirmar la verdad de la recíproca o de la contraria. Pero, si son verdaderos un condicional y su recíproco o contrario, entonces son verdaderos los cuatro, y las proposiciones antecedente y consecuente son equivalentes.

Demostración matemática

Se presenta continuamente la necesidad de demostrar la verdad de

$$\underset{\text{Hipótesis}}{p} \implies \underset{\text{Tesis}}{q}$$

y, de acuerdo con lo expuesto, se presentan dos métodos:

I) *Directo*: Si $p = F$, nada hay que probar, pues en este caso $p \implies q$ es V. Si p es V hay que establecer que el valor de verdad de q es V.

II) *Indirecto*:

a) Se utiliza la *contrarrecíproca*, es decir, demostrar la verdad de $p \implies q$ es equivalente a probar la verdad de $\neg q \implies \neg p$.

b) Por *contradicción* o *reducción al absurdo*:

1) Se supone que la tesis (q) es falsa, es decir, se parte del caso $p = V$ y $q = F$;

2) Se derivan otras afirmaciones utilizando reglas lógicas;

3) Si se llega a una contradicción (por ejemplo $q \wedge \neg q = V$), se concluye que $q = V$.

Nota: También se tiene el *método de inducción* del que se hablará en la sección 2.3.2, pág. 69.

Negación de una implicación

Las proposiciones $p \implies q$ y $\neg(p \wedge \neg q)$ son equivalentes, por implicación material y ley de De Morgan:

$$p \implies q \equiv \neg p \vee q \equiv \neg\left(p \wedge \neg q\right)$$

En consecuencia, la negación de la primera equivale a la negación de la segunda, es decir:

$$\neg(p \implies q) \iff \neg[\neg(p \wedge \neg q)]$$

y por la propiedad de *involución* se tiene:

$$\neg(p \implies q) \iff (p \wedge \neg q)$$

Es decir, la negación de una implicación no es una implicación, sino la conjunción del antecedente con la negación del consecuente.

Ejemplo 2.12. Negación de una implicación $\neg(p \implies q) \iff (p \wedge \neg q)$

Sean las implicaciones:

I) Si hoy es lunes (p), entonces mañana es miércoles (q).

Cuya negación es: "Hoy es lunes (p) y mañana no es miércoles ($\neg q$)"

II) "Si estudias para el examen (p), entonces obtendrás una buena calificación (q)"

La negación de esta afirmación sería: "Estudias para el examen (p), pero no obtienes una buena calificación ($\neg q$)"

III) "Si un número es divisible por 4, entonces también es divisible por 2" ($p \implies q$).

La negación es: "Hay un número que es divisible por 4, pero no es divisible por 2" ($p \wedge \neg q$).

2.1.9. Concepto de argumento y razonamiento deductivo válido

Argumento

Definición 2.3. Argumento

Un *argumento* es una secuencia de proposiciones (llamadas premisas) que pretenden respaldar o justificar una proposición final (llamada conclusión). Un argumento se presenta usualmente de la siguiente forma:

$$p_1 \wedge p_2 \wedge \cdots \wedge p_n \implies q$$

- p_1: premisa 1
- p_2: premisa 2
- $\vdots$
- p_n: premisa n
- Por lo tanto, q: conclusión.

Razonamiento deductivo válido

Definición 2.4

Un argumento se considera un *razonamiento deductivo válido* si, y solo si, es imposible que todas sus premisas sean verdaderas y su conclusión sea falsa. En otras palabras, la verdad de las premisas garantiza la verdad de la conclusión. La validez de un argumento depende únicamente de su forma lógica, no del contenido específico de las proposiciones.

El razonamiento deductivo válido es un proceso lógico en el que, a partir de premisas o afirmaciones, se llega a una conclusión de manera irrefutable. Un razonamiento es válido si la conclusión sigue necesariamente de las premisas, siguiendo las reglas de la lógica.

Por ejemplo:

$$\begin{array}{l} p \implies q \\ p \\ \hline q \end{array}$$

Si tenemos las premisas ($p \Rightarrow q$) y (p), entonces la conclusión (q) es válida. Esta es la ley del *modus ponens* de la que se hablará más en la pág. 62.

Relación entre argumento y razonamiento deductivo válido

Un argumento puede ser válido o inválido. Un argumento válido es aquel en el que la conclusión se sigue necesariamente de las premisas, es decir, representa un razonamiento deductivo válido. Por otro lado, un argumento inválido es aquel en el que la conclusión no se sigue lógicamente de las premisas, incluso si las premisas son verdaderas.

Ejemplo 2.13. Argumento válido

$$\begin{array}{l} p \implies q \\ p \\ \hline q \end{array}$$

- *Premisa 1*: Si llueve, entonces la calle está mojada ($p \implies q$).
- *Premisa 2*: Está lloviendo (p)
- *Conclusión*: Por lo tanto, la calle está mojada (q).

Este argumento es válido porque si las dos premisas son verdaderas, la conclusión también debe ser verdadera.

Ejemplo 2.14. Argumento inválido

$$\begin{array}{l} p \implies q \\ q \\ \hline p \end{array}$$

- *Premisa 1*: Si llueve, entonces la calle está mojada ($p \implies q$)
- *Premisa 2*: La calle está mojada (q).
- *Conclusión*: Por lo tanto, está lloviendo (p).

Este argumento es inválido porque la calle podría estar mojada por otras razones además de la lluvia. Aunque las premisas sean verdaderas, la conclusión no se sigue necesariamente de ellas.

El razonamiento deductivo válido es esencial en la lógica matemática y en muchas otras disciplinas, ya que nos permite construir argumentos sólidos y confiables. Al utilizar argumentos válidos, podemos estar seguros de que si nuestras premisas son verdaderas, nuestra conclusión también lo será.

2.1.10. Reglas de Inferencia

Las *reglas de inferencia* son patrones lógicos fundamentales que nos permiten deducir nuevas proposiciones a partir de un conjunto de proposiciones dadas (premisas). Son herramientas esenciales en la construcción de argumentos válidos y en la demostración de teoremas en lógica matemática.

Son como las reglas de un juego. El juego se juega con proposiciones o fórmulas lógicas. Se empieza con conjuntos de fórmulas que se denominan *premisas*. El objeto del juego es uti-

lizar las reglas de inferencia de manera que conduzcan a otras fórmulas que se denominan *conclusiones*. El paso lógico de las premisas a la conclusión es una *deducción*.

La conclusión que se obtiene se dice que es una *consecuencia lógica* de las premisas si cada paso que se da para llegar a la conclusión está permitido por una regla.

La idea de inferencia es: *de premisas verdaderas se obtienen sólo conclusiones verdaderas*.

Características:

- *Validez*: Una regla de inferencia es válida si, siempre que las premisas sean verdaderas, la conclusión deducida también es verdadera.
- *Forma lógica*: Las reglas de inferencia se basan en la forma lógica de las proposiciones, no en su contenido específico. Esto significa que se pueden aplicar a cualquier conjunto de proposiciones que tengan la misma estructura lógica, independientemente de su significado.
- *Deducción*: Las reglas de inferencia nos permiten realizar deducciones, es decir, pasar de proposiciones conocidas a nuevas proposiciones que se siguen lógicamente de ellas.

a) Ley del *modus ponens*:

$$(p \implies q) \wedge p \implies q$$

Se utiliza para derivar una conclusión a partir de una afirmación condicional y su antecedente.

Notación clásica:

$$\begin{array}{l} p \implies q \\ \underline{p \qquad\qquad} \\ q \end{array}$$

Ejemplo 2.15. Modus ponens

Supongamos que tenemos la afirmación:

$p \implies q$: "Si sigues comiendo de esa manera, entonces no lograrás tu peso ideal"

- Si se verifica p: "sigues comiendo de esa manera"
- entonces q: "no lograrás a tu peso ideal"

b) Ley del *modus tollens*:

$$(p \implies q) \wedge \neg q \implies \neg p$$

Es otra regla de inferencia que se utiliza para derivar una conclusión negando el consecuente de una afirmación condicional.

Notación clásica:

$$\begin{array}{l} p \implies q \\ \neg q \\ \hline \neg p \end{array}$$

Ejemplo 2.16. Modus tollens

Supongamos que tenemos la afirmación:

$p \implies q$: "Si llueve, entonces la calle estará mojada"

- Si observamos $\neg q$: "la calle no está mojada"
- entonces podemos concluir $\neg p$ "no está lloviendo"

c) Ley del silogismo hipotético:

$$[(p \implies q) \wedge (q \implies r)] \implies (p \implies r)$$

Nos permite combinar dos afirmaciones condicionales para obtener una nueva afirmación condicional

Notación clásica:

$$\begin{array}{l} p \implies q \\ q \implies r \\ \hline p \implies r \end{array}$$

Ejemplo 2.17. Silogismo hipotético

Supongamos que tenemos las afirmaciones:

- $p \implies q$: Si no me despierto a hora, entonces no voy a ir a trabajar;
- $q \implies r$: Si no voy a trabajar, entonces no me pagan mi sueldo.
- Por lo tanto, $p \implies r$: si no me despierto a hora, entonces no me van a pagar mi sueldo.

Ejemplo 2.18

1. Justificar la validez del razonamiento:

$$\begin{array}{ll} \textit{Premisa } 1: & p \implies q \\ \textit{Premisa } 2: & \neg r \implies \neg q \\ \textit{Premisa } 3: & \neg(\neg p \wedge \neg t) \\ \textit{Premisa } 4: & t \implies s \\ \textit{Premisa } 5: & \neg r \\ \hline \textit{Conclusión}: & s \end{array}$$

2. Justificar la validez del razonamiento cuyas premisas son:

- *Premisa* 1: Hoy llueve o hace frío,
- *Premisa* 2: Hoy llueve o no hace frío,
- *Conclusión*: Hoy llueve.

Consideremos p: "hoy llueve"; q: "hace frío", entonces:

$$\frac{\begin{array}{l} p \vee q \\ p \vee \neg q \end{array}}{p}$$

2.1.11. Falacias formales

Falacias lógicas

Una *falacia* es un razonamiento incorrecto pero con apariencia de correcto.

$$\textbf{Falacias} \begin{cases} \text{Formales} \\ \text{Informales} \begin{cases} \text{Ambigüedad} \begin{cases} \text{Por equívoco} \\ \text{Anfibología} \end{cases} \\ \text{Materiales} \begin{cases} \text{Datos insuficientes} \\ \text{Pertinencia} \end{cases} \end{cases} \end{cases}$$

$$\text{Datos insuf.} \begin{cases} \text{Generalización} \\ \text{inadecuada} \\ \text{Falsa prueba} \\ \text{Falsa causa} \end{cases} \qquad \text{Pertinencia} \begin{cases} \text{Ad hominen} \\ \text{Ad baculum} \\ \text{Ad populum} \\ \text{Ad verecundiam} \\ \text{Ad ignorantiam} \\ \text{Tu quoque} \end{cases}$$

Algunos ejemplos:

- **Anfibología**: ambigüedad estructural. *"Todo hombre ama a una mujer, Romeo ama a Julieta, luego todo hombre ama a Julieta"*
- **Datos insuficientes**: *"Todos los hombres son iguales"*.
- **Falsa causa y prueba**: *"El fumar es malo para la salud. Me duele un pie. Eso es por el tabaco"*.
- **Ad hominem**: se ataca a la persona y no al argumento.
- **Ad baculum**: Falsas autoridad. *"Porque lo digo yo!"*
- **Ad populum**: *"Todo un pueblo no puede equivocarse"*
- **Ad verecundiam**: *"La raíz de 2 es irracional, porque lo dijo Euclides"*
- **Ad ignorantiam**: *"Nadie ha demostrado que hay vida en otros planetas, luego no la hay"*
- **Tu quoque**: *"Tu también"* o *"tu más"*.

Falacias formales

Definición 2.5. Falacias formales

Las *falacias formales* son errores de razonamiento que ocurren debido a una estructura lógica incorrecta en un argumento, independientemente de la verdad o falsedad de las proposiciones involucradas. Es decir, el problema radica en la forma del argumento, no en su contenido.

A pesar de parecer convincentes a primera vista, las falacias formales violan las reglas de inferencia válidas, lo que las hace inválidas desde el punto de vista lógico. Identificar y evitar estas falacias es crucial para construir argumentos sólidos y confiables.

Veamos algunos ejemplos comunes de falacias formales:

1. **Afirmación del consecuente**
   - Estructura:
   $$\begin{array}{l} p \implies q \\ q \\ \hline p \end{array}$$
   - Ejemplo:
     - Si llueve, entonces la calle está mojada.
     - La calle está mojada.
     - Por lo tanto, está lloviendo. (Incorrecto, la calle podría estar mojada por otras razones)
2. **Negación del antecedente**
   - Estructura:
   $$\begin{array}{l} p \implies q \\ \neg p \\ \hline \neg q \end{array}$$
   - Ejemplo:
     - Si estudio mucho, aprobaré el examen
     - No estudié mucho
     - Por lo tanto, no aprobaré el examen (Incorrecto, podría aprobar por otras razones).
3. **Falacia del término medio no distribuido**
   - Estructura:
     - Premisa 1: Todo A es B
     - Premisa 2: Todo C es B
     - Conclusión: Por lo tanto, todo A es C
   - Ejemplo:

- Todos los perros son mamíferos
- Todos los gatos son mamíferos
- Por lo tanto, todos los perros son gatos (Incorrecto)

4. **Falacia de la división**
   - Estructura:
     - Premisa 1: El todo tiene la propiedad x
     - Conclusión: Por lo tanto, cada parte del todo tiene la propiedad x
   - Ejemplo
     - El equipo de fútbol es el mejor del mundo
     - Por lo tanto, cada jugador es el mejor en su posición (Incorrecto)

Reconocer las falacias formales es esencial para evaluar críticamente los argumentos y evitar ser engañado por razonamientos que parecen válidos pero que en realidad son lógicamente defectuosos. Al estudiar y comprender estas falacias, podemos fortalecer nuestras habilidades de razonamiento y construir argumentos más sólidos y persuasivos.

2.2. Lógica predicativa

La lógica predicativa, también conocida como lógica de primer orden o cálculo de predicados, es una extensión de la lógica proposicional que nos permite expresar relaciones y propiedades de objetos, así como cuantificar sobre ellos. Mientras que la lógica proposicional se limita a tratar proposiciones completas como unidades indivisibles, la lógica predicativa nos permite descomponer las proposiciones en sujetos y predicados, lo que nos da un mayor poder expresivo para formalizar el lenguaje natural y razonar sobre él.

Conceptos clave

Definición 2.6. Función proposicional $P(x)$

Función proposicional en una variable o indeterminada x es toda oración en la que figura x como sujeto u objeto directo, la cual se convierte en proposición para cada especificación de x.

Ejemplo 2.19

$$P(x, y) : x \mid y$$

- $x \mid y$ se lee: x es divisor de y

$P(x, y)$ no es proposición ya que no podemos afirmar la verdad o falsedad del enunciado. Mas para cada particularización de valores se tiene un proposición:

$$P(-2, 6) : -2 \mid 6 \quad (V)$$

$$P(12, 6) : 12 \mid 6 \quad (F)$$

- **Predicados**: Los predicados son funciones proposicionales que toman uno o más argumentos (objetos) y devuelven un valor de verdad (verdadero o falso). Representan propiedades o relaciones entre objetos. Por ejemplo, "ser rojo" o "ser mayor que" son predicados.
- **Constantes**: Las constantes representan objetos específicos en el dominio del discurso. Por ejemplo, "Juan" o "5" son constantes.
- **Variables**: Las variables representan objetos genéricos o desconocidos en el dominio del discurso. Se utilizan para cuantificar sobre objetos. Por ejemplo, x o y son variables.

Los cuantificadores nos permiten expresar afirmaciones sobre la cantidad de objetos que cumplen una determinada propiedad o relación.

2.2.1. Cuantificador existencial

El cuantificador existencial se utiliza para afirmar que existe al menos un elemento en un conjunto o dominio que cumple una determinada propiedad o relación.

- Símbolo: $\exists$ (se lee "existe" o "hay")
- Estructura: $\exists x\ P(x)$, donde:
  - $\exists x$: Indica que existe al menos un elemento x en el dominio que satisface la afirmación.
  - $P(x)$: Es un predicado que expresa una propiedad o relación sobre el elemento x.
- Ejemplo:

  "Algunos estudiantes aprobaron el examen" se formalizaría como:

  $$\exists x\,(E(x) \land A(x))$$

  donde $E(x)$ significa "x es un estudiante" y $A(x)$ significa "x aprobó el examen".

2.2.2. Cuantificador universal

El cuantificador universal se utiliza para afirmar que una propiedad o relación se cumple para todos los elementos de un conjunto o dominio específico.

- Símbolo: $\forall$ (se lee "para todo" o "para cada")
- Estructura: $\forall x\ P(x)$, donde:
  - $\forall x$: Indica que la afirmación se aplica a todos los elementos x en el dominio.
  - $P(x)$: Es un predicado que expresa una propiedad o relación sobre el elemento x.
- Ejemplo:

  "Todos los perros ladran" se formalizaría como: $\forall x\ (P(x) \implies L(x))$ donde $P(x)$ significa "x es un perro" y $L(x)$ significa "x ladra".

2.2.3. Negación de cuantificadores

La negación de una proposición universal es una proposición existencial, y viceversa.

I) $\neg\,(\forall x\ P(x)) \equiv \exists\ x\ \neg P(x)$

Esto es:

- Proposición original: $\forall x\ P(x)$, "Para todo x, $P(x)$ es verdadero
- Negación: $\exists\, x\ \neg P(x)$, "Existe al menos una x para la cual $P(x)$ es falso"

Ejemplo:

- Original: "Todos los gatos son negros", ($\forall x\ P(x)$, donde x es un gato, $P(x)$ "x es negro")
- Negación: "Existe al menos un gato que no es negro", ($\exists\ x\ \neg P(x)$).

II) $\neg\,(\exists\, x\ P(x)) \equiv \forall x\ \neg P(x)$

Esto es:

- Proposición original: $\exists\, x\ P(x)$, "Existe al menos una x para la cual $P(x)$ es verdadero
- Negación: $\forall x\ \neg P(x)$, "Para toda x, $P(x)$ es falso"

Ejemplo:

- Original: "Algunos estudiantes aprobaron el examen" o "Al menos un estudiante aprobó el examen" ($\exists\, x\ P(x)$, donde x es un estudiante, $P(x)$ "x aprobó el examen")
- Negación: "Ningún estudiante aprobó el examen" o, dicho de otra manera, "todos los estudiantes no aprobaron el examen" ($\forall x\ \neg P(x)$).

2.3. Sistema axiomático de Peano

2.3.1. Axiomas de Peano

Sistema axiomático:

- *Términos primitivos*: elementos, conjuntos o relaciones, cuya naturaleza no queda especificada de antemano.
- *Axiomas*: propiedades que debe satisfacer los términos primitivos.
- *Definiciones*: de los términos no primitivos.
- *Teoremas*: propiedades que se deducen de los axiomas.

