

Preliminares

Modelos de Computación

Elaboración: Prof. Gabriel Navarro Garulo

1. Conjuntos

Vamos a considerar un *conjunto* X como una colección de *elementos*. Los elementos de un conjunto son distintos dos a dos, esto es, cualesquiera dos elementos de un conjunto o son el mismo elemento o son elementos distintos, y no hay ningún orden o relación entre ellos. Por ejemplo, observar que $\{1, 2, a, a\}$ no es un conjunto ya que en él aparecen dos elementos repetidos, esto es, un mismo elemento aparece dos veces. Los conjuntos pueden ser definidos de dos formas distintas:

(a) por *extensión*, esto es, haciendo una lista de todos sus elementos

$$A = \{1, 2, 3, a, b, c, \alpha\},$$

(b) o por *comprensión*, esto es, mediante una propiedad que caracteriza a sus elementos

$$P = \{x \text{ tal que } x \text{ es un número natural par}\}.$$

Si un elemento x pertenece a un conjunto X , escribimos $x \in X$, y si no pertenece, escribimos $x \notin X$. En los ejemplos anteriores tenemos que $1 \in A$ y $1 \notin P$.

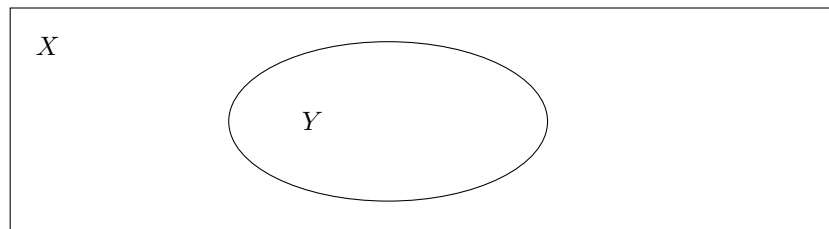
Dado un conjunto X , un *subconjunto* de X es un conjunto Y verificando que para cada elemento $y \in Y$ se tiene que $y \in X$. Escribimos entonces $Y \subseteq X$. Dos subconjuntos X_1 y X_2 de un conjunto X son *iguales* si $X_1 \subseteq X_2$ y $X_2 \subseteq X_1$, y escribimos $X_1 = X_2$. Si dos subconjuntos X_1 y X_2 de un conjunto X no son iguales, entonces decimos que son *distintos*, y escribimos $X_1 \neq X_2$. Si X_1 es un subconjunto de X y $X_1 \neq X$, podemos escribir $X_1 \subset X$ ó $X_1 \subsetneq X$.

Ejemplo 1. 1. Cada conjunto es un subconjunto de sí mismo. Esto es, para cada conjunto X se tiene $X \subseteq X$; llamamos a X el subconjunto impropio de X . Al resto de los subconjuntos de X los llamamos subconjuntos propios de X .

2. El conjunto $B = \{1, 2\}$ es un subconjunto de $A = \{1, 2, a, b, c, \alpha\}$, esto es, $B \subset A$. En cambio el conjunto $C = \{1, 2, 3\}$ no es un subconjunto de A , esto es, $C \not\subseteq A$.

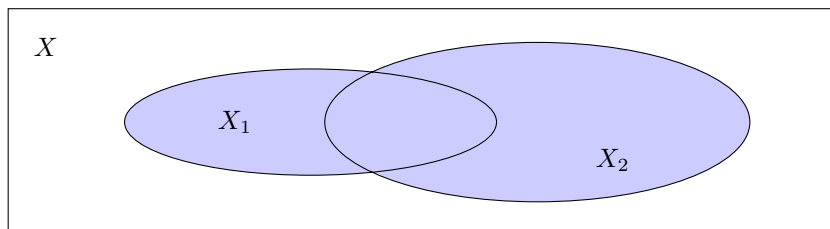
3. El conjunto $B_0 = \{2, 1\}$ es igual al conjunto B , esto es, $\{1, 2\} = \{2, 1\}$.

Si Y es un subconjunto de un conjunto X , a veces se representan según el *diagrama de Venn*, esto es, el conjunto X se representa por el interior del cuadrado y el conjunto Y por el interior de la línea curva.



