Capítulo 1

Conjuntos, aplicaciones y relaciones

1.1. Conjuntos

1.1.1. Generalidades sobre conjuntos.

Comenzamos esta notas con una introducción de algunos conceptos básicos sobre conjuntos.

La idea de conjunto es una de las más importantes en matemáticas, pues gran parte de ellas está escrita en lenguaje de teoría de conjuntos.

Un conjunto va a ser para nosotros una colección de objetos. En principio, estos objetos pueden tener cualquier naturaleza, y pueden ser de cualquier tamaño. Normalmente, los objetos que agrupamos suelen tener algunas propiedades comunes aunque esto no tiene porqué ser así. Por ejemplo, los estudiantes de primero C del grado en Ingeniería Informática de la ETSIIT forman un conjunto. O los números naturales menores que 100 forman otro conjunto. Pero también podemos agrupar en un conjunto a tres estudiantes de primero C junto con el número π, las uvas que me tomé el pasado 1 de enero y la estrella más cercana al Sol. En este caso, no hay relación alguna entre los distintos elementos que forman el conjunto.

El lenguaje de teoría de conjuntos permite un estudio organizado de estas colecciones y proporciona un soporte para el estudio de otras estructuras.

El primero en definir esta noción de conjunto fue el matemático ruso-alemán George Cantor, que lo hizo en 1895. Esta definición, no obstante, es muy imprecisa, pues no se especifica que se entiende por un objeto. Esto provoca que la teoría desarrollada dé lugar a paradojas y contradicciones lógicas, como mostró Bertrand Russell en 1902. Para evitar estos problemas fue necesario estudiar los conjuntos en base a una axiomática. La más usada actualmente es la debida a Zermelo y Fraenkel, que fue establecida en 1922. Sin embargo, lo que se gana en rigor al establecer esta axiomática se pierde en intuición.

Como hemos dicho nosotros aquí nos basaremos en la idea de Cantor (algunos conocen esta teoría como *teoría naif de conjuntos*).

Un conjunto es entonces para nosotros una colección de objetos. Sobre los objetos que pueden formar un conjunto no se dice nada más, pues podrían ser cualquier cosa.

A los objetos que forman parte de un conjunto, los llamaremos *elementos* del conjunto.

Relación de pertenencia.

Cuando un elemento forma parte de un conjunto, diremos que ese elemento *pertenece* al conjunto, y lo representaremos mediante el símbolo $\in$. Es decir, si tenemos un conjunto X, y a es un elemento que pertenece al conjunto X, escribiremos $a \in X$. Así, si llamamos X al conjunto de los números naturales menores que 10 tenemos que 5 es un elemento de X, luego $5 \in X$ (se lee 5 pertenece a X).

Cuando tengamos que varios elementos $a_1, a_2, \cdots, a_n$ tal que todos ellos pertenecen a un conjunto X escribiremos $a_1, a_2, \cdots, a_n \in X$. Por ejemplo, con el conjunto X que hemos descrito anteriormente, podríamos escribir $2, 3, 5, 7 \in X$, en lugar de $2 \in X$, $3 \in X$, $5 \in X$ y $7 \in X$.

Si hay algún objeto que no pertenece a un conjunto, emplearemos el símbolo $\notin$. De esta forma tenemos que $13 \notin X$. Informalmente, cuando un elemento pertenezca a un conjunto diremos que dicho elemento *está* en el conjunto.

Entre los conjuntos consideramos uno formado por la colección de cero objetos, es decir, un conjunto que no tiene elementos. Dicho conjunto lo llamaremos *conjunto vacío* y será nombrado como $\emptyset$.

Descripción de conjuntos.

Un conjunto queda caracterizado por los elementos que tiene. Para determinar un conjunto entonces podemos hacerlo enumerando todos sus elementos. En tal caso, los elementos se escriben serparados por comas y entre llaves. Por ejemplo, el conjunto X que hemos nombrado antes sería

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

Siguiendo esta notación, el conjunto vacío lo podemos representar como $\{\}$ (aunque preferimos la notación $\emptyset$).