Axiomas de Peano

N1 : Existe una función inyectiva, la función "siguiente", $s : \mathbb{N} \to \mathbb{N} \setminus \{1\}$;

N2 : Existe un único elemento en $\mathbb{N}$, denotado por 1, tal que: $\forall n \in \mathbb{N}, 1 \neq s(n)$;

N3 : Dado cualquier subconjunto $X \subseteq \mathbb{N}$, si $1 \in X$ y $n \in X \implies s(n) \in X$, entonces $X = \mathbb{N}$.

Dado $n \in \mathbb{N}$, su imagen $s(n)$ se llama su **sucesor**.

- N1 establece que todo número tiene un sucesor y que números naturales diferentes tienen sucesores diferentes (inyectiva)
- N2 establece que existe un único número natural que no tiene sucesor, el 1.
- N3 es una formulación del **principio de inducción matemática**. La condición $n \in X \implies s(n) \in X$ es equivalente a $s(X) \subseteq X$.

2.3.2. Principio de inducción

La idea básica es: P es un propiedad válida de 1 hasta $n \in \mathbb{N}$, se argumenta que su sucesor $s(n)$ también satisface la propiedad P, entonces P es válido $\forall n \in \mathbb{N}$. En otras palabras:

- $P(1)$ es V (base)
- $P(h)$ es V $\implies$ $P(s(h))$ es V, entonces $P(n)$ es V para todo $n \in \mathbb{N}$.

Basados en los axiomas de Peano, podemos definir:

Definición 2.7. Adición en $\mathbb{N}$

a) $a + 1 = s(a)$ cualquiera sea $a \in \mathbb{N}$

b) $a + s(b) = s(a + b)$ cualesquiera que sean $a, b \in \mathbb{N}$

Definición 2.8. Multiplicación en $\mathbb{N}$

a) $a \cdot 1 = a$, $\forall a \in \mathbb{N}$

b) $a \cdot s(b) = a \cdot b + a$, cualesquiera sean $a, b \in \mathbb{N}$.

Estas definen la ley de composición interna en $\mathbb{N}$ y se cumplen $\forall a, b, c \in \mathbb{N}$:

1. *Asociatividad*: $(a + b) + c = a + (b + c)$ y $(ab)c = a(bc)$
2. *Distributividad*: $a(b + c) = ab + ac$
3. *Conmutatividad*: $a + b = b + a$ y $ab = ba$
4. *Ley de corte o cancelación*: $a + b = a + c \implies b = c$ y $ab = ac \implies b = c$

Se define la **potenciación** en $\mathbb{N}$, mediante:

Definición 2.9. Potenciación en $\mathbb{N}$

a) $a^1 = a$

b) $a^{s(b)} = a^b a$

Proposición 2.1

La potenciación es distributiva respecto al producto: $(ab)^n = a^n b^n$

Prueba 2.1.1

Por inducción

I) $n = 1 \implies (ab)^1 = ab = a^1 b^1$ (caso base)

II) $(ab)^h = a^h b^h \implies (ab)^{s(h)} = a^{s(h)} b^{s(h)}$

$$(ab)^{s(h)} = (ab)^h (ab) = a^h b^h ab = a^h a b^h b = a^{s(h)} b^{s(h)}$$

2.3.3. Relación de orden

Definición 2.10. Relación de orden

La relación $\leq$ es una *relación de orden*, es decir, satisface $\forall a, b, c \in \mathbb{N}$:

1. Reflexividad: $a \leq a$
2. Antisimetría: $a \leq b \wedge b \leq a \implies a = b$
3. Transitividad: $a \leq b \wedge b \leq c \implies a \leq c$

Teorema 2.2. Principio del buen orden

Si $A \subseteq \mathbb{N}$ es un conjunto no vacío, entonces admite un elemento mínimo $a_0 \in A$, es decir, $\exists a_0 \in A / a_0 \leq a, \forall a \in A$.

Prueba 2.2.1

Supongamos que se verifica el principio de inducción.

Tomemos un subconjunto $A \subseteq \mathbb{N}$ no vacío y supongamos que no tiene un mínimo. Consideremos ahora el conjunto S de todos los números menores que todos los elementos de A. Naturalmente $1 \ni A$, que es menor que cualquier otro número, luego $1 \in S$. Además, para cada $n \in S \implies n + 1 \in S$, de lo contrario $n + 1$ sería el mínimo de A. Por tanto, por el principio de inducción $S = \mathbb{N}$ y A es el conjunto vacío.

Sin embargo, esto contradice nuestra hipótesis inicial, luego A debe tener un elemento mínimo.

2.3.4. Teorema fundamental de la aritmética

Previos:

- Decimos que q es un *múltiplo* de p si $\exists n \in \mathbb{N} / q = np$
- También decimos que n y p son *factores* de q o que *dividen* a q.

- Un elemento $p \in \mathbb{N}$ distinto de 1 se llama *primo* si sus únicos factores son el 1 y el propio p.

Teorema 2.3. Teorema fundamental de la aritmética

Todo número natural $p \neq 1$ es primo o puede descomponerse como producto de números primos. La descomposición prima es única a menos de orden de los factores.

Prueba 2.3.1

Consideremos el conjunto:

$$P \coloneqq \{p \in \mathbb{N}; p \neq 1 \text{ y } p \text{ no es primo ni es producto de factores primos}\}$$

Si la afirmación del teorema fuese falso, el conjunto P sería no vacío, y por lo tanto, por el Principio del Buen Orden, debe tener un elemento mínimo. Llamemos p_0 a dicho elemento. Tenemos que $p_0 \neq 1$, y p_0 no es primo, por lo cual tiene factores q, n distintos de 1 y del propio p_0, es decir, tenemos $p_0 = qn$, con q y n ambos menores que p_0, y ambos distintos del 1. Pero p_0 tampoco es producto de factores primos, por lo cual o bien q o bien n no es primo. Pero esto contradice la minimalidad de p_0 como elemento de P. Esta contradicción indica que debemos tener $P = \emptyset$.

Falta probar la unicidad de la descomposición prima.

2.3.5. Conjuntos finitos e infinitos

Definición 2.11. Conjuntos finitos e infinitos

Dado un natural $n \in \mathbb{N}$, escribiremos:

$$I_n \coloneqq \{m \in \mathbb{N}; 1 \leq m \leq n\}$$

Dado un conjunto X diremos que es **finito**, si es vacío o existe $n \in \mathbb{N}$ y una biyección: $f : I_n \to X$.

Un conjunto que no es finito es *infinito*.

Notas:

- $\forall n \in \mathbb{N}$, el propio I_n es finito, con $X = I_n$;
- Si $X = \emptyset$ decimos que tiene 0 elementos;
- Si $f : I_n \to X$ es una biyección, decimos que X tiene n elementos;
- Llamamos a n la **cardinalidad** de X, se suele escribir: $|X| = n$.
- Si $g : X \to Y$ es una biyección, entonces $f : I_n \to X$ será una biyección si y sólo si, $g \circ f : I_n \to Y$ es una biyección. Es decir, X será finito si Y es finito y tendrán la misma cardinalidad n.

Numerabilidad

No todos los conjuntos infinitos tienen la misma cardinalidad. Un conjunto es *numerable* si y solo si es biyectable con $\mathbb{N}$. Un conjunto es *contable* si y sólo si es finito o numerable.

Ejemplo 2.20

1. El conjunto de los enteros $\mathbb{Z}$ es numerable.
2. El conjunto de los números racionales $\mathbb{Q}$ es numerable.
3. $\mathbb{R}$, el conjunto de los números reales no es numerable.

Teorema 2.4. Teorema de Cantor

El conjunto potencia $\mathcal{P}(A)$ de cualquier conjunto A tiene una cardinalidad estrictamente mayor que la cardinalidad de A, es decir:

$$|\mathcal{P}(A)| > |A|$$

Prueba 2.4.1. Procedemos por contradicción como lo hizo Cantor[a]. Supongamos que existe una función $f : A \to \mathcal{P}(A)$ que es sobreyectiva, es decir, que para todo elemento B en $\mathcal{P}(A)$, existe un elemento $a \in A$ tal que $f(a) = B$.

Considere el siguiente conjunto: $C = \{a \in A \mid a \notin f(a)\}$

C es el conjunto de todos los elementos $a \in A$ tales que a no pertenece al conjunto $f(a)$. Como $f(a)$ es un elemento de $\mathcal{P}(A)$, $f(a) \subset A$ de donde C es un subconjunto de A, por lo tanto, $C \in \mathcal{P}(A)$.

Como f es sobreyectiva, debe existir un elemento $c \in A$ tal que $f(c) = C$.

Ahora analicemos los casos:

- Caso 1:

  Si $c \in C$, entonces $c \notin f(c)$ por definición de C, pero $f(c) = C$, por lo que $c \notin C$ que es una contradicción.

- Caso 2:

  Si $c \notin C$, entonces $c \in f(c)$, por definición de C, pero $f(c) = C$, por lo que $c \in C$, que es también una contradicción.

En ambos casos llegamos a una contradicción. Por lo tanto, nuestra suposición inicial de que existe una función sobreyectiva $f : A \to \mathcal{P}(A)$ debe ser falsa, lo que implica que la cardinalidad de $\mathcal{P}(A)$ es estrictamente mayor que la cardinalidad de A.

[a] Georg Cantor, 1845-1918, matemático ruso.

2.4. Ejercicios

Incompleto

1. Escribe en símbolos:

- "Si no hay ruidos y no estás sordo, entonces debes oírme".
- "Iré al cine o al teatro, si me invitas".
- "Si el aumento de la inflación implica la disminución de la balanza de pagos, entonces, si no disminuye la balanza de pagos no aumenta la inflación".
- "Federico irá a Encarnación o a Virgen del Paraná si y sólo si gana la lotería y no se arruina con las apuestas".
- "Si $x = 1$ e $y = 2$, entonces $z = 3$. Si, si $y = 2$, $z = 3$ entonces $w = 0$. $x = 1$. Por consiguiente, $w = 0$".

2. Realiza la tabla de valores de verdad para probar:

- $p \oplus q = \neg(p \wedge q) \wedge (p \vee q)$;
- La distributividad de la conjunción respecto de la disyunción.

Capítulo 3

Estructuras algebraicas

Una estructura algebraica es una par $(G, *)$, en donde G es un conjunto no vacío y $*$ es una operación aplicable a los elementos dicho conjunto. Podrían haber más operaciones aplicables, por ejemplo, sin son aplicables las operaciones $*$ y $\cdot$, la estructura algebraica sería $(G, *, \cdot)$.

En general, una estructura algebraica es una $n - tupla : (a_1, a_2, \ldots, a_n)$, donde a_1 es un conjunto no vacío dado, y $\{a_2, \ldots, a_n\}$ es un conjunto de operaciones aplicables a los elementos del conjunto a_1.

Las estructuras algebraicas nos permiten estudiar y clasificar objetos matemáticos en función de sus propiedades algebraicas. Algunos ejemplos de estructuras algebraicas incluyen grupos, anillos y campos.

3.1. Grupos

3.1.1. Axiomas de grupo

Definición 3.1. Grupo

Dado un conjunto G, no vacío, una operación binaria o función $* : G \times G \to G$, define en G una *estructura de grupo* $(G, *)$ si se cumplen las siguientes propiedades:

G1: **Asociatividad**: $\forall x, y, z \in G \implies (x * y) * z = x * (y * z)$

G2: **Existencia del neutro**: $\exists\, e \in G \mid \forall x \in G \implies x * e = e * x = x$

G3: **Existencia de inversos**: $\forall x \in G, \exists x' \in G \mid x * x' = x' * x = e$

Por lo tanto, un grupo es una estructura algebraica que consta de:

a) Un conjunto no vacío;

b) Una operación binaria (una función con dos argumentos);

c) Tres propiedades.

Ejemplo 3.1

Conjunto: $\mathbb{Z}$; Operación binaria: suma $(+)$; Propiedades:

1. Asociatividad: $(3+4)+2=3+(4+2)$
2. Neutro: el cero, $0+3=3+0=3$
3. Inversos: $4+(-4)=(-4)+4=0$

En general: $\forall x, y, z \in \mathbb{Z}$

1. Asociatividad: $(x+y)+z=x+(y+z)$
2. Neutro: $\exists\, 0 \in \mathbb{Z}/0+x=x+0=x$
3. Inversos: $\forall x \in \mathbb{Z}, \exists\,(-x) \in \mathbb{Z}/x+(-x)=(-x)+x=0$

$(\mathbb{Z},+)$ es un grupo.

Definición 3.2. Grupo abeliano

En caso de que $(G,*)$ cumpla además la propiedad conmutativa,

G4: **Conmutatividad**: $\forall x, y \in G \implies x*y=y*x$

se llama grupo *abeliano*[a] o *conmutativo*.

[a] En homenaje al matemático noruego Niels Henrik Abel (1802-1829)

Notas:

I) Se dice que la operación $(*)$ es **cerrada** en el conjunto G, si $*: G \times G \to G$, en este caso, se dice que $(G,*)$ tiene una regla o **ley de composición interna**.

II) Cuando $(G,*)$ es abeliana, es común llamar *suma* o *adición* a $*$, se dice que $*$ es aditiva, suele usarse el signo $+$, su inverso es el *opuesto* y se indica $a'=-a$. Es común llamar *cero* al neutro y denotarlo por 0;

III) Cuando $(G,*)$ es *no abeliana* (o no lo sabemos), decimos que $*$ es multiplicativa, se usa "$\cdot$", su inverso se dice *recíproco* y se utiliza $a'=a^{-1}$. Es usual llamar *unidad* al neutro y denotarlo 1.

IV) Cuando la cardinalidad[1] $|G|$ es finita, decimos que el grupo es *finito*.

V) Dado un grupo $(G,*)$, $a \in G$ y $m \in \mathbb{Z}$, por convención $a^m = a*a*\cdots*a$, con m factores si $m>0$, y $a^m=(a^{|m|})^{-1}=(a*a*\cdots*a)'=a'*a'*\cdots*a'$ con $|m|$ factores a' si $m<0$.

[1] Ver sección 2.3.5

Definición 3.3. Monoide

El par $(M, *)$, donde $M \neq \emptyset$, y $*$ es una función, es un monoide[a] si y solo si $*$ es una *ley de composición interna* en M.

[a] Corresponde a la definición dada en [1].

Definición 3.4 (Idempotencia)**.** Si $(G, *)$ es un monoide, es decir, una estructura algebraica con una ley de composición interna, se dice que $g \in G$ es idempotente si $g * g = g$

La idempotencia es la propiedad de realizar una operación determinada varias veces y aún así obtener siempre el mismo resultado que se obtendría si se realizase una sola vez.

Definición 3.5. Semigrupo

El par $(A, *)$, donde $A \neq \emptyset$, y $*$ es una función, es un semigrupo si y solo si $*$ es una ley interna y asociativa en A.

Proposición 3.1 (Unicidad del neutro)**.** *En cualquier grupo el neutro es único.*

Prueba 3.1.1. Sae $(G, *)$ un grupo cualquiera. Supongamos $e, e' \in G$ dos elementos que cumplen la propiedad del neutro:

$$\begin{cases} \forall x \in G: & e * x = x * e = x \\ \forall x \in G: & e' * x = x * e' = x \end{cases}$$

Entonces:

$$\begin{cases} x = e': & e * e' = e' * e = e' \\ x = e: & e' * e = e * e' = e \end{cases}$$

por tanto:

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

Proposición 3.2. Ley de corte o de cancelación

Sea $(G, *)$ un grupo. $\forall a, b, c \in G$ se cumple:

a) Ley de corte por la izquierda: $a * b = a * c \implies b = c$

b) Ley de corte por la derecha: $b * a = c * a \implies b = c$

Prueba 3.2.1. Para demostrar a) basta con premultiplicar por el inverso a' y en b) posmultiplicar.

Se dice que los elementos son **regulares** si se cumple la ley de corte.

Proposición 3.3 (Unicidad del inverso)**.** *Para cualquier elemento $x \in G$ existe un inverso y es único.*

Prueba 3.3.1. Sea $(G, *)$ un grupo cualquiera. Supongamos $x', x'' \in G$ dos elementos que cumplen la propiedad del inverso:

$$\begin{cases} \forall x \in G: & x * x' = x' * x = e \\ \forall x \in G: & x * x'' = x'' * x = e \end{cases}$$

Entonces:

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

por ley de cancelación:

$$x' = x''$$

Definición 3.6. Orden de un grupo

Sea $(G, *)$ grupo. Llamamos orden de G al número de elementos de G (si G es finito). Lo denotamos por $o(G) \coloneqq |G| = \text{card}(G) = \#(G)$

Decimos que G es de **orden par** u **orden impar** si $o(G)$ es par o impar respectivamente.

El grupo de orden 1, llamado **grupo trivial**, es el que consta de un solo elemento, el cual debe ser el neutro para cumplir con las propiedades de grupo. Es común utilizar tablas para representar las operaciones, denominadas **tablas de Cayley**[2].

Los conjuntos correspondientes a los grupos de orden 1, 2 y 3 son $\{e\}$, $\{e, a\}$, $\{e, a, b\}$. Sus respectivas tablas de Cayley se muestran en la tabla 3.1:

$*$	e
e	e

$*$	e	a
e	e	a
a	a	e

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Tabla 3.1. Tablas de Cayley para grupos de orden 1, 2 y 3.

- Notar que cada fila y columna contiene todos los elementos del grupo. No existen duplicados en ninguna fila ni columna.
- Estos grupos son abelianos ya que las tablas son simétricas respecto de la diagonal principal.
- Notar la similitud con las operaciones entre números enteros, si convertimos $* \to +, e \to 0, a \to 1, b \to 2$, que se muestran en la tabla 3.2, en este caso se dice que el grupo $(G, *)$ es **isomorfo** con su correspondiente $(\mathbb{Z}_n, +)$. Más adelante se verán estos conceptos con más detalle.

$+$	0
0	0

$+$	0	1
0	0	1
1	1	0

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Tabla 3.2. Tablas de Cayley para enteros módulo 1, 2 y 3.

[2]En homenaje al matemático británico Arthur Cayley (1821-1895)

Tarea: Realizar las tablas de Cayley para grupos de orden 4.

Ejemplo 3.2. Grupo de Klein

El grupo de Klein[a] es abeliano con 4 elementos, en el cual cada elemento es su propio inverso (*propiedad involutiva*), y componiendo cualesquiera dos de ellos, a excepción del neutro, produce el tercero, es decir:

$$V = \{e, a, b, c\}; \quad a^2 = b^2 = (ab)^2 = c^2 = e$$

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Tabla 3.3. Tabla de Cayley para el grupo de Klein.

[a] En honor al matemático alemán Felix Klein (1849-1925).

