Capítulo 1

Fundamentos y principio de inducción

La *Teoría de Conjuntos* es el fundamento de las matemáticas y de diversas áreas de las Ciencias de la Computación. En este tema introducimos los conceptos y operadores básicos para trabajar con conjuntos.

1.1. Teoría de Conjuntos

1.1.1. Preliminares y definiciones básicas

De forma intuitiva, un *conjunto* es una colección de objetos, cuyos objetos pueden ser cualquier cosa, como números, letras, coches, animales, personas, etc.

Ejemplo 1.1.1. Algunos ejemplos de conjuntos serían los siguientes:

- El conjunto de los números naturales, $\mathbb{N} = \{1, 2, 3, ...\}$.
- El conjunto de los números enteros, $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$.
- El conjunto de los números racionales $\mathbb{Q} = \left\{\pm\frac{p}{q}, p, q \in \mathbb{N} \,:\, \text{mcd}(p, q) = 1\right\}$.
- El conjunto $A = \{a, b, c, d\}$.
- El conjunto $B = \{1, 2, 3, a, b\}$.
- El conjunto $I = \{2k + 1, k \in \mathbb{Z}\}$.

Los conjuntos se denotan habitualmente por letras mayúsculas. Los objetos que componen el conjunto se llaman *elementos*, y se suelen denotar por letras minúsculas (si se trataran de letras).

Para indicar que un elemento *a pertenece* a un conjunto A, se utiliza la notación $a \in A$ (leído a pertenece a A). Por el contrario, para indicar que un elemento *a no pertenece* a un conjunto A, utilizaremos la notación $a \notin A$ (a no pertenece a A).

Definición 1.1.2. Sean A y B dos conjuntos. Diremos que A y B *son iguales* ($A = B$) si tienen los mismos elementos.

Es decir, un conjunto queda completamente determinado por sus elementos. Si describimos un conjunto dando la lista de sus elementos encerrada entre llaves, diremos que se define *por extension*.

Ejemplo 1.1.3. $A = \{a, b, c, d\}$, $B = \{1, 2, 3, a, b\}$ y $\mathbb{N} = \{1, 2, 3, ...\}$ son conjuntos definidos por extensión.

Sin embargo, si P es una propiedad y A es el conjunto cuyos elementos verifican dicha propiedad, diremos entonces que A está definido *por comprensión*.

Ejemplo 1.1.4.

- $A = \{x \in \mathbb{R} : x^2 - 5x + 6 = 0\}$.
- $B = \{n \in \mathbb{N} : n \text{ es primo}\}$.
- $\mathbb{Q} = \left\{\pm\frac{p}{q}, p, q \in \mathbb{N} : \text{mcd}(p, q) = 1\right\}$.

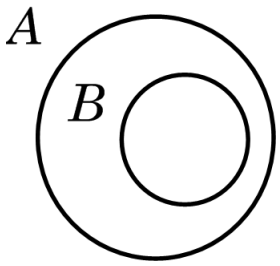
Observación 1.1.5. Debemos tener en cuenta que, atendiendo a la definición de igualdad, en las representaciones por extensión no importa el orden en que se escriban los elementos ni las posibles repeticiones.

Ejemplo 1.1.6. Los siguientes conjuntos son iguales:

- $\{a, b, c\} = \{b, a, c\}$.
- $\{a, b, a\} = \{a, b, b\} = \{a, b\}$.

1.1.2. Subconjuntos

Definición 1.1.7. Sean A y B dos conjuntos. Diremos que B *es un subconjunto de* A, y lo denotaremos por $B \subseteq A$ (o bien, $B \subset A$, también leído B contenido en A), si todo elemento de B es también elemento de A. Si $B \subseteq A$ y $B \neq A$ diremos que B es un *subconjunto propio de* A.



Ejemplo 1.1.8.

- Sean $A = \{1, 2, 3, a, b\}$ y $B = \{2, b, 1\}$. Claramente $B \subseteq A$, ya que todo elemento de B es también elemento de A.
- Consideremos ahora los conjuntos $A = \{1, a, b, c\}$ y $B = \{a, b, c, d\}$. En este caso, B no es subconjunto de A ($B \subsetneq A$ o $B \nsubseteq A$), ya que $d \notin A$.

De la definición de subconjunto se concluye inmediatamente que $A \subseteq A$, para cualquier conjunto A.

Observación 1.1.9. Debemos tener mucho cuidado y no confundir la relación de pertenencia $\in$, y la relacion de inclusion $\subseteq$. La relación de pertenencia nos decía si un elemento está o no en un conjunto, y la relación de inclusión nos dice si un conjunto está contenido (o no) dentro de otro conjunto.

Teorema 1.1.10. *Sean A y B dos conjuntos. Entonces $A = B$ si, y solo si, $A \subseteq B$ y $B \subseteq A$.*

Definición 1.1.11. Existe un conjunto que no tiene elementos. Este conjunto se denomina *conjunto vacío,* y se denota por $\emptyset$.

Observación 1.1.12. Una de las definiciones por compresión del conjunto vacío es $\emptyset = \{x \in A : x \notin A\}$, donde A es cualquier conjunto no vacío. Con esta definición, se puede ver que $\emptyset$ es un subconjunto de A. La más usual es simplemente escribir $\emptyset = \{\}$ (definición por extensión).

Definición 1.1.13. Sea A un conjunto. Definimos el conjunto *partes de* A, y lo denotamos por $\mathcal{P}(A)$ (a veces se le denota por 2^A), como el conjunto de todos los subconjuntos de A.

Ejemplo 1.1.14.

- Si $A = \{a, b\}$, entonces $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.
- Sea $A = \{1, 2, 3\}$, entonces $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

Observación 1.1.15. Nótese que, en el primero de los ejemplos anteriores, A tiene dos elementos y $\mathcal{P}(A)$ tiene $4 = 2^2$ elementos. Lo mismo ocurre con el segundo ejemplo, en el que A tiene 3 elementos y $\mathcal{P}(A)$ tiene $8 = 2^3$ elementos. Este hecho no es casualidad y se detallará más adelante.