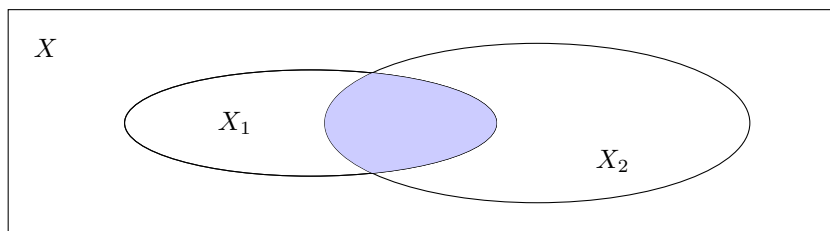
Operaciones con subconjuntos. Si X_1 y X_2 son dos subconjuntos de un conjunto X , podemos definir su *unión* como el subconjunto de X definido por:

$$X_1 \cup X_2 = \{x \in X \text{ tal que } x \in X_1 \text{ ó } x \in X_2\},$$



y su *intersección* como el subconjunto de X definido por:

$$X_1 \cap X_2 = \{x \in X \text{ tal que } x \in X_1 \text{ y } x \in X_2\}.$$



Ejemplo 2. 1. Sea $D = \{1, a\}$. Como $B = \{1, 2\}$ y D son subconjuntos del conjunto $A = \{1, 2, a, b, c, \alpha\}$, entonces podemos calcular su unión y su intersección. Concretamente,

$$B \cup D = \{1, 2, a\} \text{ y } B \cap D = \{1\}.$$

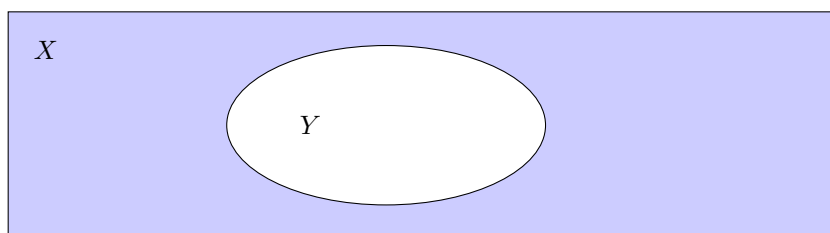
2. También B y B_0 son subconjuntos del conjunto A ; en este caso tenemos que

$$B \cup B_0 = B = B_0 \text{ y } B \cap B_0 = B = B_0.$$

Existe un conjunto especial que está definido por la propiedad de no tener ningún elemento. Este conjunto se llama *conjunto vacío* y se representa por el símbolo \emptyset . Cada conjunto X tiene un único subconjunto que no tiene ningún elemento, si representamos por \emptyset también a este subconjunto, entonces \emptyset es un subconjunto de X . El subconjunto \emptyset se llama *subconjunto trivial* de X . Si la intersección de dos subconjuntos X_1 y X_2 de un conjunto X es igual a \emptyset , decimos que son *subconjuntos disjuntos*.

Sea Y un subconjunto de un conjunto X , llamamos *subconjunto complemento* de Y en X al subconjunto de X definido por

$$\overline{Y} = X \setminus Y = \{x \in X \text{ tal que } x \notin Y\}.$$



Ejemplo 3. El complemento de $B = \{1, 2\}$ en $A = \{1, 2, a, b, c, \alpha\}$ es $\overline{B} = A \setminus B = \{a, b, c, \alpha\}$.

Observar que para cada subconjunto Y de un conjunto X , los subconjuntos Y y \overline{Y} son siempre disjuntos, esto es, $Y \cap \overline{Y} = \emptyset$.

Ejercicio 4. Sea X un conjunto e Y un subconjunto de X . Probar que $\overline{\overline{Y}} = Y$.

Solución. Tenemos que probar que $\overline{\overline{Y}} \subseteq Y$ y que $Y \subseteq \overline{\overline{Y}}$. Para esto último, tomemos un elemento $y \in Y$, entonces $y \in X$ y además $y \notin \overline{Y}$, luego $y \in \overline{\overline{Y}}$. Recíprocamente, si $y \in \overline{\overline{Y}}$, entonces por definición, $y \in X$ y además $y \notin \overline{Y}$, luego $y \in Y$.

Dado un conjunto X existe un conjunto cuyos elementos son todos los subconjuntos de X . Este conjunto lo llamamos *conjunto de las partes* ó *conjunto potencia* de X y lo representamos por $\mathcal{P}(X)$ (también se suele notar por 2^X).