3.1.2. Grupos de números

Sistemas numéricos.

Veamos el concepto de grupo para los *sistemas numéricos* $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ y las operaciones usuales de suma $(+)$ y multiplicación $(\cdot)$.

En la fig. 3.1 se representan gráficamente. Se observa que: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

	$(\mathbb{N}, +)$ $(\mathbb{N}, \cdot)$	$(\mathbb{Z}, +)$ $(\mathbb{Z}, \cdot)$	$(\mathbb{Q}, +)$ $(\mathbb{Q}^*, \cdot)$	$(\mathbb{R}, +)$ $(\mathbb{R}^*, \cdot)$	$(\mathbb{C}, +)$ $(\mathbb{C}^*, \cdot)$
Asociativa	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓
Neutro	0 1	0 1	0 1	0 1	0 1
Inversos	✗ ✗	✓ ✗	✓ ✓	✓ ✓	✓ ✓

Tabla 3.4. Comprobación de las propiedades de Grupo para sistemas numéricos. Los conjuntos con $*$ indican que se excluye el cero. Los 7 grupos que comprueban las tres propiedades, además, son *abelianos*.

Notar que, a partir de $(\mathbb{Z}, \cdot)$ se deduce que restringiendo al par $(\{-1, 1\}, \cdot)$, este cumple las propiedades de grupo.

3.1.3. Grupos de matrices

Consideremos $\mathbf{M}_{m\times n}(\mathbb{R})$, el conjunto de todas las matrices $m \times n$ con $m, n \in \mathbb{N}$ y elementos reales, el conjunto también puede ser representado por $\mathbb{R}^{m\times n}$.

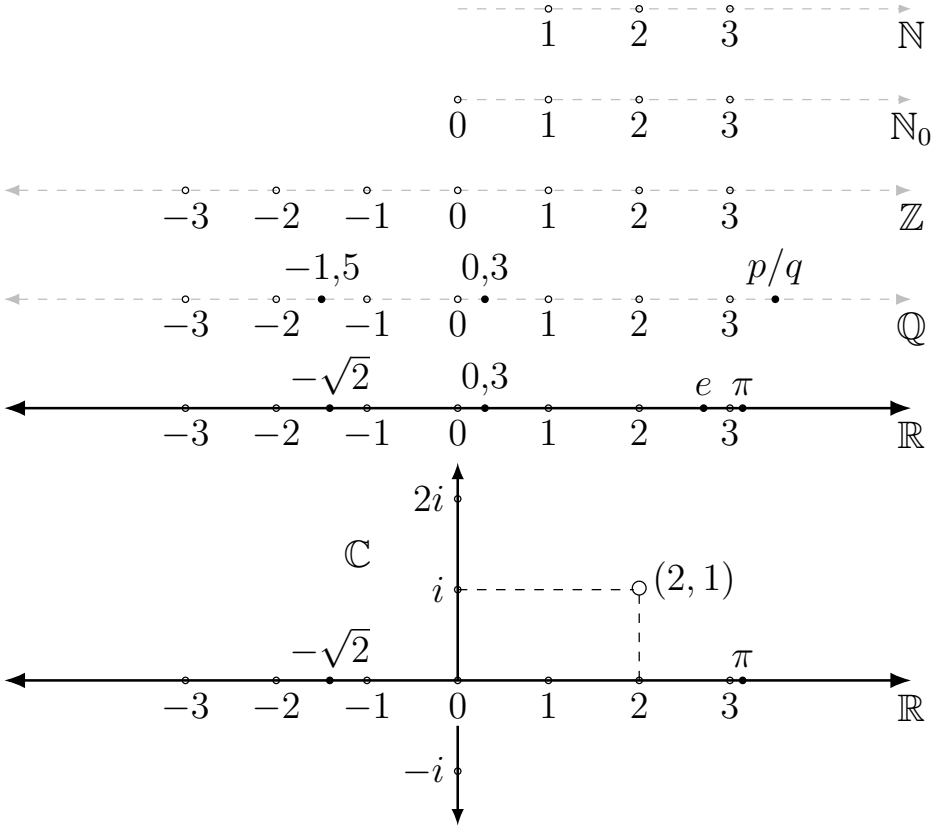


Figura 3.1. Representación gráfica de los sistemas numéricos.

$$\mathbf{M}_{m\times n}(\mathbb{R}) = \left\{ \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \mid a_{ij} \in \mathbb{R} \right\} \tag{3.1}$$

Suma de matrices

Dadas las matrices $A = (a_{ij})$ y $B = (b_{ij})$, se define la suma: $S = A + B = (s_{ij})$ de modo que $s_{ij} = a_{ij} + b_{ij}$, es decir, la matriz S tiene como elementos la suma de los elementos correspondientes de A y B.

Ejemplo:

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} + \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} = \begin{bmatrix} 6 & 8 \\ 10 & 12 \end{bmatrix}$$

Notar que la suma elemento a elemento ocurre en $\mathbb{R}$, conforme a la definición dada en (3.1). Por lo tanto, probar que $(\mathbf{M}_{m\times n}(\mathbb{R}), +)$ es un grupo se reduce a probar que $(\mathbb{R}, +)$ es un grupo, lo cual ya fue analizado junto con los demás sistemas numéricos, y se vió que $(\mathbb{R}, +)$ es un grupo abeliano, con lo cual,

las matrices cuadradas con la operación suma, cumplen:

G1 Asociatividad: $(A + B) + C = A + (B + C)$ ✓

G2 Neutro: $e_{2\times 3} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$; $e_{m\times n} = \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix}$; $a_{ij} = 0$ ✓

G3 Inversos (opuestos): $(a_{ij})' = (-a_{ij})$ ✓

G4 Conmutatividad: $A + B = B + A$ ✓

por tanto:

$$(\mathbf{M}_{m\times n}(\mathbb{R}), +) \text{ es un grupo abeliano.}$$

El producto indicado $m \times n$ se conoce como **orden de la matriz**, así se dice por ejemplo de $A_{2\times 3}$ es una matriz de orden 2×3.

Grupos de vectores

Un caso especial de matrices son los vectores. Consideremos, el conjunto de vectores en $\mathbb{R}^n$:

$$\mathbf{M}_{1\times n}(\mathbb{R}) = \left\{ \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \mid a_i \in \mathbb{R} \right\} = \mathbb{R}^n = \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{n \text{ veces}} \tag{3.2}$$

con la operación usual de suma.

Vectores con la operación suma. $\forall u, v, w \in \mathbb{R}^n$ se cumple:

G1 Asociatividad: $(u + v) + w = u + (v + w)$ ✓

G1 Neutro: $e_2 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$; $e_n = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$, $a_i = 0$ ✓

G1 Inversos (opuestos): $u' = -u$ ✓

G1 Conmutatividad: $u + v = v + u$ ✓

$$(\mathbb{R}^n, +) \text{ es un grupo abeliano.}$$

Los vectores en $\mathbb{R}^2$ se representan en la fig. 3.2:

i) Neutro: $(0, 0)$

ii) Inverso de $u = (u_1, u_2)$ es $-u = (-u_1, -u_2)$.

Producto de matrices

Dadas las matrices $A = (a_{ik}) \in \mathbf{M}_{m\times n}$ y $B = (b_{kj}) \in \mathbf{M}_{n\times r}$,

$$A \cdot B = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \cdot \begin{bmatrix} b_{11} & \cdots & b_{1r} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nr} \end{bmatrix} = \begin{bmatrix} c_{11} & \cdots & c_{1r} \\ \vdots & \ddots & \vdots \\ c_{m1} & \cdots & c_{mr} \end{bmatrix} = C \tag{3.3}$$

donde:

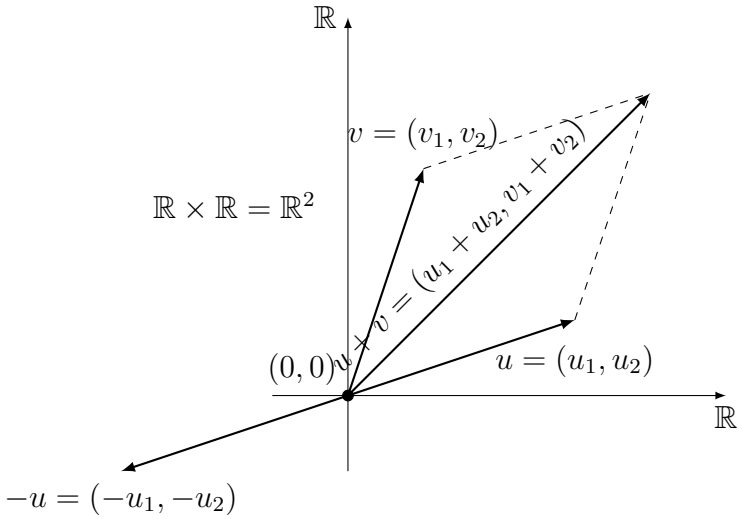


Figura 3.2. $(\mathbb{R}^2, +)$ es un grupo abeliano

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \tag{3.4}$$

es, por definición, el producto de matrices.

Ejemplo:

$$\begin{bmatrix} 1 & 2 & 3 \\ -1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 5 \\ 1 \end{bmatrix} = \begin{bmatrix} 17 \\ -3 \end{bmatrix}$$

Notas:

I) La operación es $\cdot : \mathbf{M}_{m\times n} \times \mathbf{M}_{n\times r} \to \mathbf{M}_{m\times r}$, es decir, $(A, B) \to C$. El número de columnas de A debe ser igual al número de filas de B para que se realizable el producto. La matriz C es de orden igual al número de filas de A por el número de columnas de B.

II) Las matrices de orden $m \times n$ con $m \neq n$ son llamadas **matrices rectangulares** y cuando $m = n$ se dice que son **cuadradas**.

III) El producto de matrices es asociativo, es decir:

$$(A_{m\times n} \cdot B_{n\times r}) \cdot C_{r\times s} = A_{m\times n} \cdot (B_{n\times r} \cdot C_{r\times s})$$

Como puede comprobarse de la definición.

IV) Las matrices rectangulares con la operación de multiplicación definida en (3.4) no forman un grupo, pues la operación no es **cerrada**, es decir, en general las matrices A, B, C, con $C = AB$ no son del mismo orden, en otras palabras, no son del mismo conjunto, de donde no se cumple la condición $\cdot : G \times G \to G$, dada en la definición de grupo.

Consideremos solo matrices cuadradas $\mathbf{M}_{n\times n}(\mathbb{R}) = \mathbf{M}_n(\mathbb{R})$, en este caso, la operación de multiplicación $(\cdot)$ es cerrada, esto es:

$$\cdot : \mathbf{M}_n \times \mathbf{M}_n \to \mathbf{M}_n$$

G1: Asociatividad: $(AB)C = A(BC)$ ✓

G2: Elemento neutro: ✓

$$I_n = \begin{bmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix}; a_{ij} = \delta_{ij} = \begin{cases} 1 & \text{si } i = j; \\ 0 & \text{si } i \neq j \end{cases}$$

I_n es la matriz identidad de orden n; δ_{ij} se conoce como delta de Kronecker[3].

G3: Inversos ✗

No toda matriz $A \in \mathbf{M}_n$ tiene inversa, como se verá más adelante en el curso.

de donde, en general las matrices cuadradas de orden n con la operación de multiplicación no son un grupo, se cumple que:

$$(\mathbf{M}_n(\mathbb{R}), \cdot) \text{ es un semigrupo con elemento neutro.}$$

Se llaman **matrices invertibles** aquellas que admiten inversa. La inversa de A se denota como A^{-1}. Esto nos lleva a la definición siguiente:

Definición 3.7. Grupo General Lineal

Dado el conjunto de matrices cuadradas invertibles con entradas en $\mathbb{R}$:

$$GL_n(\mathbb{R}) = \left\{ A \in \mathbf{M}_n(\mathbb{R}) \mid \exists A^{-1} \right\} \subset \mathbf{M}_n(\mathbb{R})$$

y la operación de multiplicación de matrices $(\cdot)$.

$(GL_n(\mathbb{R}), \cdot)$ se llama *grupo general lineal*.

Notar que $(GL_n(\mathbb{R}), \cdot)$ es efectivamente un grupo.

Se verá más adelante en el curso que el determinante de matrices invertibles es distinto de cero. Incorporando este concepto de determinante definimos otro grupo más pequeño que el anterior.

Definición 3.8. Grupo Especial Lineal

El conjunto de matrices cuadradas invertibles con determinantes iguales a uno:

$$SL_n(\mathbb{R}) = \{ A \in \mathbf{M}_n(\mathbb{R}) \mid \det A = 1 \}$$

con la operación de multiplicación matricial, $(SL_n(\mathbb{R}), \cdot)$ se llama *grupo especial lineal*.

Notar que:

$$SL_n(\mathbb{R}) \subset GL_n(\mathbb{R}) \subset \mathbf{M}_n(\mathbb{R})$$

[3]En homenaje al matemático alemán Leopold Kronecker (1823-1891).

3.1.4. Homomorfismo de grupos

Definición 3.9. Homomorfismo de grupos

Dados los grupos $(G, *)$ y $(H, \cdot)$, un homomorfismo de G a H es una función $\phi : G \to H \,/\, \forall a, b \in G \implies \phi(a * b) = \phi(a) \cdot \phi(b)$.

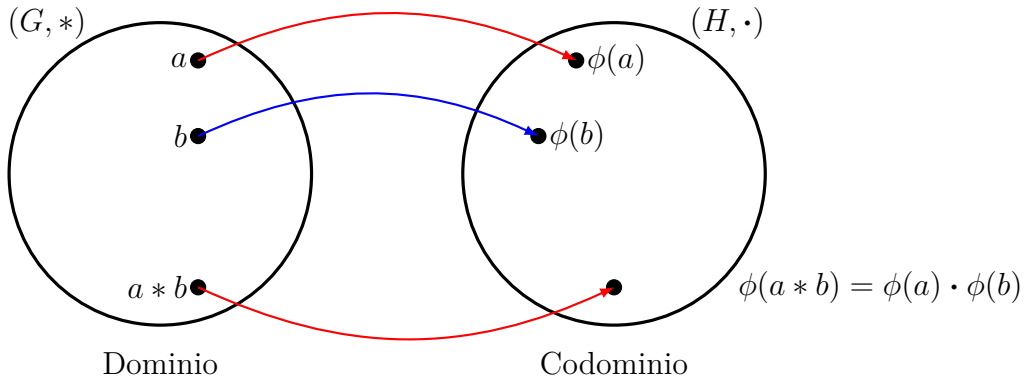


Figura 3.3

Propiedades básicas

1. La imagen del neutro de G es el neutro de H: $\phi(e_G) = e_H$.

$$\phi(a) = \phi(a * e_G) = \phi(a) \cdot \phi(e_G) = \phi(a) \cdot e_H \implies \phi(e_G) = e_H$$

   por elemento neutro en $(G, *)$, homomorfismo, elemento neutro en $(H, \cdot)$ y ley de cancelación.

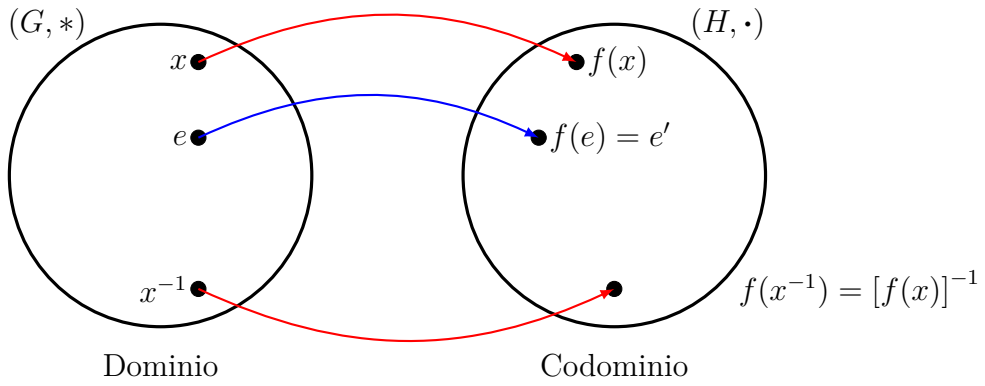
2. La imagen del inverso de todo elemento en G es el inverso de su imagen en H: $\phi(a'_G) = a'_H$ o, en otra notación: $f(x^{-1}) = [f(x)]^{-1}$.

$$\forall x \in G : x * x^{-1} = e \implies f(x * x^{-1}) = f(e)$$

   por homomorfismo y propiedad 1:

$$f(x) \cdot f(x^{-1}) = e_H \implies f(x^{-1}) = [f(x)]^{-1}$$

   En un diagrama:



Se dice que:

I) ϕ es un *mono*morfismo si es *inyectiva*;

II) ϕ es un *epi*morfismo si es *sobreyectiva*;

III) ϕ es un *iso*morfismo si es *biyectiva*;

IV) ϕ es un *endo*morfismo si $G = H$;

V) ϕ es un *auto*morfismo si es un endomorfismo biyectivo.

A veces deja de escribirse $*$ y $\cdot$ de modo que $\phi(ab) = \phi(a)\phi(b)$, sin embargo no debe perderse de vista que ab ocurre en G y $\phi(a)\phi(b)$ en H.

Ejemplo 3.3

Dados $(\mathbb{R}, +)$ grupo de números reales para la adición y $(\mathbb{R}^+, \cdot)$ grupo de números reales positivos para la multiplicación. La aplicación $f : \mathbb{R} \to \mathbb{R}^+$ definida por $f(x) = 2^x$ es un homomorfismo ya que:

$$f(x + y) = 2^{x+y} = 2^x 2^y = f(x)f(y)$$

En particular, f es biyectiva, luego $(\mathbb{R}, +)$ y $(\mathbb{R}^+, \cdot)$ son isomorfos.

Ejemplo 3.4

Para cualquier grupo G

1. El mapa nulo $\phi : G \to G$, dado por $\phi(x) = e_G, \forall x \in G$ y el mapa identidad $id : G \to G$, dado por $id(x) = x, \forall x \in G$, son endomorfismos.
2. Si $a \in G$, el mapa $C_a : G \to G / C_a(b) = a^{-1}ba$ es un automorfismo. En efecto:

   $$C_a(bc) = a^{-1}bca = a^{-1}b(aa^{-1})ca = (a^{-1}ba)(a^{-1}ca) = C_a(b)C_a(c)$$

   es un homomorfismo, falta verificar que es invertible, su inversa es $C_{a^{-1}} : G \to G$ (verificar).

Ejemplo 3.5

Dados $(\mathbb{R}^+, \times)$ grupo de números reales positivos con la operación de multiplicación y $(\mathbb{R}, +)$ grupo de números reales con la adición. Probar que la aplicación $f : \mathbb{R}^+ \to \mathbb{R}$ definida por $f(x) = \ln x$ es un isomorfismo.