1.1.3. Operaciones con conjuntos

Definición 1.1.16. Sean A y B dos conjuntos. Se define el conjunto A *unión* B, y lo denotaremos por $A \cup B$, como $A \cup B = \{x : x \in A \text{ o bien } x \in B\}$.

Observación 1.1.17. De forma intuitiva, la unión de dos conjuntos es el conjunto formado por los dos conjuntos.

Ejemplo 1.1.18.

- $\left.\begin{array}{c} A = \{1, 2, 3\} \\ B = \{a, b\} \end{array}\right\} \Longrightarrow A \cup B = \{1, 2, 3, a, b\}.$
- $\left.\begin{array}{c} A = \{1, 2, a, b\} \\ B = \{1, a, b, c\} \end{array}\right\} \Longrightarrow A \cup B = \{1, 2, a, b, c\}.$

Observación 1.1.19. Aunque en la definición aparezca solamente dos conjuntos, tiene sentido plantearse la unión de más de dos conjuntos. Por ejemplo:

$$\left.\begin{array}{c} A = \{1, 2, a\} \\ B = \{rojo\} \\ C = \{3, a, b\} \end{array}\right\} \Longrightarrow A \cup B \cup C = \{1, 2, 3, a, b, rojo\}.$$

Proposición 1.1.20. *Sean A y B dos conjuntos y consideremos $A \cup B$. Entonces $A \subseteq A \cup B$ y también $B \subseteq A \cup B$. De hecho, $A \cup B$ es el conjunto más pequeño que contiene a A y a B.*

Definición 1.1.21. Sean A y B dos conjuntos. Se define el conjunto A *intersección* B, y lo denotaremos por $A \cap B$, como $A \cap B = \{x : x \in A \text{ y } x \in B\}$ o, equivalentemente, $A \cap B = \{x \in A : x \in B\} = \{x \in B : x \in A\}$.

Observación 1.1.22. De forma intuitiva, la intersección de dos conjuntos es el conjunto formado por los elementos comunes de ambos conjuntos.

Ejemplo 1.1.23.

- $\left.\begin{array}{l} A = \{1, 2, a, b\} \\ B = \{1, 2, 3, a\} \end{array}\right\} \Longrightarrow A \cap B = \{1, 2, a\}.$
- $\left.\begin{array}{l} A = \{1, 2, a, b\} \\ B = \{1, a, b, c\} \end{array}\right\} \Longrightarrow A \cap B = \{1, a, b\}.$

Observación 1.1.24. Como antes, aunque en la definición aparezca solamente dos conjuntos, tiene sentido plantearse la intersección de más de dos conjuntos. Por ejemplo:

$$\left.\begin{array}{l} A = \{1, 2, 3, a\} \\ B = \{1, 2, 3, b\} \\ C = \{1, 3, a, b\} \end{array}\right\} \Longrightarrow A \cap B \cap C = \{1, 3\}.$$

Definición 1.1.25. Sean A y B dos conjuntos. Se dice que A y B son *disjuntos* si $A \cap B = \emptyset$.

Ejemplo 1.1.26.

- El conjunto de los números irracionales y el de los números racionales son disjuntos.
- Los conjuntos $A = \{1, 3, 5, 7\}$ y $B = \{0, 2, 4, 6\}$ son disjuntos.

Proposición 1.1.27. *Sean A y B dos conjuntos y consideremos $A \cap B$. Entonces $A \cap B \subseteq A$ y también $A \cap B \subseteq B$. De hecho, $A \cap B$ es el conjunto más grande contenido en A y en B.*

En muchas ocasiones se suele trabajar dentro de un *Universo*, es decir, un conjunto que contiene a todos los conjuntos con los que trabajamos en dicha aplicación (un contexto). En estos casos, aparece una operación de conjuntos que llamamos conjunto contrario.

Definición 1.1.28. Sea A un conjunto dentro de un conjunto $\mathcal{U}$ ($A \subseteq \mathcal{U}$). Se define el conjunto *contrario* (o *complementario*) de A, y lo denotamos por $\overline{A}$ o A^c, como el conjunto $A^c = \{x : x \notin A\}$, es decir, $A^c = \{x \in \mathcal{U} : x \notin A\}$.

Ejemplo 1.1.29. Consideremos el conjunto $A = \{1, 2, 3, 4, a, b, c, d\}$ y sea $B = \{1, a, b, d\}$. Claramente $B \subseteq A$, con lo que tiene sentido hablar de B^c. De hecho, $B^c = \{2, 3, 4, c\}$.

Proposición 1.1.30. *Sea A un conjunto tal que tiene sentido hablar de A^c. Entonces A y A^c son conjuntos disjuntos, es decir, $A \cap A^c = \emptyset$.*

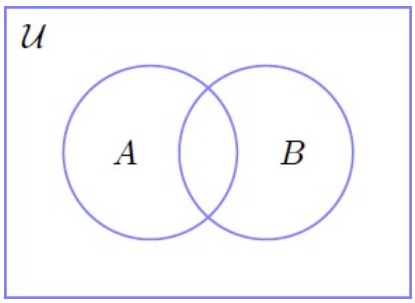
Definición 1.1.31. Sean A y B dos conjuntos. Se define la *diferencia de A y B*, y se denota por $A - B$ o $A \setminus B$, como el conjunto $A \setminus B = \{x \in A : x \notin B\}$.

Ejemplo 1.1.32.

- Sean $A = \{1, 2, 8, 9\}$ y $B = \{2, 6, 7\}$. Entonces $A \setminus B = \{1, 8, 9\}$ y $B \setminus A = \{6, 7\}$.
- Consideremos ahora los conjuntos $A = \{1, 2, a, b, verde\}$ y $B = \{2, b, c, rojo, verde\}$. Entonces $A \setminus B = \{1, a\}$ y $B \setminus A = \{c, rojo\}$.