Como hemos dicho, no vamos a poner restricciones a la naturaleza de los elementos de un conjunto. En particular, un conjunto puede ser elemento de otro conjunto (e incluso de sí mismo). Así, podemos tomar $Y = \{X, 3\}$, un conjunto que tiene dos elementos: el conjunto X y el número 3. El conjunto $\{X, \emptyset\}$ tiene también dos elementos: el conjunto X y el conjunto vacío.

El conjunto cuyo único elemento es el conjunto vacío es $\{\emptyset\}$ (que es distinto de $\emptyset$). También se puede denotar ese conjunto como $\{\{\}\}$.

Cuando el conjunto tiene muchos elementos, o bien cuando es un conjunto infinito, esta forma de especificar el conjunto no es útil. Pensemos, por ejemplo, en el conjunto de números naturales menores que 100000. No vamos a hacer una lista con todos los elementos del conjunto. Una forma para describir este conjunto podría ser $Y = \{0, 1, 2, 3, \cdots, 999998, 999999\}$.

Lo que hace falta es que quede claro cuando un objeto pertenece o no al conjunto. En este ejemplo, tenemos que $573459 \in Y$ pero $5734592 \notin Y$.

El siguiente conjunto

$$\{0, 1, 2, \cdots\}$$

representa el conjunto de todos los números naturales, y es denotado como $\mathbb{N}$. También podemos describir el conjunto de los números enteros, que denotaremos como $\mathbb{Z}$

$$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$$

Otros conjuntos infinitos con los que trabajaremos a lo largo del curso son, por ejemplo, el conjunto de los números racionales ($\mathbb{Q}$), el conjunto de los números reales ($\mathbb{R}$), el conjunto de los números complejos ($\mathbb{C}$), etc.

Hay otra forma de especificar un conjunto, y es a partir de una o varias propiedades que determinen de forma exclusiva los elementos de ese conjunto. Normalmente, en este caso, haremos referencia a un conjunto y especificaremos los elementos de este conjunto que verifican la propiedad. Por ejemplo, el conjunto X podemos describirlo:

$$X = \{n \in \mathbb{N} | n < 10\}$$

Y se leería X *es el conjunto de todos los* $n \in \mathbb{N}$ *tales que* n *es menor que 10*, o si preferimos, el conjunto de todos los números naturales menores que 10. En este caso, hemos hecho referencia al conjunto de los números naturales. También podríamos haberlo descrito haciendo referencia a los números enteros como

$$X = \{n \in \mathbb{Z} | 0 \leq n < 10\}$$

A esta forma de describir un conjunto la llamaremos implícita, en contraposición a la que consiste en enumerar los elementos, que llamaremos explícita.

Por ejemplo, si P es el conjunto de los números pares, entonces podemos describirlo como sigue:

$$P = \{\cdots - 6, -4, -2, 0, 2, 4, 6, \cdots\} = \{n \in \mathbb{Z} | n \text{ es par }\} = \{n \in \mathbb{Z} | \text{existe } m \in \mathbb{Z} : n = 2m\}$$

$$P = \{n \in \mathbb{Z} | n = 2m \text{ para algún } m \in \mathbb{Z}\}$$

Incluso, podríamos escribir:

$$P = \{2n : n \in \mathbb{Z}\} = 2\mathbb{Z}$$

Con la notación $2\mathbb{Z}$ queremos decir el conjunto de todos los números que se obtienen de multiplicar por 2 los elementos de $\mathbb{Z}$. No interpretar como el producto de un número por un conjunto.

¿Cómo podríamos entonces especificar el conjunto de los números impares? ¿y el de los números que dan resto 2 al dividirlos por 5?

El que no conozcamos si un objeto pertenece o no a un conjunto no significa que no esté bien descrito. Por ejemplo, el conjunto $\mathbb{Q}$ está perfectamente determinado. El número real γ (la constante de Euler)[1] también. Sin embargo, no se sabe con certeza si γ pertenece a $\mathbb{Q}$ o no.

Igualdad e inclusión de conjuntos.