Ejemplo 5. 1. El conjunto de las partes del conjunto $A = \{1, 2, a, b, c\}$ es

$$\begin{aligned} \mathcal{P}(A) = \{ & \emptyset, \{1\}, \{2\}, \{a\}, \{b\}, \{c\}, \{1, 2\}, \{1, a\}, \{1, b\}, \\ & \{1, c\}, \{2, a\}, \{2, b\}, \{2, c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{1, 2, a\}, \{1, 2, b\}, \\ & \{1, 2, c\}, \{1, a, b\}, \{1, a, c\}, \{1, b, c\}, \{2, a, b\}, \{2, a, c\}, \{2, b, c\}, \{a, b, c\}, \\ & \{1, 2, a, b\}, \{1, 2, a, c\}, \{1, 2, b, c\}, \{1, a, b, c\}, \{2, a, b, c\}, \{1, 2, a, b, c\} \}. \end{aligned}$$

2. El conjunto de las partes del conjunto $D = \{u, v, w\}$ es $\mathcal{P}(D) = \{\emptyset, u, v, w, u, v, u, w, v, w, v, w, u, v, w\}$.

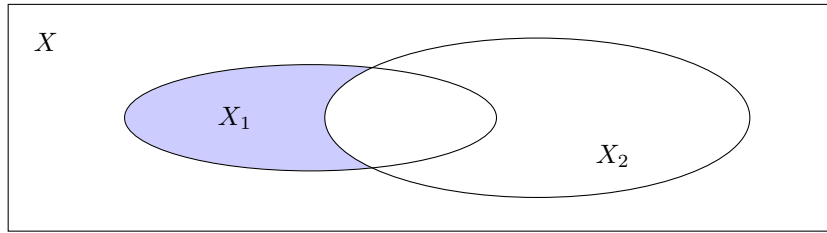
3. El conjunto de las partes del conjunto \emptyset es $\mathcal{P}(\emptyset) = \{\emptyset\}$. Observar que $\mathcal{P}(\emptyset)$ es un conjunto con un elemento (entonces no es el conjunto vacío).

4. El conjunto de las partes del conjunto $\{\emptyset\}$ es $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.

Ejercicio 6. ¿Es cierto que $\mathcal{P}(X \cup Y) = \mathcal{P}(X) \cup \mathcal{P}(Y)$? ¿Y que $\mathcal{P}(X \cap Y) = \mathcal{P}(X) \cap \mathcal{P}(Y)$?

Dados dos subconjuntos X_1 y X_2 de un conjunto X llamamos *diferencia* de X_1 y X_2 al subconjunto $X_1 \setminus X_2$ definido por

$$X_1 \setminus X_2 = X_1 \cap \overline{X_2} = \{x \in X_1 \text{ tal que } x \notin X_2\}.$$



También se suele notar por $X_1 - X_2$. Observar que en general se tiene $X_1 \setminus X_2 \neq X_2 \setminus X_1$.

Dados dos subconjuntos X_1 y X_2 de un conjunto X llamamos *producto cartesiano* de X_1 y X_2 al conjunto

$$X_1 \times X_2 = \{(a, b) \text{ tales que } a \in X_1 \text{ y } b \in X_2\}$$

Por ejemplo, si $X_1 = \{1, 2, 3\}$ y $X_2 = \{a, b\}$ entonces $X_1 \times X_2 = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$.

Proposición 7. Dados los conjuntos A , B y C , se tiene lo siguiente:

1. $\emptyset \cap A = \emptyset$
2. $\emptyset \cup A = A$
3. Si $A \subseteq B$, entonces $A \cup B = B$
4. Si $A \subseteq B$, entonces $A \cap B = A$
5. $A \cup A = A \cap A = A$
6. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ y $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
7. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ y $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
8. $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$ y $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$ (leyes de Morgan)

2. Aplicaciones

Sean X e Y dos conjuntos, una *aplicación* de X a Y es una regla que permite asignar a cada elemento del conjunto X un único elemento del conjunto Y . Si f es una aplicación de X en Y , vamos a representar f por $f : X \rightarrow Y$, ó bien, $X \xrightarrow{f} Y$.