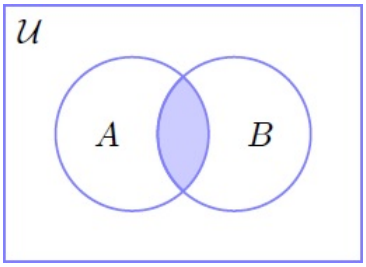
1.1.4. Diagramas de Venn

Los diagramas de Venn son una representación esquemática de conjuntos. Estos diagramas están pensados para visualizar las relaciones y operaciones entre dos o más conjuntos. Representamos con un rectángulo el universo y dentro dibujamos dos o más círculos para representar conjuntos dentro de ese universo.

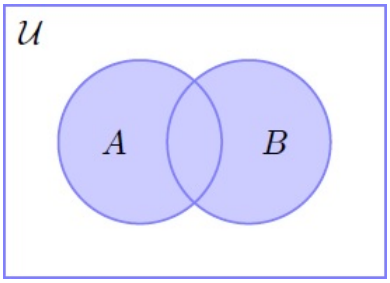


De esta forma, coloreando o sombreando regiones, podemos visualizar las operaciones que hemos definido hasta ahora.

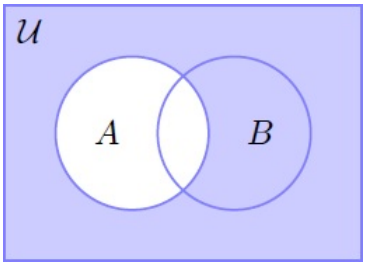
La región sombreada en la figura, corresponde a $A \cap B$



La región sombreada en la figura, corresponde a $A \cup B$



La región sombreada en la figura, corresponde a A^c



1.1.5. Cardinal de un conjunto

Definición 1.1.33. Sea A un conjunto. Se define el *cardinal de* A, y se denota por $|A|$, $\#A$ o $\text{card}(A)$, como el número de elementos que contiene el conjunto A.

Ejemplo 1.1.34.

- Si $A = \{1, 2, a\}$, entonces $\#A = 3$.
- El cardinal de el conjunto de todos los números naturales, $\mathbb{N}$, es infinito.
- $\#\mathbb{R} = +\infty$.

Observación 1.1.35. $\#\mathbb{N}$ y $\#\mathbb{R}$ son distintos entre sí, aunque ambos sean infinitos. Esto se verá con detalle más adelante.

Definición 1.1.36. Sea A un conjunto. Diremos que A es un conjunto

- *finito* si $\#A = n \in \mathbb{N}$.
- *infinito numerable*, si $\#A = \#\mathbb{N}$.
- *infinito no numerable* si $\#A = \#\mathbb{R}$.

Ejemplo 1.1.37.

- $A = \{-1, 0, 1, 2\}$ es finito.
- $\mathbb{Z}$ es infinito numerable.
- $[0, 1] = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$ es infinito no numerable.

Definición 1.1.38. Sean A y B dos conjuntos. Diremos que A y B son *equipotentes* si $\#A = \#B$.

Proposición 1.1.39. *Sean A y B dos conjuntos. Entonces se verifica:*

1. $\#\mathcal{P}(A) = 2^{\#A}$.
2. *Si $A \subseteq B$, entonces $\#A \leq \#B$.*

Corolario 1.1.40. *Sean A y B dos conjuntos tales que $A \subseteq B$. Entonces se verifica:*

- *Si $\#A = +\infty$, entonces $\#B = +\infty$.*
- *Si $\#B = n \in \mathbb{N}$ (B es finito con n elementos), entonces $\#A \leq \#B$.*

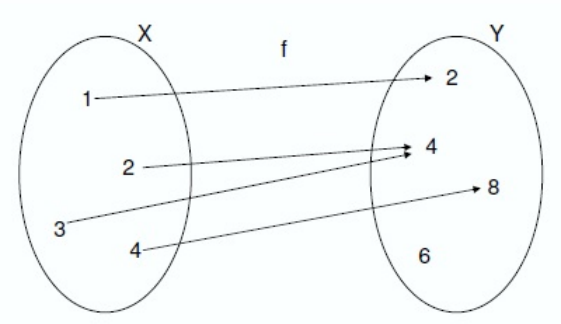
Observación 1.1.41. Nótese que, sin ningún problema, puede pasar que A sea finito y B sea infinito, por ejemplo $A = \{1, 2\}$ y $B = \mathbb{N}$. Del mismo modo, puede ocurrir que ambos sean infinitos como, por ejemplo, si tomamos $A = \mathbb{N}$ y $B = \mathbb{Z}$.

1.1.6. Funciones

Las *funciones* son, junto a los conjuntos, los elementos más básicos en los que se sustentan las matemáticas.

Definición 1.1.42. Sean A y B dos conjuntos. Definimos una *función* (o aplicación) entre A y B, y lo denotamos por $f : A \longrightarrow B$, como una asociación que a cada elemento de A le asigna un único elemento de B. En este caso, al conjunto A se le llama *dominio* y al conjunto B *codominio*.

Normalmente daremos una función dando una regla que asigna a cada elemento de A un y solo un elemento de B. Podemos representar funciones a partir de diagramas de Venn. Por ejemplo:



En este caso la función f tiene dominio $A = \{1, 2, 3, 4\}$ y codominio $B = \{2, 4, 8, 6\}$; y puede ser representada por $f : A \longrightarrow B$, con $f(x) = -8 + 16x - 7x^2 + x^3$ para todo $x \in A$.

Definición 1.1.43. Sean A y B dos conjuntos y sea $f : A \longrightarrow B$ una función. Sea A_1 un subconjunto de A y B_1 un subconjunto de B. Se define:

- La *imagen de A_1 por f*, y se denota por $f(A_1)$, como el conjunto $f(A_1) = \{f(a) : a \in A_1\}$.
- La *imagen de f*, denotada por $\mathrm{Im}(f)$, como $\mathrm{Im}(f) = f(A)$.
- La *preimagen de B_1 por f* como $f^{-1}(B_1) = \{a \in A : f(a) \in B_1\}$.

Observación 1.1.44. Nótese que $f(A_1) \subseteq B$ y $f^{-1}(B_1) \subseteq A$.