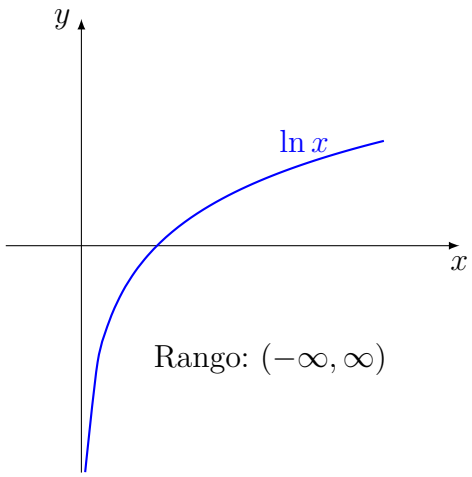
Es un homomorfismo ya que $\ln(xy) = \ln x + \ln y$. Para probar que es un isomorfismo debemos mostrar que f es biyectiva.

a) f es 1-1 si $f(x) = f(y) \implies x = y$

$$\ln x = \ln y \implies e^{\ln x} = e^{\ln y} \implies x = y$$

f es inyectiva.

b) f es sobreyectiva pues $\text{Im}(f) = \mathbb{R}$



De donde f es biyectiva, por lo tanto los grupos mencionados son isomorfos bajo la función logaritmo natural.

3.1.5. Grupos de simetrías

Grupos de funciones

¿Cómo construimos grupos cuyos elementos sean funciones? ¿Cuál debe ser la operación?

Una función asigna a un elemento de A un único elemento de B, $f : A \to B$, es una regla de correspondencia, por lo que la opción natural es adoptar la operación de composición, ahora bien, la composición, en general "cambia de conjunto"

$$A \xrightarrow{f} B \xrightarrow{g} C = A \xrightarrow{g \circ f} C$$

La operación debe ser cerrada:

$$A \xrightarrow{f} A \xrightarrow{g} A = A \xrightarrow{g \circ f} A$$

Adoptamos la notación $B^A := \{f : A \to B\}$, de donde: $A^A = \{f : A \to A\}$.

Como la composición es asociativa y tiene elemento neutro, hasta aquí podemos decir que:

$$(A^A, \circ) \text{ es un semigrupo con neutro } \mathbf{1}_A : A \to A / \mathbf{1}_A(x) = x$$

No es un grupo porque no toda función tiene inversa, en este sentido es similar al caso de las matrices visto en 3.1.3, para que una función admita inversa debe ser biyectiva (ver 1.3.6).

Grupos de permutaciones

Definición 3.10. Permutación

Dado un conjunto A, una **permutación** sobre A es una función biyectiva $f : A \to A$

Notación $S_A \coloneqq \{f : A \to A | \, f \text{ es biyectiva}\}$.

Conforme a todo lo dicho:

$$(S_A, \circ) \text{ es un grupo.}$$

En particular, consideremos un conjunto finito $A = \{a_1, \ldots, a_n\}$, de n elementos, es decir, $|A| = n$. En este caso se escribe $S_A = S_n$, el cual recibe el nombre de **grupo de simetrías** de A.

Por ejemplo: para $n = 3$ el conjunto sería $A = \{a, b, c\}$, y el de simetrías denotamos por S_3.

¿Cuáles serían los elementos de S_3?

La cantidad de asociaciones posibles, es decir, la cardinalidad de A^A sean las funciones biyectivas o no, es $3^3 = 27$, si restringimos solo a las biyectivas, tenemos $|S_3| = 3! = 6$.

El conjunto S_3 con sus 6 elementos es:

$$\begin{aligned} S_3 = & \left\{ \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \right\} \\ = & \quad \{\varepsilon \qquad \sigma_1 \qquad \sigma_3 \qquad \phi_1 \qquad \phi_2 \qquad \sigma_2\} \end{aligned}$$

En donde los elementos no deben entenderse como matrices, aunque se denomina **notación matricial**, en cuyas primeras filas se muestran los elementos de A y en segundas filas sus asignaciones correspondientes, $\begin{pmatrix} a & b & c \\ i & j & k \end{pmatrix}$ es la permutación que aplica $a \mapsto i, b \mapsto j, c \mapsto k$. Como ejemplo se muestran los diagramas de la fig. 3.4.

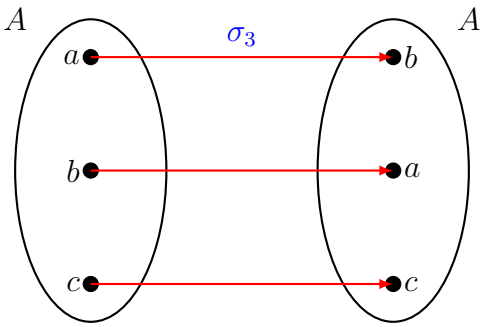


Figura 3.4

Si colocamos los elementos de A en un triángulo equilátero, trazando bisectrices en cada ángulo, como se muestra en la fig. 3.5, cada elemento de S_3 puede entenderse como:

- Identidad: $i_A = \varepsilon$
- Reflexiones (σ): respecto a cada bisectriz.

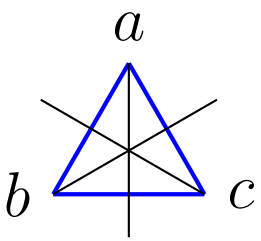


Figura 3.5

- Respecto de la bisectriz que pasa por a: σ_1 (a es un **punto fijo**)
- Respecto de b: σ_2 (b es un punto fijo)
- Respecto de c: σ_3 (c es un punto fijo)

- Rotaciones (ϕ): los elementos *giran*[4] y se reubican en nuevos vértices.
  - ϕ_1: $a \mapsto b, b \mapsto c, c \mapsto a$, es decir: $(a, b, c) \mapsto (b, c, a)$
  - ϕ_2: $a \mapsto c, c \mapsto b, b \mapsto a$, es decir: $(a, c, b) \mapsto (c, b, a)$

$$S_3 = \{\varepsilon, \sigma_1, \sigma_2, \sigma_3, \phi_1, \phi_2\}$$

El conjunto S_3 se conoce como **simetrías del triángulo**, similarmente S_4 contiene las **simetrías del cuadrado**. En general las simetrías son transformaciones de reflexiones y rotaciones que mantienen las formas. Estas simetrías forman un grupo llamado **grupo de simetrías** S_n. Cuando la forma es un polígono regular el grupo de simetrías es llamado **grupo diédrico** D_n.

Utilizando números $A = \{1, 2, 3\}$ en sustitución de $\{a, b, c\}$ se tiene la tabla 3.5.

A	e	r	r^2	f	rf	r^2f
1	1	3	2	1	2	3
2	2	1	3	3	1	2
3	3	2	1	2	3	1

Tabla 3.5

En donde hemos llamado r a una rotación y f a una reflexión:

$$\begin{array}{lll} \varepsilon = e; & r = \phi_1; & r^2 = \phi_2; \\ f = \sigma_1; & rf = \sigma_3; & r^2f = \sigma_2 \end{array}$$

Los grupos de simetrías para diferentes triángulos son:

- Equilátero: $\{e, r, r^2, f, rf, r^2f\}$;
- Isósceles: $\{e, f\}$;

[4] El giro es de 60° (en general $360/n$), en sentido antihorario de acuerdo a cómo fueron colocados a, b, c en la fig. 3.5

- Escaleno: $\{e\}$

Tarea: Escribe el grupo de simetrías del cuadrado y del rectángulo.

Composición de funciones en S_3

Se muestra en la fig. 3.6 un ejemplo de composición de funciones y en la tabla 3.6 la composición de todos los pares de funciones, la operación es:

$$\sigma_3 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \phi_2$$

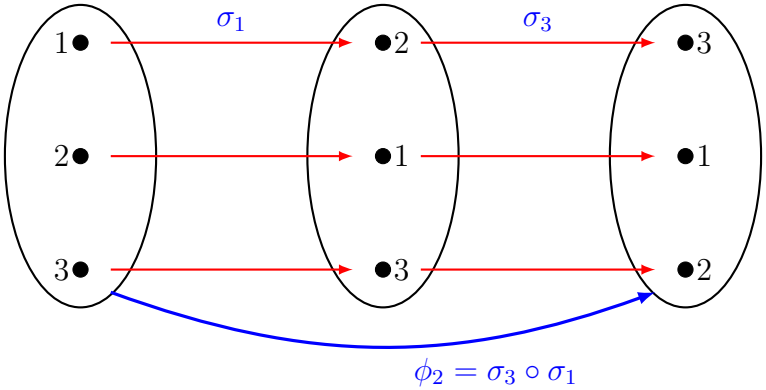


Figura 3.6

$\circ$	ε	σ_1	σ_2	σ_3	ϕ_1	ϕ_2
ε	ε	σ_1	σ_2	σ_3	ϕ_1	ϕ_2
σ_1	σ_1	ε	ϕ_1	ϕ_2	σ_2	σ_3
σ_2	σ_2	ϕ_2	ε	ϕ_1	σ_3	σ_1
σ_3	σ_3	ϕ_1	ϕ_2	ε	σ_1	σ_2
ϕ_1	ϕ_1	σ_3	σ_1	σ_2	ϕ_2	ε
ϕ_2	ϕ_2	σ_2	σ_3	σ_1	ε	ϕ_1

Tabla 3.6. Grupo $(S_3, \circ)$.

G1: Asociatividad ✓

G2: Elemento neutro: ε ✓

G3: Inversos: ✓

- Todos son sus propios inversos a excepción de ϕ_1 y ϕ_2 que son inversos entre si.

G4: Conmutatividad: ✗

3.1.6. Subgrupos

Definición 3.11. Subgrupo

El subconjunto no vacío H de G, es un subgrupo de $(G, *)$ si y solo si $(H, *)$ es un grupo.

Notar que como el neutro es único y $H \subseteq G \implies e_G = e_H$

Subgrupos:

1. $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$
2. $(\{1, -1\}, \cdot) \leq (\mathbb{Q} \setminus \{0\}, \cdot) \leq (\mathbb{R} \setminus \{0\}, \cdot) \leq (\mathbb{C} \setminus \{0\}, \cdot)$

Teorema 3.4. Condición suficiente para existencia de subgrupo

Dado el grupo $(G, *)$, si $H \subseteq G$, con $H \neq \emptyset$, que verifica:

$$a \in H \wedge b \in H \implies a * b' \in H$$

entonces $(H, *)$ es un subgrupo de $(G, *)$.

Prueba 3.4.1

- Asociatividad: se verifica por ser $H \subset G$.
- El neutro pertenece a H. En efecto: $H \neq \emptyset \implies \exists a \in H$
$$a \in H \wedge a \in H \implies a * a' \in H \implies e \in H$$
- Todo elemento de H admite inverso en H.
$$e \in H \wedge a \in H \implies e * a' \in H \implies a' \in H$$
- H es cerrado para $*$
$$a \in H \wedge b \in H \implies a \in H \wedge b' \in H \implies a * (b')' \in H \implies$$
$$a * b \in H$$

Es fácil verificar que la condición también es necesaria.

Observemos que los enteros pares forman subgrupo de $(\mathbb{Z}, +)$ pero los impares no ¿por qué?

Definición 3.12 (Subgrupo trivial)**.** Sea $(G, *)$ un grupo no vacío, consideremos el conjunto $H = \{e\}$, claramente $H \subset G$, se cumple que $(H, *)$ es un subgrupo de $(G, *)$, pues:

$$e \in H \wedge e \in H \implies e * e' = e \in H$$

Al subgrupo $(H, *)$ definido de esta manera se le llama *subgrupo trivial*.

Definición 3.13. Subgrupo cíclico

Sea $(G, *)$ un grupo y $a \in G$, consideremos el conjunto $H = \{a^n : n \in \mathbb{Z}\}$, $(H, *)$ es un subgrupo de $(G, *)$.

Prueba 3.4.2. Sean $g, h \in H$ entonces $\exists m, n \in \mathbb{Z} / g = a^m \wedge h = a^n$, en consecuencia $g * h^{-1} = a^m * a^{-n} = a^{m-n} \in H$ así tenemos que $(H, *)$ es un subgrupo de $(G, *)$

Notemos que si $a = 1_G$ entonces $H = \{a^n : n \in \mathbb{Z}\} = \{1_G\}$, pero si $a \neq 1_G$ en H tenemos al menos dos elementos:

$$a = a^1 \text{ y } 1_G = a^0$$

Al subgrupo $(H, *)$ se le llama *subgrupo cíclico* generado por a y se denota por

$$H = \langle a \rangle$$

Sea G un grupo y $a \in G$:

- **Notación multiplicativa**:

$$a^1 = a,\ a^0 = 1,\ a^n = \underbrace{a \cdots a}_{n\, veces}, \forall n \geq 2; \quad a^{-n} = (a^{-1})^n = \underbrace{a^{-1} \cdots a^{-1}}_{n\, veces}$$

- **Notación aditiva**:

$$1a = a,\ 0a = 0,\ na = \underbrace{a + \cdots + a}_{n\, veces}, \forall n \geq 2; \quad -na = \underbrace{-a - \cdots - a}_{n\, veces}$$

Ejemplo 3.6

El grupo $(\mathbb{Z}, +)$ es cíclico, pues cualquier elemento $p \in \mathbb{Z}$ es de la forma: $p = 1^p = \underbrace{1 + 1 + \cdots + 1}_{p\, veces} = 1 \cdot p$

$\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ no son cíclicos. El grupo de números pares $\langle 2 \rangle$ es cíclico. El menor grupo cíclico es el trivial.

Utilizando la notación multiplicativa los subgrupos cíclicos con generador x deben ser de la forma:

$$\langle x \rangle = \{\ldots, x^{-3}, x^{-2}, x^{-1}, 1, x, x^2, x^3, \ldots\}$$

En la notación aditiva tenemos:

$$\langle y \rangle = \{\ldots, -3y, -2y, -y, 0, y, 2y, 3y, \ldots\}$$

Definición 3.14. Orden de un elemento

Sean $(G, *)$ un grupo y $a \in G$. Consideremos al conjunto $\{n \in \mathbb{Z}^+ : a^n = 1_G\}$. Se define el *orden* de a como:

$$o(a) = |a| = \text{mín}\{n \in \mathbb{Z}^+ : a^n = 1_G\} \in \mathbb{Z}^+$$

en este caso diremos que a es de orden finito.

Si $\{n \in \mathbb{Z}^+ : a^n = 1_G\} = \emptyset$ definimos el orden de a como $o(a) = \infty$.

- Notar que $o(1_G) = 1$ y es único, i.e., $\exists!\, a \in G$ con $o(a) = 1$ $(a = 1_G)$.
- El orden del generador coincide con el del subgrupo cíclico que genera:

$$o(a) = |\langle a \rangle|$$

Ejemplo 3.7

Sea $G = \{1, i, -1, -i\}$ siendo $i = \sqrt{-1}$ la unidad imaginaria. Su tabla de Cayley para la operación de multiplicación es:

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Notar que el grupo es abeliano y cíclico, generado por i, es decir $G = \langle i \rangle$. El elemento neutro es el 1.

El orden del elemento -1 es 2, porque $(-1)^2 = 1$, el orden del elemento generador i es 4, porque $i^4 = 1$, que es igual al orden $|G|$ del subgrupo generado.

Ejemplo 3.8

Considerando el grupo de simetrías del triángulo equilátero $D_3 = \{e, r, r^2, f, rf, r^2 f\}$, en donde r es una rotación y f una reflexión.

Como $r^3 = e$ el orden de r es $|r| = 3$, análogamente, como $f^2 = e$ el orden de f es $|f| = 2$.

Tarea: Probar que:

1. Si un grupo es cíclico, entonces es abeliano.
2. Cualquier subgrupo de un grupo cíclico, también es cíclico.
3. Cualquier grupo $(G, \cdot)$ de orden 1, 2, 3 o 4 es abeliano

Sean $(G, *)$ un grupo y $\{G_i\}_{i \in I}$ una familia de subgrupos de $(G, *)$

Teorema 3.5

La intersección de toda familia no vacía de subgrupos de $(G, *)$ es un subgrupo.

Prueba 3.5.1

H) $(G, *)$ es grupo. $\{G_i\}$ es tal que $(G, *)$ es un subgrupo de $G, \forall i \in I$.

T) $(\bigcap_{i\in I} G_i, *)$ es subgrupo de $(G, *)$

I) $\forall i : e \in G_i$, pues $(G_i, *)$ es un grupo: $e \in \bigcap_{i\in I} G_i \implies \bigcap_{i\in I} G_i \neq \emptyset$

II) $\bigcap_{i\in I} G_i \subset G$ por definición de inclusión

III) Sean $a, b \in \bigcap_{i\in I} G_i \implies a \in G_i \wedge b \in G_i, \forall i \implies$
$a * b' \in G_i, \forall i \implies a * b' \in \bigcap_{i\in I} G_i$

Esta propiedad no se verifica en el caso de la unión.

Definición 3.15. Núcleo de homomorfismo

Núcleo o *kernel* del homomorfismo $f : G \to G'$ es la totalidad de los elementos de G, cuyas imágenes por f se identifican con el neutro de G'.

$$N(f) = \ker f = \{x \in G / f(x) = e'\}$$

Es claro que el núcleo de f es la preimagen de e'.

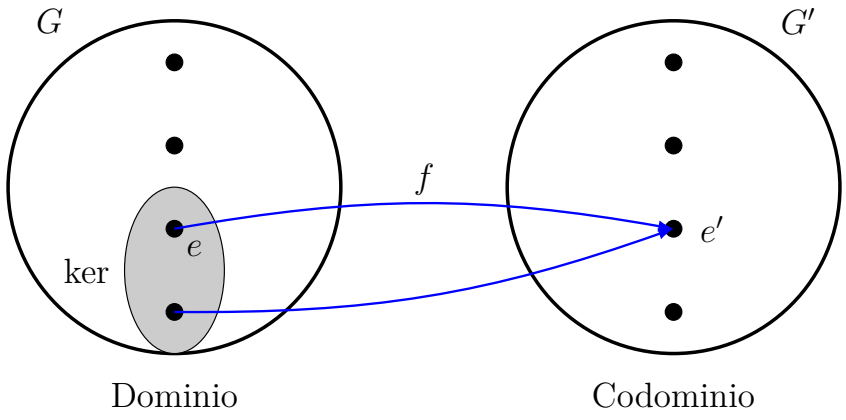


Figura 3.7

Proposición 3.6. *El núcleo de todo homomorfismo de grupos es un subgrupo del primero.*

Prueba 3.6.1. En efecto:

- $\forall a, b \in \ker f \implies f(ab) = f(a)f(b) = e_{G'}e_{G'} = e_{G'} \implies ab \in \ker f$.
- $a \in \ker f \implies f(a^{-1}) = [f(a)]^{-1} = e_{G'}^{-1} = e_{G'} \implies a^{-1} \in \ker f$

Proposición 3.7. *El homomorfismo $f : G \to G'$ es inyectivo, es decir, un monomorfismo si y solo si el núcleo es unitario:* $\ker(f) = \{e\}$.