Si $x \in X$ y $f : X \rightarrow Y$ es una aplicación, llamamos $f(x)$ al único elemento de Y que asigna f a x , y lo llamamos *imagen* de x por f . El conjunto $\Im(f) = \{f(x) \in Y \text{ tal que } x \in X\}$ se llama la *imagen* de la aplicación f , y es un subconjunto de Y . En general, si X_1 es un subconjunto de X , llamamos *imagen de X_1 por f* al subconjunto $f(X_1)$ de Y definido como $f(X_1) = \{f(x) \in Y \text{ tal que } x \in X_1\}$.

Si Y_1 es un subconjunto de Y , llamamos *imagen inversa de Y_1 por f* al subconjunto $f^{-1}(Y_1)$ de X definido como $f^{-1}(Y_1) = \{x \in X \text{ tal que } f(x) \in Y_1\}$.

Ejemplo 8. Sean $A = \{1, 2, a, b, c\}$ y $E = \{\alpha, \beta, \gamma, \delta\}$ dos conjuntos y $f : A \rightarrow E$ la aplicación definida por $f(1) = \beta, f(2) = \delta, f(a) = \alpha, f(b) = \alpha, f(c) = \beta$. Entonces la imagen de f es $\Im(f) = \{\alpha, \beta, \delta\}$. La imagen de $B = \{1, 2\} \subseteq A$ es $f(B) = \{\beta, \delta\}$. La imagen inversa de $F = \{\gamma, \delta\} \subseteq E$ es $f^{-1}(F) = \{2\}$.

Ejercicio 9. Sea $f : X \rightarrow Y$ una aplicación. Sean A y B subconjuntos de X , y C y D subconjuntos de Y .

1. Probar que $f(A \cup B) = f(A) \cup f(B)$.
2. ¿Qué relación existe entre $f(A \cap B)$ y $f(A) \cap f(B)$?
3. Probar que $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.
4. ¿Qué relación existe entre $f^{-1}(A \cap B)$ y $f^{-1}(A) \cap f^{-1}(B)$?
5. Si $A \subseteq B$ entonces $f(A) \subseteq f(B)$.
6. Si $C \subseteq D$ entonces $f^{-1}(C) \subseteq f^{-1}(D)$.
7. $f^{-1}(D) - f^{-1}(C) = f^{-1}(D - C)$.

Tipos de aplicaciones. Sea $f : X \rightarrow Y$ una aplicación, decimos que f es *sobreyectiva* si $\Im(f) = Y$, esto es, si para cada elemento $y \in Y$ existe un elemento $x \in X$ tal que $f(x) = y$. Llamamos *inyectiva* a una aplicación $f : X \rightarrow Y$ tal que para cualesquiera dos elementos $x_1, x_2 \in X$, si $f(x_1) = f(x_2)$, entonces $x_1 = x_2$. Diremos que es *biyectiva* si es inyectiva y sobreyectiva.

Ejercicio 10. Sea $g : Q^+ \rightarrow Q^+$ definida por $f(x) = x^2$ para cada $x \in Q^+$. Probar que la aplicación g es inyectiva y no es sobreyectiva.

Supongamos que $f : X \rightarrow Y$ y $g : Y \rightarrow Z$ son aplicaciones, entonces podemos definir una nueva aplicación $g \circ f : X \rightarrow Z$ como sigue:

$$(g \circ f)(x) = g(f(x)) \text{ para cada } x \in X.$$

A $g \circ f$ se llama la *composición* de f y g . La composición de f y g se suele representar también simplemente por gf .

Para cada conjunto X existe una aplicación especial, llamada *identidad* en X , a la que representamos por 1_X y que está definida por $1_X(x) = x$ para cada $x \in X$.

Lema 11. Sea $f : X \rightarrow Y$ una aplicación. Se verifica que $f \circ 1_X = f$ y $1_Y \circ f = f$.

Si $f : X \rightarrow Y$ es una aplicación, llamamos una aplicación inversa de f a una aplicación $g : Y \rightarrow X$ que verifica $f \circ g = 1_Y$ y $g \circ f = 1_X$. En general si una aplicación f tiene una inversa, esta inversa se representa por f^{-1} (¡OJO!. No confundir con la notación f^{-1} utilizada para la imagen inversa de un subconjunto).