Ejemplo 1.1.45. Si el dominio de la función es infinito, la asociación del elemento de la imagen correspondiente a cada elemento del dominio se hará mediante una regla:

- $f_1 : \mathbb{R} \longrightarrow \mathbb{R}$, con $f_1(x) = x^2$ para todo $x \in \mathbb{R}$. Es fácil ver que, en este caso, $\mathrm{Im}(f_1) = [0, +\infty)$.
- $f_2 : \mathbb{N} \longrightarrow \mathbb{N}$, siendo $f(n) = 2n + 1$. En este caso, $\mathrm{Im}(f_2) = \{3, 5, 7, 9, ...\}$.

Si el dominio es un conjunto finito, también podemos utilizar una tabla para definir las funciones:

- Sea $A = \{1, 2, 3, 4, 5\}$ y $B = \{a, b, c\}$. Podemos considerar $f : A \longrightarrow B$ como la aplicación que asigna de la siguiente manera:

$$\begin{array}{rccc} f: & A & \longrightarrow & B \\ & 1 & \mapsto & c \\ & 2 & \mapsto & a \\ & 3 & \mapsto & c \\ & 4 & \mapsto & b \\ & 5 & \mapsto & a \end{array}.$$

Definición 1.1.46. Sea A un conjunto y sea B un subconjunto de A. Definimos:

- La *aplicación identidad* como $1_A : A \longrightarrow A$ dada por $1_A(x) = x$ para todo $x \in A$.
- La *aplicación inclusión* como $i : B \longrightarrow A$ dada por $i(x) = x$ para todo $x \in B$.

Definición 1.1.47. Sean A, B y C tres conjuntos y consideremos las funciones $f : A \longrightarrow B$ y $g : B \longrightarrow C$. Se define la *función composición* como $g \circ f : A \longrightarrow C$ dada por $(g \circ f)(x) = g(f(x))$ para todo $x \in A$.

Ejemplo 1.1.48. Sean $A = \{1, 2, 3, 4, 5\}$, $B = \{a, b, c\}$ y $C = \{1, 2, z\}$, y consideremos $f : A \longrightarrow B$ y $g : B \longrightarrow C$ como

$$\begin{array}{rccc} f: & A & \longrightarrow & B \\ & 1 & \mapsto & c \\ & 2 & \mapsto & a \\ & 3 & \mapsto & c \\ & 4 & \mapsto & b \\ & 5 & \mapsto & a \end{array} \qquad \begin{array}{rccc} g: & B & \longrightarrow & C \\ & a & \mapsto & 2 \\ & b & \mapsto & z \\ & c & \mapsto & 1 \end{array} .$$

En ese caso

$$\begin{array}{rccc} g \circ f: & A & \longrightarrow & C \\ & 1 & \mapsto & 1 \\ & 2 & \mapsto & 2 \\ & 3 & \mapsto & 1 \\ & 4 & \mapsto & z \\ & 5 & \mapsto & 2 \end{array} .$$

Definición 1.1.49. Sean A y B dos conjuntos y sea $f : A \longrightarrow B$ una función. Decimos que

- la función f es *inyectiva* si elementos distintos tienen imágenes distintas, es decir, si $x \neq y$, entonces $f(x) \neq f(y)$ o, equivalentemente, si $f(x) = f(y)$, entonces $x = y$.
- la función f es *sobreyectiva* si todo elemento de B es la imagen de algún elemento de A, es decir, si para todo $y \in B$ existe un $x \in A$ tal que $f(x) = y$ o, equivalentemente, si $\mathrm{Im}(f) = B$.
- la función f es *biyectiva* si es inyectiva y sobreyectiva.

Ejemplo 1.1.50.

- Si $A \subseteq B$, entonces la inclusión $i : A \longrightarrow B$ es inyectiva.
- La identidad $1_A : A \longrightarrow A$ es sobreyectiva para cualquier conjunto A no vacío.
- La función $f : \mathbb{N} \longrightarrow \mathbb{N}$, definida por $f(n) = 2n$ es inyectiva. En efecto, si $f(n) = f(m)$, entonces $2n = 2m$, con lo que $n = m$.
- La función $g : \mathbb{R} \longrightarrow [-1, 1]$, dada por $g(x) = \mathrm{sen}(x)$ para todo $x \in \mathbb{R}$, es sobreyectiva, pero no inyectiva, ya que $g(0) = 0 = g(2\pi)$, pero $0 \neq 2\pi$.
- La función $h : \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \longrightarrow [-1, 1]$, definida por $h(x) = \mathrm{sen}(x)$, es biyectiva.

Teorema 1.1.51. *Sean A y B dos conjuntos y sea $f : A \longrightarrow B$ una función. Si f es biyectiva entonces $\#A = \#B$.*

Observación 1.1.52. Recordemos ahora el ejemplo de la sección dedicada al cardinal de un conjunto, cuando veíamos que $\#\mathbb{Z} = \#\mathbb{N}$. Pues bien, basta con considerar la función $f : \mathbb{N} \longrightarrow \mathbb{Z}$,

$$f(n) = \begin{cases} \frac{n}{2}, & \text{si } n \text{ es par} \\ \frac{1-n}{2}, & \text{si } n \text{ es impar} \end{cases},$$

y aplicar el teorema anterior, ya que la función f es biyectiva.

Teorema 1.1.53. *Sean A, B y C tres conjuntos y consideremos las funciones $f : A \longrightarrow B$ y $g : B \longrightarrow C$. Entoces se verifica:*

1. *Si f y g son inyectivas, entonces $g \circ f$ es inyectiva.*
2. *Si $g \circ f$ es inyectiva, entonces f es inyectiva.*
3. *Si f y g son sobreyectivas, entonces $g \circ f$ es sobreyectiva.*
4. *Si $g \circ f$ es sobreyectiva, entonces g es sobreyectiva.*
5. *Si f y g son biyectivas, entonces $g \circ f$ es biyectiva.*
6. *Si $g \circ f$ es biyectiva, entonces f es inyectiva y g es sobreyectiva.*

Definición 1.1.54. Sean A y B dos conjuntos y sea $f : A \longrightarrow B$ una función. Se dice que f es *invertible* si existe una función $g : B \longrightarrow A$ tal que $g \circ f = 1_A$ y $f \circ g = 1_B$.