Hemos dicho más arriba que un conjunto queda determinado por los elementos que tiene. No influye por tanto el orden en que estén dados esos elementos ni ningún otro factor. En tal caso, los conjuntos $A = \{3, 1, 5\}$ y $B = \{1, 3, 5\}$ son iguales, e iguales al conjunto $\{m \in \mathbb{N} | m \text{ impar y } m \leq 6\}$. También el conjunto A es igual al conjunto $C = \{1, 3, 3, 5, 5, 5, 3, 5, 5\}$ pues todos los elementos que pertenecen a C pertenecen a A y todos los elementos que pertenecen a A pertenecen también a C.

La igualdad de conjuntos, por tanto, podría definirse así:

Definición 1. *Sean A y B dos conjuntos. Se dice que A y B son iguales ($A = B$) si para cualquier $x \in A$ se tiene que $x \in B$ y viceversa, es decir, para cualquier $x \in B$ se tiene que $x \in A$.*

Cuando todos los elementos de un conjunto A son también elementos de un conjunto B diremos que A es un subconjunto de B, y lo representaremos como $A \subseteq B$. También puede leerse esto como A está contenido en B o B contiene a A.

Esto queda recogido en la siguiente definición:

Definición 2. *Sean A y B dos conjuntos. Diremos que A es un subconjunto de B, que A está contenido en B, o que B contiene a A, y escribiremos $A \subseteq B$ si para cualquier elemento $x \in A$ se tiene que $x \in B$.*

Notemos que si X es un conjunto, es lo mismo decir $a \in X$ que $\{a\} \subseteq X$.

De acuerdo con lo que hemos dicho antes, dos conjuntos A y B son iguales cuando A es subconjunto de B y B es subconjunto de A, pues en tal caso, todos los elementos de A están en B y todos los elementos de B pertenecen a A. Normalmente, para demostrar que dos conjuntos son iguales, probaremos que cada uno es subconjunto del otro.

$$\left.\begin{array}{l} A \subseteq B \\ B \subseteq A \end{array}\right\} \Longrightarrow A = B$$

(de hecho, la anterior implicación es una equivalencia)

Esta propiedad se conoce como *antisimétrica*

Si A es un subconjunto de B distinto de B y queremos hacer notar esta relación escribiremos $A \subsetneq B$ (algunos autores emplean la notación $A \subset B$). En tal caso, diremos que A está contenido propiamente en B. Obviamente, $A \subsetneq B$ si, y sólo si, $A \subseteq B$ y existe un elemento $b \in B$ tal que $b \notin A$.

Ejemplo 1.1.1. *$P \subsetneq \mathbb{Z}$, pues $P \subseteq \mathbb{Z}$ (todo elemento de P es un número entero) y existe un número entero (de hecho existen muchos), por ejemplo, 1 que no pertenece a P (recordemos que P denotaba el conjunto de los números pares).*

Dado cualquier conjunto X, el conjunto vacío es un subconjunto de X (es decir, $\emptyset \subseteq X$), pues todos los elementos del vacío, absolutamente todos, sin excepción, son elementos de X.

Por ejemplo, tomamos $A = \{m \in \mathbb{N} | m < 0\}$. Es claro que A es un subconjunto de $\mathbb{N}$, pues en A hemos tomado todos los números naturales que cumplen una propiedad (ser menor que cero). Además, es claro que $A = \emptyset$. Por tanto, $\emptyset \subseteq \mathbb{N}$.

El conjunto vacío es el conjunto de todos los círculos cuadrados, luego $\emptyset$ es un subconjunto del conjunto de todos los círculos, y es un subconjunto del conjunto de todos los cuadrados.

[1] Se define la constante de Euler γ como $\gamma = \lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - log(n) \right)$. Su valor aproximado es $\gamma \sim 0'577...$

El conjunto vacío es el conjunto de todos los hombres con 7 manos (creo que no hay ninguno) por tanto, el conjunto vacío es un subconjunto del conjunto de todos los hombres.

El conjunto vacío es el conjunto de todos los números racionales e irracionales, luego es un subconjunto de $\mathbb{Q}$ y del conjunto de todos los números irracionales.

Hemos visto que la inclusión de conjuntos es antisimétrica. También es reflexiva (todo conjunto es subconjunto de sí mismo) y transitiva (si A es subconjunto de B y B es subconjunto de C entonces A es subconjunto de C).