Observar que al decir que una aplicación $f : X \rightarrow Y$ tiene una inversa hemos dicho que existe una aplicación $g : Y \rightarrow X$ verificando $fg = 1_Y$ y $gf = 1_X$, no basta con sólo una de las igualdades, ya que dada la aplicación $f : \{1, 2\} \rightarrow \{a\}$ existe una aplicación $g : \{a\} \rightarrow \{1, 2\}$ verificando $fg = 1_{\{a\}}$, pero no es biyectiva.

Lema 12. Una aplicación tiene una inversa si, y sólo si, es biyectiva. Además, en ese caso, sólo tiene una única inversa.

3. Relaciones

Una *relación* R en un conjunto X es una regla que permite distinguir si dos elementos están o no relacionados. Si dos elementos $x, y \in X$ están relacionados mediante la relación R escribimos xRy . Veamos algunas de las propiedades que puede verificar una relación.

Propiedad reflexiva. Decimos que la relación R verifica la propiedad reflexiva si para cada elemento $x \in X$ se verifica xRx .

Propiedad simétrica. Decimos que R verifica la propiedad simétrica si cuando para dos elementos $x, y \in X$ se verifica que si xRy , entonces también se tiene yRx .

Propiedad transitiva. Decimos que R verifica la propiedad transitiva si cuando para tres elementos $x, y, z \in X$ se verifica que si xRy e yRz , entonces también se verifica xRz .

Propiedad antisimétrica. Decimos que R verifica la propiedad antisimétrica si cuando para dos elementos $x, y \in X$ se verifica xRy e yRx , entonces se verifica $x = y$.

Ejemplo 13. (a) Consideramos el conjunto \mathbb{N} de los números naturales y definimos aRb si existe $c \in \mathbb{N}$ tal que $a = b + 2c$ o $b = a + 2c$. Entonces R verifica las propiedades reflexiva, simétrica y transitiva.

(b) Consideramos el conjunto \mathbb{Z} de los números enteros y definimos aRb si $a - b$ es un múltiplo de 2. Entonces R verifica las propiedades reflexiva, simétrica y transitiva.

(c) Consideramos el conjunto \mathbb{N} de los números naturales y definimos la relación aRb si existe $c \in \mathbb{N}$ tal que $b = ac$. Entonces R verifica las propiedades reflexiva, antisimétrica y transitiva.

Decimos que una relación R que verifica las propiedades reflexiva, simétrica y transitiva es una *relación de equivalencia*. Si R es una relación de equivalencia en un conjunto X , para cada elemento $a \in X$ definimos la *clase de equivalencia* de a como el subconjunto $[a] = \{x \in X \text{ such that } aRx\}$.

Lema 14. Si $a, b \in X$ entonces se verifica que $[a] = [b]$ ó $[a] \cap [b] = \emptyset$, esto es, cada dos clases de equivalencia o son iguales, o son disjuntas.

Si R es una relación de equivalencia en un conjunto X , el conjunto de todas las clases de equivalencia se llama el *conjunto cociente* de X por R , y se representa por X/R . Si R es una relación de equivalencia en un conjunto X y X/R es el conjunto cociente, existe una aplicación sobreyectiva $p : X \rightarrow X/R$ que a cada elemento $x \in X$ le asocia $p(x) = [x]$.

Decimos que una relación R que verifica las propiedades reflexiva, antisimétrica y transitiva es una *relación de orden*. Un conjunto X junto con una relación de orden se llama un *conjunto parcialmente ordenado*. Si Y es un subconjunto de un conjunto parcialmente ordenado X con relación orden R , llamamos *elemento maximal* de Y a un elemento $m \in Y$ tal que no existe ningún elemento $y \in Y$ tal que mRy ; *cota superior* de Y en X a un elemento $c \in X$ tal que yRc para cada elemento $y \in Y$; *elemento máximo* de Y a un elemento $m \in Y$ tal que yRm para cada elemento $y \in Y$. Esto es, un máximo de Y es una cota superior de Y en X que pertenece a Y .

Ejercicio 15. Demostrar que en un conjunto parcialmente ordenado el elemento máximo de un subconjunto, si existe, es único.