Observación 1.1.55. En este caso, si existe una función g con esas cualidades, entonces es única. A dicha función se le denomina *función inversa de f*, y se denota por f^{-1}.

Observación 1.1.56. Hemos utilizado la notación f^{-1} para dos operaciones distintas, el contexto resolverá la ambigüedad, ya que en un caso aplicamos el operador a un conjunto (preimagen) y en el otro a un elemento (función inversa). Ademas, los dos operadores están relacionados, ya que si f es invertible, entonces $\{f^{-1}(y)\} = f^{-1}(\{y\})$.

Ejemplo 1.1.57. La función $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ definida por $f(x) = x + 7$ es invertible. En efecto

$$x + 7 = y \Leftrightarrow x = y - 7,$$

con lo que podemos tomar $f^{-1} : \mathbb{Z} \longrightarrow \mathbb{Z}$ como $f^{-1}(y) = y - 7$. Haciendo unos pocos cálculos observamos que:

$$(f^{-1} \circ f)(x) = f^{-1}(x + 7) = (x + 7) - 7 = x = 1_{\mathbb{Z}}(x).$$
$$(f \circ f^{-1})(y) = f(y - 7) = (y - 7) + 7 = y = 1_{\mathbb{Z}}(y).$$

Con lo que, efectivamente, f es invertible con inversa f^{-1}.

Teorema 1.1.58. *Sean A y B dos conjuntos y sea $f : A \longrightarrow B$ una función. Entonces f es invertible si, y solo si, f es biyectiva.*

1.1.7. Relaciones

Las relaciones en matemáticas formalizan las conexiones entre elementos de dos o más conjuntos. Son importantes en matemáticas y en computación tanto por sus aplicaciones teóricas (relaciones de orden, equivalencias, etc), como por su aplicaciones más prácticas (bases de datos, redes sociales, ...). Constantemente nos encontramos y manejamos relaciones: ordenación de números, relaciones de parentesco, guías telefónicas, directorios de personas, etc.

1.1.7.1. Relaciones binarias

Definición 1.1.59. Sean A y B dos conjuntos. Se define el *producto cartesiano de* A y B como el conjunto $A \times B = \{(a, b) : a \in A, b \in B\}$.

Los elementos del producto cartesiano de dos conjuntos se denominan *pares ordenados*. En ese caso, la palabra orden se refiere a la posición que ocupan los elementos dentro de la pareja. Por ejemplo, los pares $(1, 2)$ y $(2, 1)$ son elementos de $\mathbb{N} \times \mathbb{N}$ y, aunque contienen las mismos elementos, son pares ordenados distintos, $(1, 2) \neq (2, 1)$.

Definición 1.1.60. Sea A un conjunto. Se define una *relación (binaria) en* A, y se denota por $\mathcal{R}$ o $\sim$, como cualquier subconjunto del producto cartesiano $A \times A$. Si un elemento $(a, b) \in \mathcal{R}$, diremos que a *está relacionado con* b, y lo denotaremos por $a\mathcal{R}b$ o bien $a \sim b$.

Ejemplo 1.1.61.

- En el conjunto de los números naturales definimos la relación «ser menor o igual que», es decir, diremos $n \sim m$ si y solo si $n \leq m$. Así, $3 \sim 5$ (3 y 5 si están relacionados), pero $5 \nsim 2$ (5 no es menor o igual que 2).
- Podemos considerar, en el conjunto de los seres humanos, la relación «ser hermano de».

Definición 1.1.62. Sea A un conjunto y sea $\sim$ una relación en A. Diremos que $\sim$ verifica la propiedad:

- *Reflexiva* si para todo $x \in A$ se verifica que $x \sim x$.
- *Transitiva* si $x \sim y$ e $y \sim z$, implica que $x \sim z$.
- *Simétrica* si $x \sim y$, entonces $y \sim x$.
- *Antisimétrica* $x \sim y$ e $y \sim x$, entonces $x = y$.

Ejemplo 1.1.63. Consideremos en $\mathbb{N}$ la relación $x \sim y$ si, y solo si, x divide a y.

- Claramente $\sim$ es reflexiva, ya que x divide a x para todo $x \in \mathbb{N}$.
- $\sim$ es también transitiva, ya que si x divide a y e y divide a z, entonces x divide a z.

  En efecto, si x divide a y, existe entonces $n \in \mathbb{N}$ tal que $y = nx$.

  Análogamente, si y divide a z, existe entonces $m \in \mathbb{N}$ tal que $z = my$.

  Luego
  $$z = my \overset{y=nx}{=} m(nx) = (mn)x = kx,$$
  con $k = mn \in \mathbb{N}$, es decir, existe $k \in \mathbb{N}$ tal que $z = kx$ y, por tanto, x divide a z.
- Además, $\sim$ es antisimétrica ya que, si x divide a y e y divide a x, necesariamente $x = y$, ya que estamos trabajando solamente con números naturales. Veámoslo.

  Si x divide a y, existe entonces $n \in \mathbb{N}$ tal que $y = nx$.

  Del mismo modo, si y divide a x, existe entonces $m \in \mathbb{N}$ tal que $x = my$.

  Luego
  $$x = my \overset{y=nx}{=} m(nx) = (mn)x = kx$$
  y, como $x \in \mathbb{N}$, entonces $k = 1$ (podemos "pasar" x dividiendo en $x = kx$), con lo que $x = y$.
- Sin embargo, $\sim$ no es simétrica ya que, por ejemplo, 2 divide a 4, pero 4 no divide a 2.

1.1.7.2. Relación de equivalencia

Definición 1.1.64. Sea A un conjunto y sea $\sim$ una relación en A. Diremos que $\sim$ es una *relación de equivalencia* si verifica las propiedades reflexiva, transitiva y simétrica.