Hemos dicho antes que un conjunto puede ser elemento de otro conjunto. Un conjunto, podría ser entonces $A = \{1, \mathbb{N}, \{0, 1, 2, 3\}\}$. Este conjunto tendría tres elementos. Estos son: 1, el conjunto de los números naturales, y el conjunto $\{0, 1, 2, 3\}$.

Si renombramos a los elementos de A, $x_1 = 1$, $x_2 = \mathbb{N}$ y $x_3 = \{0, 1, 2, 3\}$ tenemos entonces que $A = \{x_1, x_2, x_3\}$. Es decir, A, como conjunto tiene exactamente 3 elementos, que son x_1, x_2 y x_3. A su vez, $x_1 \in x_2$, $x_1 \in x_3$ y $x_3 \subseteq x_2$.

El conjunto vacío, como conjunto que es, puede ser elemento de otro conjunto. Así, podemos formar un conjunto cuyo único elemento sea el conjunto vacío. Es decir, el conjunto $X = \{\emptyset\}$ (que también podemos denotar como $\{\{\}\}$). No confundir este conjunto con el conjunto vacío, que no tiene elementos (no es lo mismo una caja vacía que una caja que contiene a una caja vacía. La primera no tiene nada, mientras que la segunda contiene a una caja).

Notemos que para este conjunto X se tiene que $\emptyset \in X$ (de hecho es su único elemento) y $\emptyset \subseteq X$ (pues el conjunto vacío es subconjunto de cualquier conjunto)

Conjunto potencia.

Definición 3. *Dado un conjunto X podemos formar el conjunto cuyos elementos son los subconjuntos de X. Este conjunto será denotado como $\mathcal{P}(X)$, y lo llamaremos el conjunto* partes de X. *Es decir:*

$$\mathcal{P}(X) = \{A | A \subseteq X\}$$

Como ya sabemos, para cualquier X, el conjunto vacío es un subconjunto de X, luego $\emptyset \in \mathcal{P}(X)$. También se tiene que $\emptyset \subseteq \mathcal{P}(X)$. Otro subconjunto de X es el propio X, es decir, $X \in \mathcal{P}(X)$.

Ejemplo 1.1.2. *Sea $X = \{1, 2\}$. Entonces $\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.*

Por otra parte, $\mathcal{P}(\emptyset) = \{\emptyset\}$ (tiene un elemento).

$\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$ (tiene 2 elementos)

$\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \{\emptyset,\ \{\emptyset\},\ \{\{\emptyset\}\},\ \{\emptyset, \{\emptyset\}\}\}$ (tiene 4 elementos). Si denotamos por $\{\}$ al conjunto vacío, nos quedaría $\mathcal{P}(\mathcal{P}(\mathcal{P}(\{\}))) = \{\{\},\ \{\{\}\},\ \{\{\{\}\}\},\ \{\{\}, \{\{\}\}\}\}$, donde la notación es un poco engorrosa.

1.1.2. Operaciones con conjuntos.

Vamos a ver a continuación cómo, a partir de algunos conjuntos podemos obtener otros nuevos.

Unión de conjuntos.

Dados dos conjuntos A y B, podemos formar un nuevo conjunto reuniendo los elementos que, bien pertenecen a A, bien pertenecen a B. Obtenemos así el conjunto denominado *unión* de A y B, y que representaremos como $A \cup B$.

Definición 4. *Sean A y B dos conjuntos. Definimos la unión de A y B como*

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

Ejemplo 1.1.3. *Si A_1 es el conjunto de los números naturales pares menores que 15, y A_2 el conjunto de los números primos menores que* 15 *entonces $A_1 \cup A_2 = \{0, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14\}$*

Los elementos $0, 2, 4, 6, 8, 10, 12, 14$ pertenecen a $A_1 \cup A_2$ pues todos ellos pertenecen a A_1, mientras que $2, 3, 5, 7, 11, 13$ pertenecen a $A_1 \cup A_2$ pues todos ellos pertenecen a A_2.