Prueba 3.7.1. :

- Si f es inyectivo, entonces $\forall a \in G \wedge a \neq e_G$ debemos tener $f(a) \neq f(e_G) = e_G$, es decir, $\ker f = \{e_G\}$;
- Recíprocamente, si $\ker f = \{e_G\}$, entones: $f(a) = f(b) \implies f(a)\,[f(b)]^{-1} = e_H \implies f(ab^{-1}) = e_H \implies ab^{-1} = e_G \implies a = b$

Definición 3.16. Imagen de un homomorfismo

Es la totalidad de las imágenes de los elementos del primer grupo.

Proposición 3.8. *La imagen de todo homomorfismo de grupos es un subgrupo del segundo:* $Im(f) \subseteq G'$.

Definición 3.17 (Subgrupo distinguido)**.** El subgrupo $(H, *)$ de $(G, *)$ es **distinguido** si y sólo si existe un grupo $(G', *')$ y un homomorfismo $f : G \to G'$, cuyo núcleo es H.

En símbolos:

$H \subset G$ es distinguido $\iff \exists G'$ grupo, y $f : G \to G'$ homomorfismo $/N(f) = H$

Subgrupos distinguidos de todo grupo $(G, *)$ son el mismo G y $\{e\}$ [1] p249.

3.1.7. Subgrupo normal

Relación de equivalencia y clases

Sea $(H, *)$ un subgrupo de $(G, *)$. Definimos en G la relación $\sim$ mediante: $a \sim b \iff a' * b \in H$, es decir, dos elementos está relacionados si y sólo si la composición del inverso del primero con el segundo pertenece a H.

La relación es de equivalencia pues verifica la reflexividad $a \sim a$, simetría $a \sim b \implies b \sim a$ y transitividad $a \sim b \wedge b \sim c \implies a \sim c$, en efecto

Prueba 3.8.1

Propiedades de equivalencia:

i) Reflexividad: $a \equiv_H a \iff aa^{-1} = e \in H$;

ii) Simetría: Si $a \equiv_H b \implies ab^{-1} \in H$ luego $(ab^{-1})^{-1} \in H$, así $ba^{-1} \in H$. De modo que $b \equiv_H a$

iii) Transitividad: Sean $a \equiv_H b$ y $b \equiv_H c$ luego $ab^{-1}, bc^{-1} \in H$ multiplicando ambos elementos $(ab^{-1})\,(bc^{-1}) = aec^{-1} = ac^{-1} \in H$. Se tiene que $a \equiv_H c$.

Concluimos que $a \equiv_H b$ es una relación de equivalencia.

Algunas definiciones $\forall a \in G \wedge H \subseteq G$:

- **Conjugado**: Para $a, b, g \in G$, se dice que b es el **conjugado** de a por g si existe este elemento g tal que $b = g^{-1}ag$.
- **Clase**[5] **lateral izquierda de H**: es el subgrupo $aH \coloneqq \{ah; h \in H\}$
- **Clase lateral derecha de H**: es el subgrupo $Ha \coloneqq \{ha; h \in H\}$
- **Grupo conjugado**[6] **de H**: es el subgrupo $a^{-1}Ha \coloneqq \{a^{-1}ha; h \in H\}$
- **Centro de G**: $Z(G) \coloneqq \{z \in G / zx = xz \forall x \in G\}$. Subgrupo que contiene todos los elementos que conmutan con cualquier elemento de G.

Definición 3.18. Subgrupo normal o invariante

El subgrupo $(H, *)$ de $(G, *)$ es normal o invariante, si y solo si se verifica: $x \in G \wedge y \in H \implies x * y * x^{-1} \in H$

En otras palabras, en un grupo normal, el conjugado de un elemento de H pertenece a H.

Notas:

1. Notación: $H \triangleleft G$ se lee H *es un subgrupo normal* (o invariante) de G;
2. En toda G siempre existen por lo menos dos subgrupos normales:
   - El subgrupo trivial: $\{e\}$;
   - El grupo entero: G
3. Un subgrupo es distinguido si y sólo si es invariante.

Proposición 3.9 (Subgrupos de grupos abelianos)**.** *Todo subgrupo de un grupo abeliano es normal, es decir:* $\forall x, y : x \in G \wedge y \in H \implies xyx^{-1} = xx^{-1}y = ey = y \in H$*;*

Definición 3.19 (Grupo simple)**.** Un **grupo simple** es un grupo no trivial con exactamente dos subgrupos normales, el subgrupo trivial y él mismo.

Proposición 3.10. *Si* $f : G \to H$ *es un homomorfismo, entonces* $\ker f \subseteq G$ *es un subgrupo normal.*

$$\ker f \trianglelefteq G$$

Prueba 3.10.1. En efecto: $\forall a \in G \wedge b \in \ker f$

$$f(a^{-1}ba) = f(a^{-1})f(b)f(a) = f^{-1}(a)e_H f(a) = f^{-1}(a)f(a) = e_H$$

así:

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

La definición 3.18 es equivalente a decir que si H es un subgrupo normal de G, entonces las clases laterales izquierda y derecha de H son iguales, es decir:

$$H \triangleleft G \implies gH = Hg \tag{3.5}$$

La expresión Hg no es otra cosa que operar $h * g = hg \, \forall \, h \in H$ y $g \in G$.

[5] Algunos autores utilizan los términos: *coclase* o *cogrupo* en vez de *clase*.
[6] Otros llaman *coclases* a las clases laterales y *clases* a los grupos conjugados.

Ejemplo 3.9

Recordemos el grupo $(S_3, \circ)$ con la tabla 3.6, que reescribimos aquí:

$\circ$	ε	σ_1	σ_2	σ_3	ϕ_1	ϕ_2
ε	ε	σ_1	σ_2	σ_3	ϕ_1	ϕ_2
σ_1	σ_1	ε	ϕ_1	ϕ_2	σ_2	σ_3
σ_2	σ_2	ϕ_2	ε	ϕ_1	σ_3	σ_1
σ_3	σ_3	ϕ_1	ϕ_2	ε	σ_1	σ_2
ϕ_1	ϕ_1	σ_3	σ_1	σ_2	ϕ_2	ε
ϕ_2	ϕ_2	σ_2	σ_3	σ_1	ε	ϕ_1

El conjunto $H = \{\varepsilon, \sigma_1\}$ es un subgrupo de S_3, sus clases a derecha e izquierda son:

Clases a derecha	Clases a izquierda
$H = \{\varepsilon, \sigma_1\}$	$H = \{\varepsilon, \sigma_1\}$
$H\phi_1 = \{\phi_1, \sigma_2\}$	$\phi_1 H = \{\phi_1, \sigma_3\}$
$H\phi_2 = \{\phi_2, \sigma_3\}$	$\phi_2 H = \{\phi_2, \sigma_2\}$

Se observa que las clases a derecha e izquierda no son iguales, por tanto, H no es un subgrupo normal de S_3.

Definición 3.20. Producto de clases laterales

Sea $H \triangleleft G$ y sean Ha y Hb clases laterales de H definimos el producto de clases laterales derechas como $(Ha)(Hb) = Hab$.

Veamos si este producto está bien definido.

Prueba 3.10.2

Sean $a_1, a_2 \in Ha$ y $b_1, b_2 \in Hb$ se debe probar que $a_1 b_1 \in Hab$ y $a_2 b_2 \in Hab$ o, lo que es lo mismo, $a_1 b_1 \equiv_H a_2 b_2$.

Se tiene que, si

$$a_1 \in Ha \,\exists\, h_1 \in H \,|\, a_1 = h_1 a_2, \quad b_1 \in Hb \,\exists\, h_2 \in H \,|\, b_1 = h_2 b_2$$

luego:

$$a_1 b_1 = (h_1 a_2)(h_2 b_2) = h_1 (a_2 h_2) b_2$$

pero por ser H un subgrupo normal $Hg = gH \,\forall g \in G$, así

$$a_1 b_1 = h_1 (a_2 h_2) b_2 = h_1 (h_3 a_2) b_2 = (h_1 h_3) a_2 b_2 \implies (a_1 b_1)(a_2 b_2)^{-1} = h_1 h_3 \in H$$

3.1.8. Grupo cociente

Teorema 3.11. Grupo cociente

Si $H \triangleleft G$ y sea el conjunto $G/H = \{\bar{g}/g \in G\} = \{Hg/g \in G\}$, entonces G/H es un grupo bajo la operación $(Ha)(Hb) = Hab, \forall a, b \in G$.

Definición 3.21. Grupo cociente

El grupo $(G/H, *)$ a que se refiere el teorema 3.11 se llama grupo cociente de G por la relación de equivalencia compatible con $*$.

Notas

- $G/\{e\} = G$;
- $G/G = \{e\}$

Ejemplo 3.10

$(\mathbb{Z}, +)$ es un grupo abeliano. Sea H el conjunto de los múltiplos de 5, esto es, $H = \{\dots, -10, -5, 0, 5, 10, \dots\}$. Las clases laterales izquierda de H en $\mathbb{Z}$ son:

$$\begin{aligned}
\bar{0} &= 0 + H = \{\dots, -10, -5, 0, 5, 10, \dots\} \\
\bar{1} &= 1 + H = \{\dots, -9, -4, 1, 6, 11, \dots\} \\
\bar{2} &= 2 + H = \{\dots, -8, -3, 2, 7, 12, \dots\} \\
\bar{3} &= 3 + H = \{\dots, -7, -2, 3, 8, 13, \dots\} \\
\bar{4} &= 4 + H = \{\dots, -6, -1, 4, 9, 14, \dots\}
\end{aligned}$$

Notar que las clases laterales derecha $\bar{x} = H + x$ serán iguales a las izquierdas, por tanto, $(H, +)$ es un subgrupo normal, $H \triangleleft \mathbb{Z}$.

Para cualquier otro entero $n \in \mathbb{Z}$, $\bar{n} = n + H$ coincide con una de las clases anteriores. Luego, el grupo cociente $\mathbb{Z}/H = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ forma un grupo para la adición según el teorema 3.11. La siguiente es la tabla de adición:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Grupos finitos

Se G un grupo. Por definición G es finito si y sólo si $|G| = n$. Orden de un grupo finito es el número cardinal del mismo.

Definición 3.22. Índice de un subgrupo

Sea H un subgrupo del grupo finito G. El grupo cociente G/H, de las clases a izquierda de H, es finito y su cardinal se llama **índice del subgrupo** H en G.

El índice de H en el ejemplo 3.10 es igual a $|\mathbb{Z}/H| = 5$.

Teorema 3.12

Si H es un subgrupo de orden k del grupo finito G, entonces toda clase izquierda de H tiene k elementos.

H) $(G, *)$ es grupo finito; $|H| = k$.

T) $|gH| = k \; \forall g \in G$.

Prueba 3.12.1

Debemos probar que H y gH son coordinables, y para ello difinimos:

$$f : H \to gH \text{ mediante } f(a) = g * a$$

I) f es la restricción de la *translación a izquierda* $f_g : G \to G$ al subconjunto H y en consecuencia es inyectiva.

II) f es sobreyectiva, pues para todo $y \in gH$ existe $x = g' * y$ tal que:

$$f(x) = f(g' * y) = g * g' * x = x$$

En consecuencia, f es biyectiva y $|gH| = |H| = k$

Teorema 3.13. Lagrange

El orden de todo subgrupo de un grupo finito es divisor del orden del grupo.

Prueba 3.13.1

En efecto:

Si H es un subgrupo de G y $o(H) = k$ por el teorema 3.12 el cardinal de toda coclase a izquierda de H es k, y como estas son disjuntas, resulta:

$$o(G) = mk = mo(H)$$

es decir:

$$o(H) \mid o(G)$$

3.1.9. Aritmética modular

La aritmética modular es un sistema aritmético para clases de equivalencia de números enteros llamadas **clases de congruencia**. Es uno de los aportes más significativos de Gauss a la Teoría de Números, en su famoso Disquisitiones Arithmeticae (Investigaciones sobre aritmética) de 1801.

Consideremos el "reloj" de la fig 3.8. Se conoce como *enteros módulo* 4 al conjunto $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

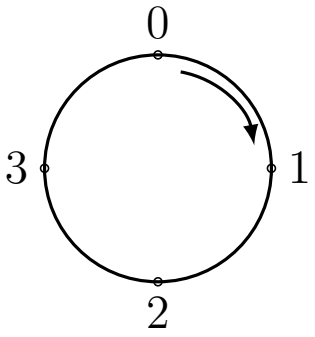


Figura 3.8. Enteros módulo 4

Veamos las operaciones de suma y multiplicación en $\mathbb{Z}_4$.

Suma

Para la operación suma se tienen los valores de la tabla 3.7.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Tabla 3.7. Enteros módulo 4 con la operación suma. Es un grupo abeliano.

La operación es cerrada ya que:

$$+ : \mathbb{Z}_4 \times \mathbb{Z}_4 \to \mathbb{Z}_4$$

Ejm: observando la tabla 3.7$(1, 3) \to 0$

G1: Es asociativa ✓

G2: Elemento neutro: 0 ✓

G3: Inversos: ✓

- 0 es su propio inverso;
- 2 es su propio inverso;
- 1 y 3 son inversos.

G4: Es conmutativa ✓

$$(\mathbb{Z}_4, +) \text{ es un grupo abeliano y finito.}$$

En general, para los enteros módulo n con la operación suma:

$$(\mathbb{Z}_n, +) \text{ es un grupo abeliano finito.}$$

Producto

- $(\mathbb{Z}_4, \cdot)$

  Para la operación producto se tienen los valores de la tabla 3.8.

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Tabla 3.8. Conjunto de enteros módulo 4 con la operación producto.

G1: Es asociativa ✓

G2: Elemento neutro: 1 ✓

G3: Inversos: ✗

$$(\mathbb{Z}_4, \cdot) \text{ no es un grupo, es un semigrupo con neutro.}$$

- $(\mathbb{Z}_4^*, \cdot)$

  Si se excluye el cero, se tiene la tabla 3.9.

$\cdot$	1	2	3
1	1	2	3
2	2	1	3
3	3	3	1

Tabla 3.9. Enteros módulo 4, excluyendo el cero $(\mathbb{Z}_4^*, \cdot)$.

G1: Es asociativa ✓

G2: Elemento neutro ✗

$$(\mathbb{Z}_4^*, \cdot) \text{ no es un grupo, es un semigrupo.}$$

- $(\mathbb{Z}_3^*, \cdot)$

  Si se excluye el cero, se tiene la tabla 3.10.

$\cdot$	1	2
1	1	2
2	2	1

Tabla 3.10. Enteros módulo 3, excluyendo el cero $(\mathbb{Z}_3^*, \cdot)$.

G1: Es asociativa ✓

G2: Elemento neutro: 1 ✓

G3: Elemento inverso: ✓

- 1 es su propio inverso;
- 2 es su propio inverso

G4: Es conmutativa: ✓

$(\mathbb{Z}_3^*, \cdot)$ es un grupo abeliano.

Proposición 3.14. $(\mathbb{Z}_p^*, \cdot)$ *es un grupo multiplicativo abeliano si y sólo si* p *es primo.*

Observemos ahora la fig. 3.9 imaginando el giro sin deslizar de la rueda, vemos que los números enteros tienen relación con $0, 1, 2$ o 3 dependiendo de su posición, esta relación es de congruencia.

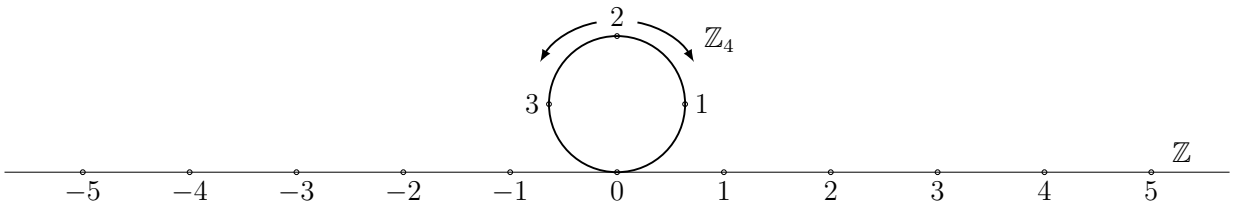


Figura 3.9

Notemos que a cada $x \in \mathbb{Z}$ le corresponderá el elemento de $\mathbb{Z}_4$ que resulta de tomar el residuo de la división de x entre 4. Los posibles residuos de la división de un entero entre 4 son 0, 1, 2, 3, en general:

Por lo tanto, podemos decir que todos los números de $\mathbb{Z}$ con el mismo residuo de la división entre 4 serán equivalentes (se puede verificar fácilmente que cumple con las propiedades de equivalencia), se dice que son congruentes módulo 4.

Por ejemplo:

$$4753 \equiv 1 \,(\text{mod } 4); \qquad 1234 \equiv 2 \,(\text{mod } 4)$$

Dos enteros $a, b \in \mathbb{Z}$ *son congruentes módulo* n *si al dividir entre* n *dan el mismo residuo.*

Proposición 3.15

La congruencia módulo n, con n entero positivo fijo, es una relación de equivalencia.

Los enteros módulo n pueden considerarse como el conjunto de clases que se forman con la relación de congruencia.

Por la definición de división sabemos que el dividendo es igual al cociente por el divisor más el residuo, por lo tanto, para dos números x, y congruentes módulo n (x, y tienen el mismo residuo), se tiene

$$\begin{array}{c} x = c_1 n + r \\ y = c_2 n + r \\ \hline x - y = (c_1 - c_2)n \end{array}$$

en consecuencia, x, y son congruentes módulo n si y sólo si n divide a $x - y$.

$$x \equiv_n y \iff n \mid x - y$$

El conjunto de números con el mismo residuo r son las **clases** de r, en el caso de $\mathbb{Z}_3$, estas son:

$$\begin{array}{ll} \text{clase del } 0: & [0] = \bar{0} = \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ \text{clase del } 1: & [1] = \bar{1} = \{\ldots, -5, -2, 1, 4, 7, \ldots\} \\ \text{clase del } 2: & [2] = \bar{2} = \{\ldots, -4, -1, 2, 5, 8, \ldots\} \end{array}$$

Se observa que hablar de, por ejemplo, la clase $\bar{4}$ es lo mismo que hablar de la clase $\bar{1}$, ya que están el mismo conjunto. Además, llamamos a 1 **representante** de la clase $\bar{1}$, 2 representante de la clase $\bar{2}$, etc.

Llamemos $3\mathbb{Z}$ al conjunto formado por los múltiplos de 3, en general $n\mathbb{Z}$ al conjunto formado por los múltiplos de n.