Ejemplo 1.1.65. Sea $\mathbb{Z}$ el conjunto de los números enteros y sea $n \in \mathbb{Z}$, con $n > 1$. Definamos la siguiente relación en $\mathbb{Z}$: $a \sim b$ si, y solo si, $a - b = \dot{n}$ ($a - b$ es múltiplo de n). Veamos que $\sim$ es una relación de equivalencia:

- Reflexiva: Claramente $a \sim a$ para todo entero a, ya que $a - a = 0 = 0{\cdot}n$.
- Transitiva: Supongamos que $a \sim b$ y $b \sim c$, es decir, $a - b$ y $b - c$ son múltiplos de n.

  Como $a - b$ y $b - c$ son múltiplos de n, existen entonces $k, m \in \mathbb{Z}$ tales que $a - b = kn$ y $b - c = mn$.

  Por lo tanto,
  $$a - c = (a - b) + (b - c) = kn + mn = (k + m)n$$
  es también múltiplo de n, es decir, $a \sim c$.
- Simétrica: Si $a \sim b$ entonces es claro que $b \sim a$ ya que, al ser $a - b$ múltiplo de n, existe $m \in \mathbb{Z}$ tal que $a - b = m{\cdot}n$. Luego $b - a = -(a - b) = -m{\cdot}n$.

Por lo tanto, tenemos en $\mathbb{Z}$ una relación de equivalencia. Esta relación de equivalencia es llamada *relación de congruencia módulo n*. Esta relación tiene una notación especial. Si dos números enteros $a, b \in \mathbb{Z}$ están relacionados, se denotará por $a \equiv b \pmod{n}$.

Definición 1.1.66. Sea A un conjunto y sea $\sim$ una relación de equivalencia en A. Dado un elemento $a \in A$ definimos la *clase de equivalencia de a*, y la representamos por $[a]$ o $\overline{a}$, como el conjunto $[a] = \{x \in A : a \sim x\}$. Al elemento a se le denomina *representante* de su clase de quivalencia.

El conjunto de todas las clases de equivalencia de una relación $\sim$ en un conjunto A se le llamará el *conjunto cociente de A respecto de* $\sim$ y se denotara por $A/\sim$ o $A/\mathcal{R}$.

Observación 1.1.67. Nótese que, si $a, b \in A$ están relacionados, $a \sim b$, entonces $[a] = [b]$.

Ejemplo 1.1.68. Consideremos la relación $x \sim y$ si, y solo si, $x{\cdot}y > 0$ para todo $x, y \in \mathbb{Z} \setminus \{0\}$. Veamos que $\sim$ es una relación de equivalencia en $\mathbb{Z} \setminus \{0\}$ y hallemos sus clases de equivalencias.

- Reflexiva: Claramente $x \sim x$ para todo $x \in \mathbb{Z} \setminus \{0\}$, ya que $x{\cdot}x = x^2 > 0$.
- Transitiva: Sean $x, y, z \in \mathbb{Z} \setminus \{0\}$ tales que $x \sim y$ e $y \sim z$. Tenemos que ver que $x{\cdot}z > 0$. Trabajaremos por casos:
  - Si $x > 0$ entonces, por el criterio de los signos, $y > 0$, ya que $x{\cdot}y > 0$. Del mismo modo, como $y > 0$, entonces $z > 0$. Con lo que $x{\cdot}z > 0$ y, por tanto, $x \sim z$.
  - Análogamente, si $x < 0$ entonces, por el criterio de los signos, $y < 0$, ya que $x{\cdot}y > 0$. Del mismo modo, como $y < 0$, entonces $z < 0$. Con lo que $x{\cdot}z > 0$ y, por tanto, $x \sim z$.

  Luego $x \sim z$

- Simétrica: Sean $x, y \in \mathbb{Z} \setminus \{0\}$ tales que $x \sim y$, es decir, $x \cdot y > 0$. Entonces es obvio que $y \cdot x > 0$, ya que $y \cdot x = x \cdot y > 0$. Luego $y \sim x$.

  Veamos ahora cuántas clases de equivalencia distintas tenemos en $(\mathbb{Z} \setminus \{0\})/\sim$.

  Por el criterio de los signos, si $x \in \mathbb{Z} \setminus \{0\}$ es positivo, entonces $x \cdot y > 0$ para todo $y \in \mathbb{Z} \setminus \{0\}$ con $y > 0$, es decir, x estará relacionado con todos los elementos positivos de $\mathbb{Z} \setminus \{0\}$.

  De forma análoga, si $x \in \mathbb{Z} \setminus \{0\}$ es negativo, entonces $x \cdot y > 0$ para todo $y \in \mathbb{Z} \setminus \{0\}$ con $y < 0$, es decir, x estará relacionado con todos los elementos negativos de $\mathbb{Z} \setminus \{0\}$.

  Por lo tanto, obtenemos que en $(\mathbb{Z} \setminus \{0\})/\sim$ solo existen dos clases de equivalencia, la de los elementos de $\mathbb{Z} \setminus \{0\}$ positivos, y la de los elementos negativos.

  Un representante de la clase de los elementos positivos de $\mathbb{Z} \setminus \{0\}$ podría ser, por ejemplo, el 1. Y un representante de los elementos negativos, el -1. Así,

$$(\mathbb{Z} \setminus \{0\})/\sim = \{[-1], [1]\}.$$

1.2. El principio de inducción matemática

En esta sección revisamos una de las técnicas más potentes que se emplean con frecuencia para demostrar propiedades de objetos discretos (complejidad de algoritmos, teoremas sobre grafos, etc.)

Teorema 1.2.1. (Principio de Inducción Matemática). *Sea A un subconjunto de los números naturales $\mathbb{N}$ tal que:*

1. *Caso base:* $1 \in A$.
2. *Paso inductivo: Si $n \in A$, entonces $n + 1 \in A$.*

Entonces $A = \mathbb{N}$.

Esta propiedad es la base de lo que se conoce como razonamiento por inducción.

Veamos otra forma de enunciar el Principio de Inducción Matemática.

Teorema 1.2.2. (Principio de Inducción Matemática). *Sea P una propiedad relativa a los números naturales tal que:*

1. *Caso base: 1 verifica la propiedad P.*
2. *Paso inductivo: Si $n \in \mathbb{N}$ verifica la propiedad P, entonces $n + 1$ verifica la propiedad P.*

Entonces, todos los números naturales verifican la propiedad P.