De la misma forma, podría definirse la unión de tres o más conjuntos. Así, si llamamos ahora A_3 al conjunto $\{1, 5, 7, 11\}$ entonces

$$A_1 \cup A_2 \cup A_3 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14\}$$

Pues cada uno de los elementos que hemos indicado pertenece al menos a uno de los conjuntos A_1, A_2 ó A_3. También podría haberse definido la unión de tres conjuntos A_1, A_2, A_3 como $A_1 \cup A_2 \cup A_3 = (A_1 \cup A_2) \cup A_3$. Puede comprobarse fácilmente que $(A_1 \cup A_2) \cup A_3 = A_1 \cup (A_2 \cup A_3)$.

Para indicar la unión de los tres conjuntos A_1, A_2, A_3 podríamos haber empleado la notación $\bigcup\limits_{i=1}^{3} A_i$. De esta forma podemos indicar de forma compacta la unión de una colección mayor de conjuntos. Incluso, la unión de infinitos conjuntos.

Ejemplo 1.1.4. *Sea $A_1 = \{1, 3, 5, 7, 9, 11\}$, $A_2 = \{2, 6, 10, 14, 18, 22\}$, $A_3 = \{1, 4, 9, 16, 25\}$, $A_4 = \{3, 6, 9, 12, 15, 18\}$. Entonces:*

$$\bigcup_{i=1}^{4} A_i = \{1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 14, 15, 16, 18, 22, 25\}$$

Un elemento pertenece a la unión de estos cuatro conjuntos si pertenece al menos a uno de ellos.

También se tiene, por ejemplo, que $\bigcup\limits_{i=1}^{2} A_{2i} = A_2 \cup A_4 = \{2, 3, 6, 9, 10, 12, 14, 15, 18, 22\}$.

Para cada número natural n vamos a considerar el conjunto $B_n = \{n, n+1, \cdots, 2n\}$. Es decir, $B_0 = \{0\}$, $B_1 = \{1, 2\}$, $B_2 = \{2, 3, 4\}$, etc.

Entonces, la unión de todos estos conjuntos es el conjunto de los números naturales (pues todo número natural pertenece a alguno de estos conjuntos) y la podemos representar como

$$\bigcup_{i=0}^{\infty} B_i = \bigcup_{n \in \mathbb{N}} B_i = \mathbb{N}$$

Notemos que si A y B son dos conjuntos, entonces tanto A como B son subconjuntos de $A \cup B$, y $A \cup B$ es el *menor* conjunto que tiene esa propiedad (tener a A y B como subconjuntos). Dicho de otra forma:

$$\begin{matrix} A \subseteq A \cup B \\ B \subseteq A \cup B \end{matrix} \quad \text{y si} \quad \begin{matrix} A \subseteq C \\ B \subseteq C \end{matrix} \quad \text{entonces} \quad A \cup B \subseteq C$$

es decir, A y B son subconjuntos de $A \cup B$ y si hubiera otro conjunto C que tuviera a A y a B como subconjuntos, entonces también tiene a $A \cup B$ como subconjunto (en este sentido decimos que $A \cup B$ es el menor conjunto con esa propiedad).

Intersección de conjuntos.

Definición 5. *Dados dos conjuntos A y B se define la intersección de A y B como el conjunto formado por los elementos que pertenecen simultáneamente a A y a B. Dicho conjunto se denota como $A \cap B$.*

$$A \cap B = \{x | x \in A \ y \ x \in B\} = \{x \in A | x \in B\} = \{x \in B | x \in A\}$$

Cuando la intersección de dos conjuntos es el conjunto vacío se dice que esos conjuntos son disjuntos.

Ejemplo 1.1.5. *Para los conjuntos A, B y C del ejemplo anterior se tiene que*

$$A \cap B = \{2\} \qquad A \cap C = \emptyset \qquad B \cap C = \{5, 7, 11\}$$

De forma análoga a como se hizo con la unión puede definirse la intersección de tres o más conjuntos. Y la misma notación que seguimos para indicar la unión de dos o más conjuntos nos vale ahora para la intersección.