$\bar{0}$ es el conjunto de todos los múltiplos de 3 ($3\mathbb{Z}$), o lo que es lo mismo, el conjunto de todos los números que al dividir entre 3 dan resto nulo. $\bar{1}$ son todos los números enteros tales que al dividir entre 3 dan resto 1, análogamente para $\bar{2}$.

Se observa que $\mathbb{Z}/3\mathbb{Z}$ tiene 3 clases, $\mathbb{Z}/4\mathbb{Z}$ tendrá 4 clases, en general $\mathbb{Z}/n\mathbb{Z}$ tiene n clases de conformidad con el teorema 3.12.

Este es precisamente el conjunto cociente, es decir:

$$\frac{\mathbb{Z}}{\sim} = \mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$$

En general

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$$

Las operaciones de suma entre las clases de congruencia de $\mathbb{Z}/n\mathbb{Z}$ se ven en las tabla 3.11. Esto es, cualquier elemento, por ejemplo, de la clase del 0 (múltiplos de 3) + cualquier elemento de la clase del 1 (números enteros tales que al dividir entre 3 dan resto 1), es igual un número de la clase del 1.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Tabla 3.11. Grupo cociente $(\mathbb{Z}/3\mathbb{Z}, +)$.

Ejemplo 3.11

Sea $(\mathbb{Z}_5 \setminus \{0\}, \cdot) = (\{[1], [2], [3], [4]\}, \cdot)$.

El orden del grupo es $o(\mathbb{Z}_5 \setminus \{0\}) = 4$.

Este es un grupo multiplicativo, ya que 5 es primo[a] y sus congruencias o clases todas tienen inverso.

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

- $[1]$ es el neutro, tiene orden 1 claramente;
- $[2]$ tiene orden 4, ya que $[2^4] = [16] = [1]$ y $[2^2] = [4]$ y $[2^3] = [3]$;

  Luego, el grupo es cíclico y $[2]$ es un generador del grupo.
- $[3]$ tiene orden 4, ya que $[3^4] = [81] = [1]$ y $[3^2] = [9] = [4]$ y $[3^3] = [2]$;

  Luego $[3]$ también es un generador del grupo.
- $[4]$ tiene orden 2, ya que $[4^2] = [16] = [1]$

Notar que, en todos los casos, el orden de los elementos (que resultaron: $1, 4, 4, 2$ para $[1], [2], [3], [4]$ respectivamente), divide al orden del grupo (que es 4), como tiene que ocurrir según el teorema de Lagrange[b].

[a] Ver proposición 3.14

[b] Teorema 3.13

Ejemplo 3.12

Se proporciona la tabla de adición para $\mathbb{Z}_4$, y la tabla de multiplicación para $S = \{1, 3, 7, 9\}$ en $\mathbb{Z}_{10}$, observe que S es un conjunto reducido de residuos para los enteros módulo 10. Sea $f : \mathbb{Z}_4 \to S$ definida por:

$$f(0) = 1, \quad f(1) = 3, \quad f(2) = 9, \quad f(3) = 7$$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Muestre que f es un isomorfismo entre los grupos $(\mathbb{Z}_4, +)$ y $(S, \times)$.

Para probar que es un isomorfismo, debemos probar que es un homomorfismo biyectivo.

- **¿Es un homomorfismo?** Por definición de homomorfismo, se debe cumplir:

$$\forall a, b \in \mathbb{Z}_4; f(a), f(b) \in S \implies f(a+b) = f(a) \times f(b)$$

  Por ejemplo, notemos que:

  - $f(1+2) = f(3) = 7$ y $f(1) \times (2) = 3 \times 9 \equiv 7$
  - $f(2+3) = f(1) = 3$ y $f(2) \times f(3) = 9 \times 7 \equiv 3$

  y así se puede verificar para cualquier para de elementos, por lo que f es un homomorfismo.

- **¿Es inyectiva?** La función es inyectiva, si:

$$a \neq b \implies f(a) \neq f(b)$$

  de la defínción de f puede observarse que es así, es decir, f es inyectiva.

- **¿Es sobreyectiva?** Se observa que el codominio coincide con el rango, por lo que f es sobreyectiva.

Conclusión f es un isomorfismo entre los grupos $(\mathbb{Z}_4, +)$ y $(S, \times)$.

3.2. Anillos

Un anillo es un conjunto equipado con dos operaciones binarias, una aditiva y otra multiplicativa, que satisfacen ciertas propiedades.

Como la sustracción se puede definir en términos de la adición, vagamente hablando en un anillo se puede sumar, restar y multiplicar.

3.2.1. Definición y propiedades básicas

Definición 3.23. Anillo

La terna $(A, *, \cdot)$ es un anillo si y sólo si:

1. $(A, *)$ es un grupo abeliano;
2. $(A, \cdot)$ es un semigrupo;
3. La segunda operación $(\cdot)$ es *distributiva* a izquierda y derecha respecto de la primera $(*)$.

La definición 3.23 se traduce en los siguientes axiomas:

A1 : La adición es ley de composición interna en A: $\forall a, b \in A \implies a + b \in A$

A2 : La adición es asociativa en A: $\forall a, b, c \in A : (a + b) + c = a + (b + c)$

A3 : Existe neutro $0 \in A$ respecto a la adición: $\exists 0 \in A / \forall a \in A : a + 0 = 0 + a = a$

A4 : Todo elemento de A admite inverso aditivo:

$$\forall a \in A, \exists - a \in A / a + (-a) = (-a) + a = 0$$

A5 : La adición es conmutativa: $\forall a, b \in A : a + b = b + a$

A6 : El producto es ley de composición interna en A. $\forall a, b \in A \implies ab \in A$

A7 : El producto es asociativo. $\forall a, bc \in A : (ab)c = a(bc)$

A8 : El producto es doblemente distributivo respecto de la suma.

$$\forall a, b, c \in A : \begin{cases} a(b + c) = ab + ac \\ (b + c)a = ba + ca \end{cases}$$

Si además, ocurre que la segunda ley de composición es conmutativa, diremos que $(A, +, \cdot)$ es un **anillo conmutativo**. Si existe elemento neutro o identidad respecto del producto, que denotamos con 1, entonces se llamará **anillo con identidad o con unidad**.

Ejemplo 3.13. Los números pares $\langle 2 \rangle = 2\mathbb{Z}$ forman un anillo conmutativo sin unidad ya que $1 \notin 2\mathbb{Z}$.

Un anillo con identidad cuyos elementos no nulos son invertibles se llama **anillo de división**.

Se define la división por:

$$x \div y \coloneqq x \times y^{-1}$$

Ejemplo 3.14

Tres importantes anillos:

1. **Anillo de los números enteros ($\mathbb{Z}$)**: Este es un ejemplo fundamental de un anillo conmutativo con unidad. El conjunto de números enteros, $\mathbb{Z}$, es un anillo con las operaciones usuales de suma y multiplicación.

2. **Anillo de Polinomios ($A[x]$)** : El conjunto de polinomios con coeficientes en un anillo, forma un anillo conmutativo con unidad. En este anillo, la suma y la multiplicación de polinomios satisfacen todas las propiedades de un anillo. Por ejemplo, el anillo de polinomios reales $\mathbb{R}[x]$ o el anillo de polinomios enteros $\mathbb{Z}[x]$ son ejemplos de anillos de polinomios. Nos extenderemos más sobre esto en la sección 3.2.4.

3. **Anillo de Matrices ($\mathbf{M}_n(\mathbb{K})$)** (con $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$)lo A, de matrices cuadradas $n \times n$ con coeficientes en $\mathbb{K}$, es un anillo unitario no conmutativo. Ver sección 3.2.3.

Proposición 3.16. *El producto de cualquier elemento de un anillo por el neutro de la primera ley es igual a éste.*

H) $(A, +, \cdot)$ *es anillo.*

T) $a \cdot 0 = 0 \cdot a = 0$

Prueba 3.16.1. Por ser anillo: $\forall x \in A : x + 0 = x$

Premultiplicando por a y aplicando distributiva: $a(x + 0) = ax + a0 = ax$, de donde

$$a0 = 0$$

Análogamente se prueba $0a = 0$.

Proposición 3.17. *En todo anillo, el producto del opuesto de un elemento, por otro, es igual al opuesto de su producto.*

H) $(A, +, \cdot)$ *es anillo.*

T) $\forall a, b \in A : (-a) \cdot b = -(ab)$

Prueba 3.17.1. Por distributividad y producto por 0: $(-a)b + ab = (-a + a)b = 0b = 0$;

De donde, debe ser: $(-a)b = -(ab)$

De manera similar se prueba que $a(-b) = -(ab)$

Proposición 3.18. *En todo anillo, el producto de los opuestos de dos elementos es igual al producto de los mismos.*

H) $(A, +, \cdot)$ *es anillo.*

T) $\forall a, b \in A : (-a)(-b) = ab$

Prueba 3.18.1. Aplicando dos veces la proposición 3,17 y por opuesto del opuesto, resulta:

$$(-a)(-b) = -[a(-b)] = -[-(ab)] = ab$$

Tarea. Probar que:

a) $a(b - c) = ab - ac \quad \wedge \quad (b - c)a = ba - ca$

b) Si el anillo es unitario:

   i) $(-1)a = a$

   ii) $(1)(-1) = 1$

Teorema 3.19. Unicidad de la unidad y los inversos

Si el anillo tiene unidad, esta es única. En un anillo de división, cada elemento tiene un inverso único.

Definición 3.24. Subanillo

Un subconjunto no vacío S de A se llama **subanillo** de A si S mismo forma un anillo para las operaciones de A.

Observamos que S es un subanillo de A si y sólo si

$$a, b \in S \implies a + b \in S \wedge ab \in S$$

Notas:

- $\{0\}$ y A son subanillos de cualquier anillo A. $\{0\}$ es llamado **anillo trivial**;
- Para todo entero positivo n, el conjunto:

  $$n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$$

  es un subanillo de $\mathbb{Z}$.
- $\{0, 2, 4\}$ es un subanillo de $\mathbb{Z}_6$. Note que, aunque 1 es la unidad en $\mathbb{Z}_6$, 4 es la unidad en $\{0, 2, 4\}$.
- El conjunto de las matrices diagonales es un subanillo de las matrices $n-$cuadradas sobre $\mathbb{R}$.

Anillos sin divisores de cero

Los anillos sin divisores de cero son una clase especial de anillos. Un anillo se considera "sin divisores de cero" cuando no contiene elementos distintos de cero que, cuando se multiplican, dan como resultado cero sin ser ellos mismos cero. En otras palabras, en un anillo sin divisores de cero, si a y b son elementos del anillo y su producto $ab = 0$, entonces a y/o b deben ser cero.

Definición 3.25. Anillos sin divisores de cero

El anillo $(A, +, \cdot)$ no tiene divisores de cero si y sólo si elementos no nulos dan producto no nulo. En símbolos:

$$(A, +, \cdot) \text{ carece de divisores de cero} \iff \forall x, y \in A : x \neq 0 \wedge y \neq 0 \implies x \cdot y \neq 0$$

Equivalentemente, por medio de implicación contrarrecíproca, se tiene:

$$(A, +, \cdot) \text{ carece de divisores de cero} \iff \forall x, y \in A : x \cdot y = 0 \implies x = 0 \vee y = 0$$

Definición 3.26. Coprimos

Dos elementos a y b de A son **coprimos** (o primos entre sí) si todo común divisor de a y b es inversible.

En $\mathbb{Z}$, los enteros 2 y 3 admiten a -1 y 1 como divisores comunes. Estos son los únicos elementos inversibles en $\mathbb{Z}$, y se dice que 2 y 3 son coprimos o primos entre sí.

Teorema 3.20

El anillo $(\mathbb{Z}_n, +, \cdot)$ no tiene divisores de cero si y sólo si n es primo.

Prueba 3.20.1

- **Parte 1**: Si n es primo, entonces el anillo no tiene divisores de cero

  Supongamos que n es un número primo. Queremos demostrar que en el anillo $(\mathbb{Z}_n, +, \cdot)$, no existen divisores de cero, es decir, no hay elementos $a, b \in \mathbb{Z}_n$ tales que $a \cdot b \equiv 0 \mod n$ con $a \not\equiv 0 \mod n$ y $b \not\equiv 0 \mod n$.

  Dado que n es primo, los únicos elementos no nulos en $\mathbb{Z}_n$ son aquellos que son coprimos con n. Esto significa que si a y b no son congruentes con 0 módulo n, entonces a y b son coprimos con n. En otras palabras, el máximo común divisor de a y n es 1, y el máximo común divisor de b y n también es 1.

  Ahora, si $a \cdot b \equiv 0 \mod n$, esto implicaría que el producto de a y b es divisible por n. Sin embargo, debido a que n es primo y a y b son coprimos con n, el producto $a \cdot b$ no puede ser divisible por n, a menos que uno de los factores sea divisible por n, lo cual es una contradicción. Por lo tanto, no existen divisores de cero en $\mathbb{Z}_n$ cuando n es primo.

- **Parte 2**: Si n no es primo, entonces el anillo tiene divisores de cero.

  Supongamos que n no es un número primo. Queremos encontrar elementos a y b en $\mathbb{Z}_n$ tales que $a \cdot b \equiv 0 \mod n$ y $a \not\equiv 0 \mod n$ y $b \not\equiv 0 \mod n$.

  Si n no es primo, entonces podemos escribir n como el producto de dos enteros positivos $n = p \cdot q$, donde p y q son enteros mayores que 1.

  Ahora, consideremos los elementos a y b en $\mathbb{Z}_n$ de la siguiente manera:

  $$a = [p]_n \text{ y } b = [q]_n$$

  Aquí, $[p]_n$ y $[q]_n$ representan las clases de congruencia módulo n. Estas clases son distintas de la clase $[0]_n$ ya que p y q no son congruentes con 0 módulo n.

  Ahora veamos lo que sucede cuando multiplicamos a y b en $\mathbb{Z}_n$:

  $$a \cdot b = [p]_n \cdot [q]_n$$

Dado que p y q no son congruentes con 0 módulo n, esto significa que $p \cdot q \equiv 0$ mód n. En otras palabras, $a \cdot b$ pertenece a la clase $[0]_n$, lo que significa que $a \cdot b \equiv 0 \mod n$.

Además, dado que $p \not\equiv 0 \mod n$ y $q \not\equiv 0 \mod n$, esto implica que $a \not\equiv 0 \mod n$ y $b \not\equiv 0 \mod n$.

Por lo tanto, hemos encontrado elementos a y b en $\mathbb{Z}_n$ tales que $a \cdot b \equiv 0 \mod n$ y $a \not\equiv 0 \mod n$ y $b \not\equiv 0 \mod n$, lo que demuestra que el anillo $\mathbb{Z}_n$ tiene divisores de cero cuando n no es primo.

En resumen, hemos demostrado que si n es primo, entonces el anillo $\mathbb{Z}_n$ no tiene divisores de cero, y si n no es primo, entonces el anillo $\mathbb{Z}_n$ tiene divisores de cero. Esto establece la afirmación "si y sólo si" que estábamos buscando.

Definición 3.27. Dominio de integridad

Todo anillo conmutativo, con unidad y sin divisores de cero, se llama *dominio de integridad*.

Las ternas $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ son dominios de integridad.

El anillo $\mathbb{Z}_p$ de enteros módulo p siendo este un número primo, es un dominio de integridad.

EL anillo $\mathbb{Z}_n$ de enteros módulo n si n no es primo, no es un dominio de integridad.

Por ejemplo, en $\mathbb{Z}_6$, los números 2 y 3 son distintos de cero, pero su producto es congruente con cero módulo 6, esto es: $2 \cdot 3 \equiv 0 \mod 6$. Esto muestra que $\mathbb{Z}_6$ no es un dominio de integridad, ya que tiene elementos no nulos (2 y 3) cuyo producto es cero sin que ninguno de los factores sea cero.

Proposición 3.21 (Cancelación)**.** *Sean a, b y c elementos de un dominio de integridad. Si $a \neq 0$ y $ab = ac$, entonces $b = c$.*

Prueba 3.21.1. De $ab = bc$ se tiene $a(b - c) = 0$. Como $a \neq 0$, tiene que ser $b - c = 0$.

Unidades de un anillo

Las unidades de un anillo son elementos especiales que tienen inversos multiplicativos dentro del anillo. El conjunto de todas las unidades de un anillo A se denota a menudo como $U(A)$. Los elementos que no tienen inversos multiplicativos se llaman elementos no invertibles o no unidades.

Definición 3.28. Unidades de un anillo

Sea A un anillo, $x \in A$ es una *unidad* si $xy = yx = 1$ para algún $y \in A$.

Ejemplo 3.15. Un ejemplo común de unidades es el conjunto de números racionales $U(\mathbb{Q}^*)$ como unidades en el anillo de los números racionales $(\mathbb{Q})$. Cada número no nulo en $\mathbb{Q}$ tiene un inverso multiplicativo en $\mathbb{Q}$, lo que significa que $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.

Ejemplo 3.16. En el anillo de los números enteros ($\mathbb{Z}$), las unidades son $\{1, -1\}$, ya que solo estos dos números tienen inversos multiplicativos en $\mathbb{Z}$. Otros números enteros no tienen inversos multiplicativos en $\mathbb{Z}$, por ejemplo, no hay ningún número entero cuyo producto con 2 sea igual a 1, el elemento neutro multiplicativo.

Ejemplo 3.17

Sea el anillo de los enteros módulo 10 $(Z_{10}, +, \times)$. Por el teorema 3.20, este anillo tiene divisores de cero, los cuales están resaltados en la tabla 3.12, por ejemplo: $2 \times 5 \equiv 0$ mód 10; $5 \times 6 \equiv 0$ mód 10.

Sus unidades son $U(10) = \{1, 3, 7, 9\}$, pues por ejemplo $3 \times 7 = 1$ mód 10; $9 \times 9 = 1$ mód 10;

Las no unidades o no invertibles son: $\{0, 2, 4, 5, 6, 8\}$

$\times$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Tabla 3.12. Tabla de Cayley de $(\mathbb{Z}_{10}, \times)$.

Ejemplo 3.18

La existencia de divisores de cero en un anillo causa resultados inusuales cuando se buscan los ceros de polinomios con coeficientes en el anillo.

Consideremos por ejemplo, la ecuación $x^2 - 4x + 3 = 0$. En el conjunto de los enteros, podemos encontrar las soluciones factorizando:

$$x^2 - 4x + 3 = 0 = (x - 3)(x - 1) = 0$$

tiene dos soluciones en los enteros: $x = 3$ y $x = 1$. Sin embargo, en $\mathbb{Z}_{12}$, la ecuación tiene cuatro soluciones: $x = 1$, $x = 3$, $x = 7$, y $x = 9$.

Esto se debe a que en $\mathbb{Z}_{12}$, $2 \cdot 6 = 0$, $3 \cdot 4 = 0$, $4 \cdot 6 = 0$, $6 \cdot 8 = 0$, y así sucesivamente. Estos productos son 0 porque 2, 3, 4, y 6 son divisores de cero en $\mathbb{Z}_{12}$.