Observación 1.2.3. De forma más general, el caso base puede ser cualquier otro natural n_0 e incluso, a veces, el 0, y la conclusión será que todos los naturales mayores que n_0 tienen la propiedad P.

Veamos algunos ejemplos prácticos del principio de inducción.

Ejemplo 1.2.4. Vamos a probar la siguiente igualdad para todo $n \geq 1$,

$$1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}.$$

- **Caso base.** Para $n = 1$ se verifica la igualdad: $1 = \frac{1(1+1)}{2}$.
- **Paso inductivo.** Supongamos que la igualdad se verifica para n, es decir,

$$1 + 2 + 3 + ... + n = \frac{n(n+1)}{2},$$

y probemos que es cierto para $n + 1$.

$$1 + 2 + 3 + ... + n + (n+1) = (1 + 2 + 3 + ... + n) + (n+1) \overset{H.I.}{=} \frac{n(n+1)}{2} + (n+1) =$$

$$\frac{n(n+1)}{2} + \frac{2(n+1)}{2} = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

Luego $1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$ para todo $n \in \mathbb{N}$.

Ejemplo 1.2.5. Vamos a probar que, para todo $n \geq 1$, $n^5 - n$ es multiplo de 5.

- **Caso base.** Para $n = 1$, se verifica la propiedad: $1^5 - 1 = 0 = 0 \cdot 5$.
- **Paso inductivo.** Supongamos que $n^5 - n$ es multiplo de 5, es decir, $n^5 - n = 5m$ para algún $m \in \mathbb{N}$. Veamos entonces que $(n+1)^5 - (n+1)$ es también múltiplo de 5. Utilizando el binomio de Newton[1] para expandir la potencia $(n+1)^5$ tenemos que

$$(n+1)^5 = n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1.$$

Con lo que

$$(n+1)^5 - (n+1) = n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1 - n - 1 =$$

$$(n^5 - n) + 5n^4 + 10n^3 + 10n^2 + 5n \overset{H.I.}{=} 5m + 5n^4 + 10n^3 + 10n^2 + 5n =$$

$$5(m + n^4 + 2n^3 + 2n^2 + n) = 5k,$$

donde $k = m + n^4 + 2n^3 + 2n^2 + n \in \mathbb{N}$.

Luego $n^5 - n$ es múltiplo de 5 para todo $n \in \mathbb{N}$.

Ejemplo 1.2.6. Un error bastante frecuente es pensar que el caso base es innecesario. Por ejemplo, la propiedad $n = n+8$ es falsa para todo $n \in \mathbb{N}$. Sin embargo, sí verica el paso inductivo: si $n = n+8$, entonces

$$n + 1 = (n + 8) + 1 = (n + 1) + 8.$$

[1] $(a \pm b)^N = \sum_{k=1}^{N} \binom{N}{k} a^N (\pm b)^k = \binom{N}{0} a \pm \binom{N}{1} a^{N-1} b + \binom{N}{2} a^{N-2} b^2 \pm ... \pm \binom{N}{N} b$, donde $\binom{N}{k} = \frac{N!}{k!(N-k)!}$.

Ejemplo 1.2.7. Vamos a demostrar que, para todo $n \geq 5$, se tiene que $2^n > n^2 + n$.

- **Caso base.** Para $n = 5$, se verifica la propiedad: $32 = 2^5 > 5^2 + 5 = 30$.
- **Paso inductivo.** Supongamos que $2^n > n^2 + n$. Veamos entonces que $2^{(n+1)} > (n+1)^2 + (n+1)$.

$$2^{(n+1)} = 2^n \cdot 2$$

$$\overset{H.I.}{>} (n^2 + n)\cdot 2 = 2n^2 + 2n = n^2 + n^2 + 2n \overset{(*)}{\geq}$$

$$n^2 + (n+2) + 2n = (n^2 + 2n + 1) + (n+1) = (n+1)^2 + (n+1).$$

En $(*)$ hemos utilizado que $n^2 \geq n + 2$, lo cual es cierto para todo $n \geq 2$ (se puede probar por inducción) y, en particular, es cierto para $n \geq 5$.

Luego $2^n > n^2 + n$ para todo $n \geq 5$.

Teorema 1.2.8. (inducción completa). *Sea P una propiedad relativa a los numeros naturales tal que:*

1. *Caso base: El numero 0 tiene la propiedad P.*
2. *Paso inductivo: Si cada $m \in \mathbb{N}$, tal que $m \leq n$ tiene la propiedad P, entonces $n+1$ tiene la propiedad P.*

En este caso, todos los numeros naturales tienen la propiedad P.

Este principio también se conoce como inducción fuerte. Muchos ejemplos se estudian más facilmente usando la formulación fuerte.

Ejemplo 1.2.9. Cosideremos la sucesión

$$a_0 = 1,\ a_1 = 2,$$

$$a_{n+1} + a_n - 6a_{n-1} = 0,\ n \geq 2.$$

Veamos que, para todo $n \in \mathbb{N}$, se tiene que $a_n = 2^n$.

- **Caso base.** Para $n = 0$ y $n = 1$ se verifica la igualdad, ya que $a_0 = 1 = 2^0$ y $a_1 = 2 = 2^1$.
- **Paso inductivo.** Supongamos que $a_m = 2^m$ para todo $m \leq n$, y veamos que se verifica para a_{n+1}. Por una parte, como $a_{n+1} + a_n - 6a_{n-1} = 0$, entonces

$$a_{n+1} = 6a_{n-1} - a_n \overset{H.I.}{=} 6\cdot 2^{n-1} - 2^n = 2^{n-1}(6-2) = 2^{n-1}\cdot 4 = 2^{n-1}\cdot 2^2 = 2^{n+1}.$$

Luego $a_n = 2^n$ para todo $n \in \mathbb{N}$.