La intersección de dos conjuntos A y B es un subconjunto de A y de B. De hecho es el *mayor* subconjunto común de ambos.

$$\begin{matrix} A \cap B \subseteq A \\ A \cap B \subseteq B \end{matrix} \quad \text{y si} \quad \begin{matrix} C \subseteq A \\ C \subseteq B \end{matrix} \quad \text{entonces} \quad C \subseteq A \cap B$$

Diferencia de conjuntos.

Definición 6. *Si A y B son dos conjuntos, se define el conjunto diferencia $A \setminus B$ como el conjunto formado por los elementos de A que no pertenecen a B (es decir, para formar $A \setminus B$ le quitamos a A los elementos que están en B).*

$$A \setminus B = \{x \in A | x \notin B\}$$

Ejemplo 1.1.6. *Para los conjuntos A y B del ejemplo anterior se tiene que $A \setminus B = \{0, 4, 6, 8, 10, 12, 14\}$ (a A le quitamos el 2 que es el único elemento que pertenece a B), mientras que $B \setminus A = \{3, 5, 7, 11, 13\}$.*

Notemos que dados dos conjuntos cualesquiera A y B se tiene que $A \setminus B = A \setminus (A \cap B)$, pues al quitarle a A un elemento que está en B en realidad estamos quitando un elemento que está en $A \cap B$ (si no estuviera en A no habría que quitarlo).

Veamos una demostración de esto. Como hemos dicho antes, para ver que dos conjuntos son iguales probaremos que uno está incluido en el otro y el otro en el uno.

En primer lugar veamos que $A \setminus B \subseteq A \setminus (A \cap B)$, es decir, que todo elemento de $A \setminus B$ pertenece a $A \setminus (A \cap B)$.

Sea $x \in A \setminus B$. Entonces $x \in A$ y $x \notin B$. Por tanto, $x \notin A \cap B$ (pues no pertenece a B). Tenemos entonces que $x \in A$ y $x \notin A \cap B$, luego $x \in A \setminus (A \cap B)$.

Recíprocamente, si $x \in A \setminus (A \cap B)$ entonces $x \in A$ y $x \notin A \cap B$. Como $x \notin A \cap B$, x no puede ser simultáneamente elemento de A y de B, luego o no es elemento de A o no es elemento de B, es decir, $x \notin A$ ó $x \notin B$. La primera opción no puede darse, pues teníamos que $x \in A$, luego se da la segunda, es decir, $x \notin B$. Y lo que tenemos ahora es que $x \in A$ y $x \notin B$, luego $x \in A \setminus B$.

Diferencia simétrica.

Definición 7. *Dados dos conjuntos A y B se define la diferencia simétrica de A y B como el conjunto $A \Delta B = (A \setminus B) \cup (B \setminus A)$.*

Es decir, en $A \Delta B$ están los elementos que pertenecen a uno de los dos conjuntos, A ó B, pero no a ambos. Podría entonces haberse definido como $(A \cup B) \setminus (A \cap B)$. Queda como ejercicio demostrar que ambas definiciones son equivalentes.

Para los conjuntos A y B de los ejemplos anteriores se tiene que

$$A \Delta B = \{0, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14\}.$$

Complementario.

Normalmente, cuando estamos trabajando con conjuntos, fijaremos un conjunto de referencia al que llamaremos *universo*, y todas las operaciones que realicemos serán entre subconjuntos del mismo. Así, en los ejemplos que hemos visto, podríamos haber trabajado con $\mathbb{N}$ como universo. Todos los conjuntos que intervienen son subconjuntos de $\mathbb{N}$.

Definición 8. *Si X es un universo, y A es un conjunto (un subconjunto de X), se define el complementario de A como el conjunto formado por todos los elementos (de X) que no pertenecen a A. El complementario de un conjunto A será denotado como $\overline{A}$ o A'.*

Si $X = \mathbb{N}$, y P es el subconjunto formado por los números pares, entonces $\overline{P}$ es el conjunto de todos los números impares.

Notemos que el conjunto $\overline{A}$ es igual al conjunto $X \setminus A$, y que dados A y B dos subconjuntos de un conjunto X entonces $A \setminus B = A \cap \overline{B}$, pues $A \setminus B$ son los elementos de A que no pertenecen a B, es decir, los elementos de A que pertenecen a $\overline{B}$.