Una *partición* de un conjunto X es un conjunto de subconjuntos de X , disjuntos dos a dos, cuya unión es X . Si R es una relación de equivalencia en un conjunto X , entonces el conjunto de las clases de equivalencia, para la relación de equivalencia R , forma una partición de X ; la llamamos la partición definida por la relación R . El resultado recíproco también es cierto, esto es, para cualquier partición $\{X_\alpha \text{ tal que } \alpha \in \Gamma\}$ de un conjunto X , existe una relación de equivalencia R en X de forma que la partición definida por R coincide con la partición $\{X_\alpha \text{ tal que } \alpha \in \Gamma\}$. Basta definir R como sigue: si x e y son elementos de X entonces xRy si x e y pertenecen a un mismo subconjunto X_α .

Lema 16. La relación R , así definida, es una relación de equivalencia.

4. Cardinalidad

De un conjunto que tiene un número finito de elementos diremos que es un *conjunto finito*, en caso contrario, si no tiene un número finito de elementos, diremos que es un *conjunto infinito*. Cuando un conjunto X es finito, al número de elementos lo llamaremos el *cardinal* de X , y lo notaremos por $\text{Card}(X)$.

Ejemplo 17. 1. $\text{Card}(\emptyset) = 0$.

2. El conjunto $A = \{1, 2, a, b, c\}$ es un conjunto finito y $\text{Card}(A) = 4$.

3. El conjunto \mathbb{R} de los números reales es un conjunto infinito.

Lema 18. Si X es un conjunto con n elementos, el conjunto $\mathcal{P}(X)$ tiene 2^n elementos.

Podemos distinguir dos tipos de conjuntos infinitos: *numerables* y *no numerables*. Un conjunto X se dice numerable si existe una aplicación biyectiva $f : X \rightarrow \mathbb{N}$. En caso contrario, diremos que es no numerable.

Ejemplo 19. El conjunto \mathbb{Z} de los números enteros es infinito numerable mediante la función $f : \mathbb{Z} \rightarrow \mathbb{N}$ definida por:

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

Ejemplo 20. El conjunto \mathbb{R} de los números reales es un conjunto infinito no numerable

Proposición 21. Si X es un conjunto infinito numerable, entonces $\mathcal{P}(X)$ es un conjunto infinito no numerable.

5. Inducción

Se dice que un subconjunto A de \mathbb{N} es *inductivo* si, para cada $a \in A$, se cumple que $a + 1 \in A$. Por ejemplo, $A = \{5, 6, 7, \dots\}$ es inductivo, pero $B = \{5, 6, 7, 9, 10, \dots\}$ no lo es ya que $7 \in A$ y $8 \notin A$.

Lema 22. Cualquier conjunto inductivo es infinito (numerable).

Proposición 23 (Principio de inducción). Dado $A \subseteq \mathbb{N}$ verificando que:

- $0 \in A$.
- Si $n \in A$ entonces $n + 1 \in \mathbb{N}$

entonces $A = \mathbb{N}$. En otras palabras, el único conjunto inductivo que contiene al cero es \mathbb{N} .

Esto se puede generalizar a lo siguiente: si A es un conjunto inductivo tal que $a \in \mathbb{N}$ es su primer elemento entonces $A = \{a, a + 1, a + 2, \dots\}$.

El principio de inducción se usa para definir funciones recursivas.

Ejemplo 24. El factorial de un elemento se define de forma inductiva como:

- $0! = 1$
- $(n + 1)! = (n + 1) \cdot n!$ para cada $n > 0$

También es usado para probar que una propiedad $P(n)$ (indexada mediante \mathbb{N}) se cumple para todo $n \geq k$. Los pasos de una demostración por inducción son los siguientes:

1. *Caso base*, probar que $P(k)$ es cierta.
2. *Paso de inducción*, probar que si $P(n)$ es cierta (*hipótesis de inducción*) entonces $P(n + 1)$ es cierta para todo $n \geq k$.

3. *Aplicar el Principio de Inducción*, entonces se prueba que $P(n)$ es cierta para $n \geq k$.

Ejemplo 25. Probar que, para todo $n \in \mathbb{N}$, $2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1$

Demostración. Seguimos los pasos de una demostración por inducción:

1. *Caso base.* Para $n = 0$, la igualdad es $2^0 = 2^1 - 1$, que claramente es cierta.
2. *Paso de inducción.* Por la hipótesis de inducción

$$(2^0 + \dots + 2^n) + 2^{n+1} = (2^{n+1} - 1) + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1$$

3. Por lo tanto, por el principio de inducción, la propiedad se cumple para $n \geq 0$.