En los dominios de integridad, como $\mathbb{Z}$, $\mathbb{Z}_{11}$ y $\mathbb{Z}_{13}$ ($\mathbb{Z}_p$, p primo), no hay divisores de cero. Por lo tanto, podemos encontrar todos los ceros de un polinomio con coeficientes

en un dominio de integridad simplemente factorizando el polinomio y luego igualando cada factor a 0.

3.2.2. Homomorfismo de anillos

Un homomorfismo de anillos es una función que preserva la estructura algebraica entre dos anillos.

Definición 3.29. Homomorfismo de anillos

Dados dos anillos $(A, +, \cdot)$ y $(B, +, \cdot)$. La aplicación $f : A \to B$ es un homomorfismo de anillos si se cumplen las siguientes condiciones:

1. $f(a + b) = f(a) + f(b), \forall a, b \in A$;
2. $f(a \cdot b) = f(a) \cdot f(b), \forall a, b \in A$

En el contexto de los homomorfismos de anillos, se utilizan términos similares a los que se emplean en los homomorfismos de grupos. De esta manera, un homomorfismo que conserva la inyectividad se llama **monomorfismo**, y un homomorfismo que es reversible o invertible se denomina **isomorfismo**. Un homomorfismo que mapea un anillo A en sí mismo se conoce como **endomorfismo**, y un isomorfismo que relaciona un anillo A consigo mismo se llama **automorfismo**.

Ejemplo 3.19

Consideremos el anillo de los polinomios en una variable x con coeficientes reales, $\mathbb{R}[x]$. La función $\phi : \mathbb{R}[x] \to \mathbb{R}$ que asigna a cada polinomio su valor en $x = 0$ es un homomorfismo de anillos.

Para ver esto, note que para cualquier para de polinomios $p(x)$ y $q(x)$, tenemos:

$$\phi\left(p(x) + q(x)\right) = p(0) + q(0) = \phi(p(x)) + \phi(q(x))$$

y:

$$\phi\left(p(x) \cdot q(x)\right) = p(0) \cdot q(0) = \phi\left(p(x)\right) \cdot \left(q(x)\right)$$

Por lo tanto, ϕ cumple las condiciones de un homomorfismo de anillos.

En particular, $\phi(x^2 + 2x + 1) = (0)^2 + 2(0) + 1 = 1$.

3.2.3. Anillo de matrices

Se vió en 3.1.3, que el conjunto de matrices con coeficientes reales y la operación suma $(\mathbf{M}_{m\times n}(\mathbb{R}), +)$ es un grupo abeliano, en particular, para matrices cuadradas $m = n$ $(\mathbf{M}_n(\mathbb{R}), +)$ es un grupo abeliano y $(\mathbf{M}_n(\mathbb{R}), \cdot)$ es un semigrupo con elemento neutro.

Matrices cuadradas

A1 Cerrada bajo la suma: $A, B \in \mathbb{R}^{n\times n} \implies A + B \in \mathbb{R}^{n\times n}$ ✓

A2 Asociatividad con la suma: $(A + B) + C = A + (B + C)$ ✓

A3 Existencia del opuesto: $\exists N \in \mathbb{R}^{n\times n} / \forall A \in \mathbb{R}^{n\times n} : A + N = N + A = A$ ✓

A4 Inversos aditivos: $\forall A \in \mathbb{R}^{n\times n}, \exists(-A) \in \mathbb{R}^{n\times n} / A + (-A) = (-A) + A = N$ ✓

A5 Conmutatividad de la adición: $A + B = B + A$ ✓

A6 Cerrado bajo el producto: $A \in \mathbb{R}^{n\times n} \wedge B \in \mathbb{R}^{n\times n} \implies AB \in \mathbb{R}^{n\times n}$ ✓

A7 Asociatividad con el producto: $(AB)C = A(BC)$ ✓

A8 Propiedad distributiva: $A(B + C) = AB + AC \wedge (B + C)A = BA + CA$ ✓

A9 Identidad: $\exists I \in \mathbb{R}^{n\times n} / \forall A \in \mathbb{R}^{n\times n} : AI = IA = A$ ✓

A10 Conmutatividad: $AB \neq BA$ ✗

Existen divisores de cero, es decir, matrices no nulas pueden dar producto no nulo. Por ejemplo, en el caso $(\mathbb{R}^{2\times 2}, +, \cdot)$:

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \neq N \quad \text{y} \quad B = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \neq N$$

y, sin embargo:

$$AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = N$$

Se trata de un anillo no conmutativo, con identidad y divisores de cero.

Ejemplo 3.20

Determinar si la aplicación entre dos anillos $(\mathbb{Z}, +_Z, \cdot_Z)$ y $(\mathbf{M}_2(\mathbb{R}), +_M, \cdot_M)$ dado por $f : \mathbb{Z} \to \mathbf{M}_2(\mathbb{R})$

$$f(n) = \begin{bmatrix} n & 0 \\ 0 & -n \end{bmatrix}$$

es un homomorfismo de anillos.

Es un homomorfismo de anillos, si cumple:

I) $f(n +_Z m) = f(n) +_M f(m)$ ✓

$$f(n +_Z m) = \begin{bmatrix} n +_Z m & 0 \\ 0 & -(n +_Z m) \end{bmatrix} = \begin{bmatrix} n +_Z m & 0 \\ 0 & -n +_Z m \end{bmatrix}$$

$$= \begin{bmatrix} n & 0 \\ 0 & -n \end{bmatrix} +_M \begin{bmatrix} m & 0 \\ 0 & -m \end{bmatrix} = f(n) +_M f(m)$$

II) $f(n \cdot_Z m) = f(n) \cdot_M f(m)$ ✗

$$f(n) \cdot_M f(m) = \begin{bmatrix} n & 0 \\ 0 & -n \end{bmatrix} \begin{bmatrix} m & 0 \\ 0 & -m \end{bmatrix} = \begin{bmatrix} n \cdot_Z m & 0 \\ 0 & n \cdot_Z m \end{bmatrix}$$

$$\neq \begin{bmatrix} n \cdot_Z m & 0 \\ 0 & -(n \cdot_Z m) \end{bmatrix} = f(n \cdot_Z m)$$

No es un homomorfismo de anillos.

3.2.4. Anillo de polinomios

En general, en los libros de álgebra, los polinomios se presentan como una expresión del tipo:

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \tag{3.6}$$

en donde cada $a_i, i = 0, 1, 2, \ldots, n$ es un número real o complejo. Ahora bien, la naturaleza de los "objetos" $x, x^2, \ldots, x^n$ está en discusión. Por ejemplo:

$$1 - 3\pi + 4\pi^2 - 7\pi^4$$

donde los coeficientes $(1, -3, 4, 0, -7)$ de las potencias de π están en $\mathbb{Z}$ pero, obviamente π y sus potencias no lo están, por lo que la expresión del polinomio no tiene sentido en $\mathbb{Z}$.

(3.6) sugiere la existencia de un conjunto "mayor" que contenga los coeficientes a_i, y un objeto especial, a saber x, no perteneciente al conjunto de los coeficientes.

Consideraciones importantes:

- Haremos la distinción entre polinomios, como (3.6) y funciones polinomiales como $P(x) = 2 + 3x - 5x^2$ que representa un valor numérico de esa expresión, para algún valor de la variable x.
- Se entenderá a los polinomios como *secuencias finitas* del tipo $(a_0, a_1, \ldots, a_n, 0, 0, \ldots)$
- Reinterpretamos a x^i, no como la potencia de un número, sino como la posición del coeficiente a_i en la secuencia.

Ahora, hagamos un repaso de la suma y multiplicación de polinomios.

Ejemplo 3.21. Repaso de suma y multiplicación de polinomios

Consideremos los polinomios $p = a_0 + a_1x + a_2x^2$ y $q = b_0 + b_1x + b_2x^2$

- Suma

  $$p + q = c_0 + c_1x + c_2x^2 = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2$$

  en general:

  $$c_i = a_i + b_i$$

- Multiplicación

  $$\begin{aligned} pq =& (a_0 + a_1x + a_2x^2)(b_0 + b_1x + b_2x^2) \\ =& a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + (a_1b_2 + a_2b_1)x^3 + a_2b_2x^4 \\ =& c_0 + c_1x + c_2x^2 + c_3x^3 + c_4x^4 \end{aligned}$$

  Se observa que la suma de los subíndices de los coeficientes, siempre es igual al exponente de x, es decir, los términos entre paréntesis son de la forma $a_jb_{i-j}x^i$

y se puede escribir, por ejemplo:

$$c_3 = a_1b_2 + a_2b_1 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0$$

considerando que $a_3 = b_3 = 0$ para en general poner:

$$c_i = \sum_{j=0}^{i} a_j b_{i-j} x^i$$

Los subíndices de a *ascienden* y los de b *descienden*.

Ahora estamos listos para analizar anillos de polinomios.

Sucesión de elementos de un anillo

Consideremos un anillo conmutativo A, y una sucesión de elementos de A, $(a_i)_{i\in\mathbb{N}}$, que cumplen $a_{n+1} = 0$ desde un cierto n en adelante, es decir:

$$(a_i)_{i\in\mathbb{N}} = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots)$$

Operaciones internas

Consideremos dado el anillo conmutativo A, y dos sucesiones de elementos de A, $(a_i)_{i\in\mathbb{N}}$ y $(b_i)_{i\in\mathbb{N}}$. Las operaciones internas están dadas por:

- Suma: $(a_i)_{i\in\mathbb{N}} + (b_i)_{i\in\mathbb{N}} = (a_0 + b_0, a_1 + b_1, \dots)$
- Multiplicación: $(a_i)_{i\in\mathbb{N}} \cdot (b_i)_{i\in\mathbb{N}} = (a_0b_0,\ a_0b_1 + a_1b_0,\ \dots,\ a_0b_k + a_1b_{k-1} + \cdots + a_kb_0, \dots)$

Teorema 3.22

Sea A^* el conjunto formado por todas las sucesiones $(a_i)_{i\in\mathbb{N}}$ definidas anteriormente, entonces la terna $(A^*, +, \cdot)$, con las operaciones internas definidas anteriormente, tiene estructura de anillo conmutativo.

El elemento x

Designemos mediante x al elemento del anillo $(A^*, +, \cdot)$ dado por:

$$x = (0, 1, 0, 0, \dots)$$

Entonces:

$$x^n = (0, 0, \dots, 0, \overbrace{1}^{n+1}, 0, \dots)$$

El anillo $A[x]$

A la terna $(A^*, +, \cdot)$ la denominamos anillos de los polinomios de variable x y la denotamos por $A[x]$

$$(a_i)_{i\in\mathbb{N}} = a_0 + a_1x + a_2x^2 + \cdots + a_bx^n = \sum_{i=0}^{n} a_i x^i$$

El anillo $\mathbb{Z}[x]$

El anillo $\mathbb{Z}[x]$ lo constituyen los polinomios de coeficientes enteros.

Ejemplo 3.22. Son polinomios de coeficientes enteros:

- $2 + 3x - 4x^3$
- $x^6 + x^7$
- $-6 + 4x^3 - 25x^8 + x^{35}$

Notación con sumatorias

$$A[x] = (a_i)_{i\in\mathbb{N}} = \sum_{i=0}^{n} a_i x^i$$

Las operaciones en $A[x]$ se pueden poner como:

- $(a_i)_{i\in\mathbb{N}} + (b_i)_{i\in\mathbb{N}} = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{\text{máx}(n,m)} a_i x^i$
- $a(x) \cdot b(x) = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j b_{i-j} x^i \right)$

Ejemplo 3.23

Consideremos los polinomios $f(x) = 2 + 2x + x^2 + 2x^3$, $g(x) = 1 + 2x + 2x^2$ en $\mathbb{Z}_3[x]$. Luego, en la notación precedente:

- $f(x) = (a_i)_{i\in\mathbb{N}} = (2, 2, 1, 2, 0, \dots)$
- $g(x) = (b_i)_{i\in\mathbb{N}} = (1, 2, 2, 0, 0, \dots)$

El grado de $f(x)$ es $n = 3$ y el grado de $g(x)$ es $m = 2$, por lo tanto, la suma va hasta el término de grado $\text{máx}(3, 2) = 3$ y la multiplicación hasta el grado $3 + 2 = 5$.

Observemos también que, por lo dicho precedentemente, $a_i = 0\ \forall i > 3$ y $b_i = 0\ \forall i > 2$.

La suma y la multiplicación de estos polinomios, en $\mathbb{Z}_3[x]$, son respectivamente:

- Suma: $f(x) + g(x) = (0, 1, 0, 2, 0, \dots) = x + 2x^3$
- Multiplicación: $c_i = \sum_{j=0}^{i} a_j b_{i-j}$

$$\begin{aligned}
c_0 &= a_0 b_0 = 2 \times 1 \equiv 2 \\
c_1 &= a_0 b_1 + a_1 b_0 = 2 \times 1 + 2 \times 2 \equiv 0 \\
c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0 = 1 \times 1 + 2 \times 2 + 2 \times 2 \equiv 0 \\
c_3 &= a_1 b_2 + a_2 b_1 + a_3 b_0 = 2 \times 1 + 1 \times 2 + 2 \times 2 \equiv 2 \\
c_4 &= a_2 b_2 + a_3 b_1 = 2 \times 2 + 1 \times 2 \equiv 0 \\
c_5 &= a_3 b_2 = 2 \times 2 \equiv 1
\end{aligned}$$

$$f(x)g(x) = (2, 0, 0, 2, 0, 1, 0, \dots) = 2 + 2x^3 + x^5$$

Definición 3.30. Anillos de polinomios con varias indeterminadas

Definimos el anillo de polinomios $A[x_1, \ldots, x_n]$ con n indeterminadas con coeficientes en el anillo A inductivamente por

$$\begin{aligned} A[x_1, x_2] &\equiv (A[x_1])\,[x_2] \\ A[x_1, x_2, x_3] &\equiv (A[x_1, x_2])\,[x_3] \\ &\vdots \\ A[x_1, \ldots, x_n] &\equiv (A[x_1, \ldots x_{n-1}])\,[x_n] \end{aligned}$$

es decir:

$$A[x_1, \ldots, x_n] \equiv A[x_1][x_2] \cdots [x_{n-1}][x_n]$$

y los polinomios de $A[x_1, \ldots, x_n]$ se expresan como suma de monomios

$$p(x_1, \ldots, x_n) = \sum a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$$

donde $a_{i_1,\ldots,i_n} \in A$ son los coeficientes.

Nota: De acuerdo con la definición, es claro que dos polinomios son iguales si y sólo si, lo son todos los coeficientes de ambos.

Ejemplo 3.24

Sea un anillo A conmutativo. Consideremos el anillo $A[x, y]$ de polinomios en dos indeterminadas y con coeficientes en A. Cualquier elemento de $A[x, y]$ es de la forma

$$p(x, y) = \sum_{i,j} a_{ij} x^i y^j$$

que puede verse como

$$A[x, y] = p(x, y) = \sum_{i,j} \left(a_{ij} x^i\right) y^j = ((a_i)_j)_{i,j\in\mathbb{N}} = A[x][y]$$

3.2.5. Ideales

Los ideales son a los anillos lo que los subgrupos normales a los grupos.

Supongamos un anillo A y un subconjunto $I \subseteq A$, la pregunta es:

¿Qué propiedades debe tener I de manera el conjunto de clases de I sea un anillo?

Como $(A, +)$ es un grupo abeliano $\implies$ $(I, +) \trianglelefteq (A, +)$, es decir por (3.5), $(I, +)$ debe ser un subgrupo normal de $(A, +)$.

En general, como $(A, +)$ es abeliano todo subgrupo es normal[7], por lo tanto el primer requerimiento para $(I, +)$ es que sea un subgrupo de $(A, +)$.

$$(I, +) \leq (A, +)$$

[7] Ver proposición 3.9.

Ahora bien, para construir el grupo cociente A/I con la operación de adición (por ejemplo la clase de $x \in A$ será $\bar{x} = x+I \in A/I$), como A es un anillo, debemos buscar la posibilidad de multiplicar entre sí los elementos de A/I tal que el resultado esté en A/I, es decir:

$$\forall x, y \in A : (x + I)(y + I) = xy + I$$

Veamos qué debe pasar para que esto se cumpla. Tomemos cualesquiera $i_1, i_2 \in I$

$$(x + i_1)(y + i_2) = xy + i_1y + xi_2 + i_1i_2 \implies i_1y + xi_2 + i_1i_2 = i_3 \in I$$

si queremos que i_3 pertenezca a I, cada término de la última igualdad debe pertenecer a I, y por lo tanto le pertenecerá la suma, pues ya hemos impuesto que $(I, +)$ sea un subgrupo.

Si $i_1i_2 \in I$, debemos suponer que I es un subanillo de A, luego para que la multiplicación sea cerrada, se debe cumplir además $i_1y, xi_2 \in I$, en otras palabras I debe *absorber* la multiplicación con los elementos de A, por derecha y por izquierda.

Definición 3.31. Ideales

Dado un anillo A, un subanillo $I \leq A$ se denomina **ideal por derecha** si:

$$a \in I \implies xa \in I, \forall x \in A$$

e **ideal por izquierda** si

$$a \in I \implies ax \in I, \forall x \in A$$

Se dice simplemente **ideal**, si lo es por derecha e izquierda.

Claramente, si el anillo es conmutativo, la distinción de ideales laterales es inconsecuente.

Teorema 3.23. Test de ideales

Un subconjunto no vacío I de un anillo A es un ideal si:

- $a - b \in I$, $\forall a, b \in I$ (ver teorema 3.4);
- $xa, ax \in I$, $\forall a \in I \wedge \forall x \in A$ (por definición 3.31 de ideales).

Ejemplo 3.25. Para todo anillo A, $\{0\}$ y A son ideales de A. El $\{0\}$ es llamado ideal *trivial*.

Ejemplo 3.26. Para cualquier entero positivo n, el conjunto $n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$ es un ideal de $\mathbb{Z}$.

3.2.6. Anillo cociente

Teorema 3.24. Existencia del anillo cociente

Sea R un anillo y A un subanillo de R. El conjunto de clases $\{r + A \,|\, r \in R\}$ es un anillo bajo las operaciones $(s + A) + (t + A) = s + t + A$ y $(s + A)(t + A) = st + A$ si y sólo si A es un ideal de R.

Prueba 3.24.1. Se demuestra con la discusión dada en la introducción a ideales, sección 3.2.5.

Ejemplo 3.27

Sea $\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = \{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$.

Por el ejemplo 3.26, $4\mathbb{Z}$ es un ideal de $\mathbb{Z}$ por tanto $\mathbb{Z}/4\mathbb{Z}$ es efectivamente un anillo cociente.