Tablas de pertenencia.

Si X es un conjunto que tomamos como universo, y $A_1, A_2, \cdots A_n$ son subconjuntos de X, para cada conjunto C que podamos formar a partir de los conjuntos $A_1, A_2, \cdots, A_n$ vamos a definir la denominada *tabla de pertenencia*. Esta tabla está formada por ceros y unos, y nos indica la posibilidad de que un elemento pertenezca o no al conjunto C en función de que ese elemento pertenezca o no a cada uno de los conjuntos A_i. Un uno nos indica que el elemento pertenece, y un cero nos indica que no pertenece.

Las tablas de pertenencia para las distintas operaciones que hemos definido serían:

A	B	$A \cup B$
0	0	0
0	1	1
1	0	1
1	1	1

A	B	$A \cap B$
0	0	0
0	1	0
1	0	0
1	1	1

A	B	$A \setminus B$
0	0	0
0	1	0
1	0	1
1	1	0

A	B	$A \Delta B$
0	0	0
0	1	1
1	0	1
1	1	0

A	$\overline{A}$
0	1
1	0

En la primera tabla, la primera fila nos dice que si un elemento no pertenece a A y no pertenece a B (eso está indicado con los dos ceros que hay debajo de A y B respectivamente), entonces no pertenece a $A \cup B$ (eso nos lo dice el cero que hay en la columna de $A \cup B$). La segunda fila nos dice que si un elemento pertenece a B, pero no pertenece a A entonces pertenece a la unión de A y B. Y así, el resto.

Vamos a calcular la tabla de pertenencia de $(A\Delta B)\Delta C$. Como partimos de tres conjuntos, esta tabla tendrá 8 filas, correspondientes a las 8 posibilidades que hay (que un elemento pertenezca o no a A, que pertenezca o no a B y que pertenezca o no a C).

A	B	C	$A\Delta B$	$(A\Delta B)\Delta C$
0	0	0	0	0
0	0	1	0	1
0	1	0	1	1
0	1	1	1	0
1	0	0	1	1
1	0	1	1	0
1	1	0	0	0
1	1	1	0	1

Las tres primeras columnas nos indican las 8 posibilidades que tenemos y que hemos dicho antes. La columna cuarta se obtiene a partir de las columnas primera y segunda, y la tabla de pertenencia de la diferencia simétrica. La columna quinta se obtiene a partir de las columnas tercera y cuarta y la tabla de pertenencia de la diferencia simétrica.

Vamos a calcular la tabla de pertenencia de $A\Delta(B\Delta C)$

A	B	C	$B\Delta C$	$A\Delta(B\Delta C)$
0	0	0	0	0
0	0	1	1	1
0	1	0	1	1
0	1	1	0	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	0	1

Vemos que las columnas correspondientes a $(A\Delta B)\Delta C$ y $A\Delta(B\Delta C)$ coinciden. Eso significa que cualesquiera que sean los conjuntos A, B y C se tiene que $(A\Delta B)\Delta C = A\Delta(B\Delta C)$.

Esto que acabamos de hacer es una forma de demostrar igualdades o identidades entre conjuntos.

A continuación enumeramos una serie de propiedades referentes a las operaciones que hemos visto entre conjuntos.

Propiedades.

Sea X un conjunto y A, B y C subconjuntos de X. Entonces:

1. $A \cup B = B \cup A$.
2. $A \cap B = B \cap A$.