Ejercicios

1. Establece si son verdaderas o falsas las siguientes afirmaciones:

$$\begin{array}{lll} \text{I) } a \in \{a\} & \text{II) } \{a\} \in \{a\} & \text{III) } \{a,b\} \in \{a,\{a,b\}\} \\ \text{IV) } a \subseteq \{a\} & \text{V) } \{a\} \subseteq \{a\} & \text{VI) } \{a,b\} \subseteq \{a,\{a,b\}\} \end{array}$$

2. En el conjunto $\mathbb{N}$ de los números naturales se consideran los siguientes subconjuntos:

   P: conjunto de todos los números naturales primos D: conjunto de múltiplos de dos, T: conjunto de múltiplos de tres, I: conjunto de números impares y S: conjunto de múltiplos de seis. Determina:

$$P \cap I, \qquad P \cap D, \qquad D \cap T, \qquad D \cap S, \qquad I \cap S,$$

$$P^c, \qquad I^c, \qquad D^c, \qquad P \cup I, \qquad P \setminus I, \qquad \overline{D \cap I}.$$

3. Sean A, B y C subconjuntos de un universo $\mathcal{U}$.

   a) Demuestra, ayudándote de un diagrama de Venn, que son ciertas las siguientes igualdades:

$$A \setminus B = A \cap B^c, \qquad (A \cup B)^c = A^c \cap B^c, \qquad (A \cap B)^c = A^c \cup B^c,$$

$$A \setminus (B \cap C) = (A - B) \cup (A - C), \qquad A \cap (B - C) = (A \cap B) - (A \cap C).$$

   b) Da un contraejemplo que demuestre que las siguientes igualdades no son válidas:

$$A - (B - C) = (A - B) - C, \qquad (A - B) \cup B = A.$$

4. Utilizando solo las definiciones, demuestra que para cualquier par de conjuntos A y B, los siguientes enunciados son equivalentes:

$$\text{I) } A \subseteq B, \qquad \text{II) } A \cap B = A, \qquad \text{III) } A \cup B = B \ .$$

5. Sea el conjunto $\mathbb{Z}$ de los números enteros y las funciones

$$f : \underset{(a,b)}{\mathbb{Z} \times \mathbb{Z}} \longrightarrow \underset{a-b}{\mathbb{Z}} \qquad \text{y} \qquad g : \underset{a}{\mathbb{Z}} \longrightarrow \underset{(a,-a)}{\mathbb{Z} \times \mathbb{Z}}.$$

   a) Determina $g \circ f$ y $f \circ g$.

   b) Estudia las propiedades de f, g, $g \circ f$ y $f \circ g$.

6. Sea $a \in \mathbb{R}$ y sea $B \subseteq \mathbb{R}$ un subconjunto infinito numerable de $\mathbb{R}$. Demostrar que el conjunto $A = \{a + b : b \in B\}$ es un conjunto infinito numerable.

7. En el conjunto $A = \{2, 3, 4, 5, 6\}$ se considera la relación $\mathcal{R}$ definida por $x\mathcal{R}y$ si, y solo si, x divide a y.

   a) Halla los pares que pertenecen a $\mathcal{R}$.

   b) Estudia si es una relación de equivalencia.

8. En el conjunto $A = \{1, 2, 3, 4\}$ se establece una relación binaria

$$\mathcal{R} = \{(1,1), (2,2), (2,3), (2,4), (3,2), (3,3), (3,4), (4,2), (4,3), (4,4)\}.$$

Justifica que $\mathcal{R}$ es una relación de equivalencia y halla el conjunto cociente.

9. En $\mathbb{Z}$, definimos la siguiente relación binaria: $x \sim y$ si, y solo si, $2x + 4y$ es multiplo de 6.

   a) Estudia las propiedades de la relación $\sim$.

   b) ¿Es una relación de equivalencia? En tal caso, determina sus clases de equivalencia.

10. Se considera la relación binaria en $\mathbb{Z}$ definida por $a\mathcal{R}b$ si, y solo si, $a \leq b + 1$.

    a) Estudia las propiedades de la relación $\mathcal{R}$. ¿Es una relación de equivalencia?

    b) Determina cada uno de los siguientes subconjuntos:

$$\{x \in \mathbb{Z} : (x, 1) \in \mathcal{R}\}, \qquad \{x \in \mathbb{Z} : (4, x) \in \mathcal{R}\}.$$

11. En el conjunto $\mathbb{Z}$ de los números enteros se define la relación $a\mathcal{R}b$ si, y solo si, $a^2 - b^2 = a - b$. Estudia si es una relación de equivalencia y, en caso afirmativo, determina las clases de equivalencia.

12. Demuestra por inducción que $n^3 + (n+1)^3 + (n+2)^3$ es múltiplo de 9 para todo $n \geq 0$.

13. Demuestra por inducción que $n^2 + 3n$ es divisible entre 2 para todo $n > 1$.

14. Demuestra por inducción que para todo entero $n \geq 1$ se verifica:

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}.$$

15. Demuestra por inducción que para todo entero $n \geq 1$ se verifica:

$$\sum_{i=1}^{n} 2^{i-1} = 2^n - 1.$$

16. Demuestra por inducción que para todo entero $n \geq 1$ se verifica:

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}.$$

17. Demuestra por inducción que $2^n > n^2 + n$ para todo $n > 4$.

18. Para cada $n \in \mathbb{N}$, sea $P(n)$ la propiedad «$n^2 + n + 11$ es primo». Comprueba que $P(1)$, $P(2)$, ..., $P(9)$ son todos verdaderos. Estudia si $P(n)$ es verdadero para todo $n \in \mathbb{N}$.

19. Para cada $n \in \mathbb{N}$, sea $P(n)$ la propiedad «$3n + 2$ es multiplo de 3». Comprueba que la implicación $P(k) \Rightarrow P(k+1)$ es verdadera para cada $k \in \mathbb{N}$ y estudia si $P(n)$ es verdadero para todo $n \in \mathbb{N}$.

20. Demuestra por inducción que para todo entero $n \geq 1$ se verica:

    a) $7^n - 2^n$ es múltiplo de 5.

    b) $2^{2n} - 1$ es múltiplo de 3.