Para ver cómo sumar y multiplicar, consideremos $\bar{2}$ y $\bar{3}$:

$$\bar{2} + \bar{3} = (2 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = 5 + 4\mathbb{Z} = 1 + 4 + 4\mathbb{Z} = 1 + 4\mathbb{Z} = \bar{1}$$

$$\bar{2} \times \bar{3} = (2 + 4\mathbb{Z})(3 + 4\mathbb{Z}) = 6 + 4\mathbb{Z} = 2 + 4 + 4\mathbb{Z} = 2 + 4\mathbb{Z} = \bar{2}$$

se concluye que las operaciones son básicamente las mismas que en aritmética módulo 4.

Ejemplo 3.28

Sea $2\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{2}, \bar{4}\} = \{0 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, 4 + 6\mathbb{Z}\}$.

Por el ejemplo 3.27, aquí efectuamos las operaciones como en aritmética módulo 6.

Por ejemplo:

$$\bar{4} + \bar{4} = (4 + 6\mathbb{Z}) + (4 + 6\mathbb{Z}) = 2 + 6\mathbb{Z} = \bar{2}$$

$$\bar{4} \times \bar{4} = (4 + 6\mathbb{Z})(4 + 6\mathbb{Z}) = 4 + 6\mathbb{Z} = \bar{4}$$

3.3. Cuerpos

También llamados *campos*. Los cuerpos son estructuras algebraicas más específicas y más ricas en propiedades que los anillos y los grupos. En la fig. 3.10 se ve un esquema que relaciona estas estructuras.

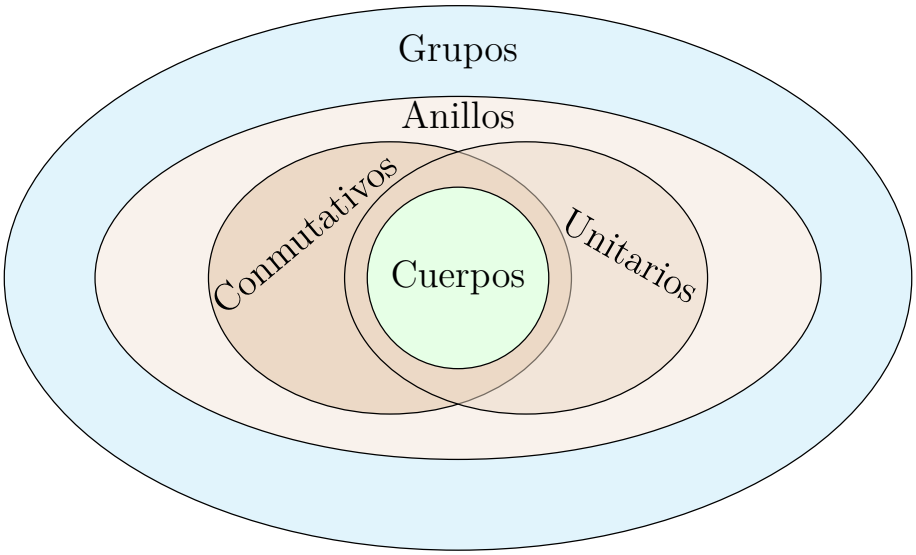


Figura 3.10. Diagrama de Venn de estructuras algebraicas.

¿Qué conjuntos nos permiten sumar, restar, multiplicar y dividir? Veamos la tabla 3.13:

	Adición					**Multiplicación**				
	Cerrado	Asoc.	0	Op.	Conm.	Cerrado	Asoc.	1	Conm.	Inv.
$\mathbb{Z}$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
$\mathbb{R}^{2\times 3}$	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗
$\mathbb{R}^{2\times 2}$	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
$\mathbb{Q}$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathbb{Z}_5$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathbb{Z}_6$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗

Tabla 3.13

Los conjuntos $\mathbb{Q}$: números racionales y $\mathbb{Z}_5$: enteros módulo 5, tienen en común las siguientes propiedades:

- Forman grupos conmutativos para la adición;
- Son cerrados para la operación de multiplicación, i.e. son anillos;
- $ab = ba \implies$ son anillos conmutativos;
- Los elementos distintos de 0, tienen inversos multiplicativos (permiten la división).

3.3.1. Definición y propiedades básicas

Definición 3.32. Cuerpo

Sea $(\mathbb{K}, +, \cdot)$ un anillo unitario conmutativo, y denotemos mediante $1 \in \mathbb{K}$ el elemento unidad. Diremos que $(\mathbb{K}, +, \cdot)$ es un **cuerpo** si para todo elemento $x \in \mathbb{K}$ distinto del neutro aditivo (el cual denotaremos con 0) existe un elemento $x^{-1} \in \mathbb{K}$ tal que $xx^{-1} = 1$.

Axiomas de cuerpo

La definición 3.32 se traduce en axiomas. Sea $\mathbb{K}$ un conjunto no vacío dotado de dos operaciones internas, que llamaremos suma ($+$) y producto ($\cdot$), que cumplen los siguientes axiomas:

1. **Axiomas de la Suma**

   (A1) *Asociatividad de la suma.*

   $\forall a, b, c \in \mathbb{K}$:

   $$(a + b) + c = a + (b + c)$$

   (A2) *Conmutatividad de la suma*:

   $\forall a, b \in \mathbb{K}$:

   $$a + b = b + a$$

   (A3) *Existencia del elemento neutro de la suma*:

   Existe un elemento en $\mathbb{K}$, denotado por 0, tal que $\forall a \in \mathbb{K}$:

   $$a + 0 = a$$

   (A4) *Existencia de elemento inverso de la suma*:

   $\forall a \in \mathbb{K}$, existe un elemento en $\mathbb{K}$, denotado por $-a$, tal que:

   $$a + (-a) = 0$$

2. **Axiomas del Producto**

   (M1) *Asociatividad del producto*:

   $\forall a, b, c \in \mathbb{K}$:

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

   (M2) *Conmutatividad del producto*:

   $\forall a, b \in \mathbb{K}$:

   $$a \cdot b = b \cdot a$$

   (M3) *Existencia de elemento neutro del producto*:

   Existe un elemento en $\mathbb{K}$, denotado por 1, distinto de 0, tal que $\forall a \in \mathbb{K}$:

   $$a \cdot 1 = a$$

   (M4) *Existencia de elemento inverso del producto*:

   $\forall a \in \mathbb{K}$, con $a \neq 0$, existe un elemento en $\mathbb{K}$, denotado por a^{-1}, tal que:

   $$a \cdot a^{-1} = 1$$

3. **Axioma de Distributividad**

(D) *Distributividad del producto respecto de la suma*:

$\forall a, b, c \in \mathbb{K}$:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

3.3.2. Propiedades generales

Sea $(\mathbb{K}, +, \cdot)$ un cuerpo. Algunas de sus propiedades generales son las siguientes:

1. **Unicidad de los elementos neutros**: El elemento neutro de la suma (0) y el elemento neutro del producto (1) son únicos.
2. **Unicidad de los elementos inversos**: Para cada elemento $a \in K$, su inverso aditivo $-a$ y, si $a \neq 0$, su inverso multiplicativo a^{-1} son únicos.
3. **Ley de cancelación para la suma**: $\forall a, b, c \in K$, si $a + c = b + c$, entonces $a = b$.
4. **Ley de cancelación para el producto**: $\forall a, b, c \in K$ con $c \neq 0$, si $a \cdot c = b \cdot c$, entonces $a = b$.
5. **Producto por cero**: $\forall a \in K$, se cumple que $a \cdot 0 = 0$.
6. **Solubilidad única de ecuaciones lineales**: Si $a \neq 0$, entonces la ecuación $ax = b$ admite solución y es única en $\mathbb{K}$;
7. **Regla de los signos**: $\forall a, b \in K$:
   - $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$
   - $(-a) \cdot (-b) = a \cdot b$
8. **No existen divisores de cero**: Si $a, b \in K$ y $a \cdot b = 0$, entonces $a = 0$ o $b = 0$.
9. **Elemento opuesto del opuesto**: $\forall a \in K$, se cumple que $-(-a) = a$.
10. **Inverso del inverso**: $\forall a \in K$ con $a \neq 0$, se cumple que $(a^{-1})^{-1} = a$

Subcuerpo

Definición 3.33. Subcuerpo

Dado un cuerpo $\mathbb{K}$, un subconjunto $\mathbb{F} \subset \mathbb{K}$ es un **subcuerpo** si es en sí mismo un cuerpo con las operaciones heredadas de $\mathbb{K}$.

3.3.3. Homomorfismo de cuerpos

Definición 3.34. Homomorfismo de cuerpos

Sean $(\mathbb{K}, +, \cdot)$, $(\mathbb{L}, +, \cdot)$ cuerpos. Una aplicación $f : \mathbb{K} \to \mathbb{L}$ se dice que es un homomorfismo entre cuerpos, si y sólo si f es un homomorfismo entre los anillos $(\mathbb{K}, +, \cdot)$ y $(\mathbb{L}, +, \cdot)$ con imagen no trivial, es decir $Im(f) \neq \{0\}$

Observaciones

De acuerdo con la definición anterior.

- f es homomorfismo entre los grupos $(\mathbb{K}, +)$ y $(\mathbb{L}, +)$;
- f es homomorfismo entre los grupos $(\mathbb{K}^* = \mathbb{K} \setminus \{0\}, \cdot)$ y $(\mathbb{L}^* = \mathbb{L} \setminus \{0\}, \cdot)$.

Teorema 3.25

Sea $f : \mathbb{K} \to \mathbb{L}$ un homomorfismo de cuerpos, entonces:

a) $f(0) = 0$ y $f(-a) = -f(a)$, $\forall a \in \mathbb{K}$;

b) $f(1) = 1$ y $f(a^{-1}) = f(a)^{-1}$, $\forall a \in \mathbb{K}, a \neq 0$;

c) $Im(f)$ es un *subcuerpo* de $\mathbb{L}$;

d) f es inyectivo.

Prueba 3.25.1

a) Se deduce del hecho de ser f un homomorfismo entre los grupos aditivos de $\mathbb{K}$ y $\mathbb{L}$;

b) Se deduce del hecho de ser f un homomorfismo entre los grupos multiplicativos de $\mathbb{K}^*$ y $\mathbb{L}^*$;

c) f es un homomorfismo entre los anillos $\mathbb{K}$ y $\mathbb{L}$, por tanto $\mathrm{Im}(f)$ es un subanillo de $\mathbb{L}$ y al ser $\mathbb{L}$ anillo conmutativo, también lo es $\mathrm{Im}(f)$. Además $1 = f(1) \in \mathrm{Im}(f)$, luego $\mathrm{Im}(f)$ es también unitario.

Falta demostrar que para todo $b \in \mathrm{Im}(f)$ con $b \neq 0$ su inverso b^{-1} pertenece a $\mathrm{Im}(f)$. En efecto, si $b \in \mathrm{Im}(f)$ con $b \neq 0$, entonces $b = f(a)$ para algún $a \neq 0$ en $\mathbb{K}$ (si fuera $a = 0$, $f(a)$ sería 0). Por tanto, $b^{-1} = f(a)^{-1} = f(a^{-1}) \in \mathrm{Im}(f)$;

d) f es un homomorfismo entre los anillos $\mathbb{K}$ y $\mathbb{L}$, y por tanto $\ker f$ es un ideal de $\mathbb{K}$. Al ser $\mathbb{K}$ un cuerpo, sus únicos ideales son $\{0\}$ y $\mathbb{K}$. Si fuera $\ker f = \mathbb{K}$ entonces f sería homomorfismo nulo, o sea $\mathrm{Im}(f) = \{0\}$, en contradicción con la definición de homomorfismo entre cuerpos. Ha de ser por tanto $\ker f = \{0\}$, lo cual implica que f es inyectivo.

3.3.4. Cuerpos ordenados

Un *cuerpo ordenado* es un cuerpo $(\mathbb{K}, +, \cdot)$ en el que además se define una relación de orden total, denotada por $\leq$, que es compatible con las operaciones del cuerpo. Es decir, satisface los siguientes axiomas adicionales:

1. **Axiomas de Orden Total**

   I) *Reflexividad:* $\forall a \in K$, $a \leq a$.

   II) *Antisimetría:* $\forall a, b \in K$, si $a \leq b$ y $b \leq a$, entonces $a = b$.

   III) *Transitividad:* $\forall a, b, c \in K$, si $a \leq b$ y $b \leq c$, entonces $a \leq c$.

iv) *Totalidad:* $\forall a, b \in K$, se cumple que $a \leq b$ o $b \leq a$.

2. **Compatibilidad con las Operaciones**
   - *Compatibilidad con la suma:* $\forall a, b, c \in K$, si $a \leq b$, entonces $a + c \leq b + c$.
   - *Compatibilidad con el producto:* $\forall a, b, c \in K$, si $a \leq b$ y $0 \leq c$, entonces $a \cdot c \leq b \cdot c$.

Ejemplo 3.29. Cuerpos ordenados

- Los números racionales $\mathbb{Q}$ con el orden usual.
- Los números reales $\mathbb{R}$ con el orden usual.
- *No es un cuerpo ordenado:* El cuerpo de los números complejos $\mathbb{C}$, ya que no se puede definir un orden total en $\mathbb{C}$ que sea compatible con sus operaciones.

Observación: La existencia de un orden en un cuerpo permite introducir conceptos como positivo, negativo, valor absoluto, y desigualdades, enriqueciendo el análisis y la geometría en estos cuerpos.

Cotas

Sea $(\mathbb{K}, +, \cdot, \leq)$ un cuerpo ordenado.

- **Cota superior**: Un elemento $M \in \mathbb{K}$ es una *cota superior* de un conjunto $S \subseteq \mathbb{K}$ si $\forall s \in S$, se cumple que $s \leq M$.
- **Cota inferior**: Un elemento $m \in K$ es una *cota inferior* de un conjunto $S \subseteq \mathbb{K}$ si $\forall s \in S$, se cumple que $m \leq s$.
- **Conjunto acotado**: Un conjunto $S \subset K$ es *acotado superiormente* si tiene una cota superior, y es *acotado inferiormente* si tiene una cota inferior. Si S es acotado superior e inferiormente, se dice simplemente que es **acotado**.

Ejemplo 3.30. Cotas

Ejemplos en $\mathbb{R}$

- El conjunto $S = \{x \in \mathbb{R} : 0 < x < 1\}$ es acotado.
- Cotas superiores: Cualquier número real mayor o igual a 1.
- Cotas inferiores: Cualquier número real menor o igual a 0.
- El conjunto $\mathbb{N}$ es acotado inferiormente (cota inferior: 0), pero no superiormente.

Valor Absoluto

El **valor absoluto** de un elemento $a \in \mathbb{K}$ se define como:

$$|a| = \begin{cases} a, & \text{si } a \geq 0 \\ -a, & \text{si } a < 0 \end{cases}$$

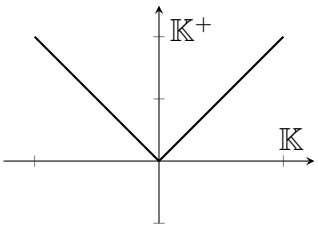


Figura 3.11. Valor absoluto

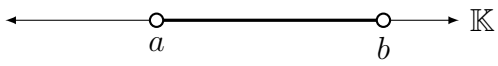
Propiedades del Valor Absoluto en un Cuerpo Ordenado

1. $|a| \geq 0, \forall a \in \mathbb{K}$.
2. $|a| = 0 \iff a = 0$.
3. $|a \cdot b| = |a| \cdot |b|, \quad \forall a, b \in \mathbb{K}$.
4. $|a + b| \leq |a| + |b|, \quad \forall a, b \in \mathbb{K}$ (desigualdad triangular).

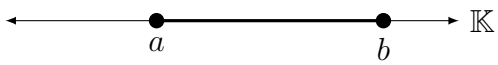
Intervalos

Sean $a, b \in \mathbb{K}$ con $a < b$. Se definen los siguientes intervalos:

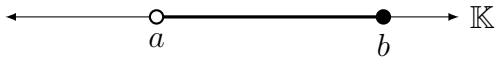
- *Intervalo abierto*: $(a, b) = \{x \in \mathbb{K} \mid a < x < b\}$



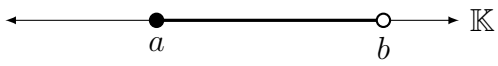
- *Intervalo cerrado*: $[a, b] = \{x \in \mathbb{K} \mid a \leq x \leq b\}$



- *Intervalos semiabiertos*:
  - $(a, b] = \{x \in \mathbb{K} \mid a < x \leq b\}$



  - $[a, b) = \{x \in \mathbb{K} \mid a \leq x < b\}$



Ejemplo 3.31. Intervalos

En $\mathbb{R}$:

- $(-2, 3)$ es un intervalo abierto por ambos lados, que representa todos los números reales estrictamente entre -2 y 3.

- $[0, 1]$ es un intervalo cerrado por ambos lados, representa todos los números reales entre 0 y 1, incluyendo 0 y 1.

Bibliografía

[1] Armando O. Rojo. «Álgebra I». 8.ª ed. El Ateneo, mar. de 1981, págs. 498-498 (vid. págs. 19, 76, 93).

[2] AL GABR. «Curso de teoría de grupos». 2021. URL: https://youtube.com/playlist?list=PLYvLhcRhd8-ExjMaK-cyKRe-WQvc2DD-b&si=JbOVwp-5ytKEA7k1 (visitado 27-10-2023).

[3] Inocencio Ortiz. «Álgebra moderna. Material de teoría». 2023.

[4] Norman B. Haaser, Joseph P. La Salle y Joseph A. Sullivan. «Análisis matemático. Curso de introducción.» 2da. Vol. 1. Trillas, 1995, págs. 1-808.

[5] James R. Munkres. «Topología». 2da. Pearson. Prentice Hall, 2002, págs. 3-84.

[6] Seymour Lipschutz. «Álgebra lineal». 2da. McGraw-Hill, 1992, págs. 1-563.

[7] Socratica. «Abstract Algebra». 2020. URL: https://youtube.com/playlist?list=PLi01XoE8jYoi3SgnnGorR_XOW3IcK-TP6&si=l3VRicXPvb3y1GqQ (visitado 27-10-2023).

[8] Benedict Gross. «Abstract Algebra». 2020. URL: https://youtube.com/playlist?list=PLelIK3uylPMGzHBuR3hLMHrYfMqWWsmx5&si=NLvwmllir_OEQm6v (visitado 27-10-2023).

[9] Joseph A. Gallian. «Contemporary abstract algebra». 9th. Cengage Learning, 2017.

[10] Tarski Alfred. «Introducción a la lógica ya la metodología de las ciencias deductivas, Ed». Espasa-Calpé, SA, Madrid, 1977.

[11] Google AI. «Google Gemini». https://ai.google/discover/gemini/. 2023.

[12] Serge Lang. «Undergraduate algebra». Springer Science & Business Media, 2005.

[13] Serge Lang. «Algebra». Vol. 211. Springer Science & Business Media, 2012.