3. $A \cup (B \cup C) = (A \cup B) \cup C = A \cup B \cup C$.
4. $A \cap (B \cap C) = (A \cap B) \cap C = A \cap B \cap C$.
5. $A \cup A = A$.
6. $A \cap A = A$.
7. $A \cup (A \cap B) = A$.
8. $A \cap (A \cup B) = A$.
9. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
10. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
11. $A \cup \emptyset = A$.
12. $A \cap \emptyset = \emptyset$.
13. Si $A \subseteq B$ entonces $A \cup B = B$ (comparar con 7. y 11.).
14. Si $A \subseteq B$ entonces $A \cap B = A$ (comparar con 8. y 12.).
15. $\overline{\overline{A}} = A$.
16. $\overline{X} = \emptyset$.
17. $\overline{\emptyset} = X$.
18. $A \cup \overline{A} = X$.
19. $A \cap \overline{A} = \emptyset$.
20. $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
21. $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
22. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.
23. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.
24. $A \Delta \emptyset = A$
25. $A \Delta A = \emptyset$.
26. $(A \Delta B) \Delta C = A \Delta (B \Delta C)$.
27. $A \Delta B = B \Delta A$.
28. $A \Delta C = B \Delta C \Longrightarrow A = B$.
29. $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$.
30. $A \cup B \subseteq A \cup C$ y $A \cap B \subseteq A \cap C$ entonces $B \subseteq C$.

Podríamos enumerar muchas propiedades más. Las dos técnicas de demostración vistas en esta sección pueden usarse para probarlas.

Vamos a ver algunos ejemplos.

Ejemplo 1.1.7.

1. *Vamos a comprobar que* $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ *para cualesquiera conjuntos* A*,* B*,* C*.*

Doble inclusión.

Demostremos que $A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C)$. Para eso, veremos que todo elemento de $A \setminus (B \cup C)$ es un elemento de $(A \setminus B) \cap (A \setminus C)$.

Sea $x \in A \setminus (B \cup C)$. Entonces, $x \in A$ y $x \notin B \cup C$. Puesto que $x \notin B \cup C$ entonces x no puede perteneces a B y x no puede perteneces a C; es decir, $x \notin B$ y $x \notin C$. Por tanto, tenemos por una parte que $x \in A$ y $x \notin B$, luego $x \in A \setminus B$; y por otra que $x \in A$ y $x \notin C$, de donde $x \in A \setminus C$. Deducimos entonces que $x \in (A \setminus B) \cap (A \setminus C)$

Demostremos ahora que $(A \setminus B) \cap (A \setminus C) \subseteq A \setminus (B \cup C)$.

Sea $x \in (A \setminus B) \cap (A \setminus C)$. Entonces $x \in A \setminus B$ y $x \in A \setminus C$. Es decir, $x \in A$, $x \notin B$ y $x \notin C$. Por tanto, $x \in A$ y $x \notin B \cup C$ (pues no pertenece a B ni a C). Entonces $x \in A \setminus (B \cup C)$, como queríamos.

Tablas de pertenencia.

A	B	C	$B \cup C$	$\mathbf{A \setminus (B \cup C)}$	$A \setminus B$	$A \setminus C$	$\mathbf{(A \setminus B) \cap (A \setminus C)}$
0	0	0	0	**0**	0	0	**0**
0	0	1	1	**0**	0	0	**0**
0	1	0	1	**0**	0	0	**0**
0	1	1	1	**0**	0	0	**0**
1	0	0	0	**1**	1	1	**1**
1	0	1	1	**0**	1	0	**0**
1	1	0	1	**0**	0	1	**0**
1	1	1	1	**0**	0	0	**0**

Al ver que las columnas correspondientes a $A \setminus (B \cup C)$ y $(A \setminus B) \cap (A \setminus C)$ son iguales, concluimos que ambos conjuntos son siempre iguales.

Identidades entre conjuntos.

$$\begin{array}{rcll} A \setminus (B \cup C) & = & A \cap \overline{(B \cup C)} & \\ & = & A \cap (\overline{B} \cap \overline{C}) & \textit{Propiedad 20. Ley de "de Morgan"} \\ & = & A \cap \overline{B} \cap \overline{C} & \textit{Propiedad 4. Asociativa.} \\ & = & A \cap \overline{B} \cap A \cap \overline{C} & \textit{Propiedad 6. Idempotencia.} \\ & = & (A \cap \overline{B}) \cap (A \cap \overline{C}) & \textit{Propiedad 4. Asociativa} \\ & = & (A \setminus B) \cap (A \setminus C) & \end{array}$$

Supongamos que nos piden estudiar qué relación existe entre los conjuntos $A \cup (B \setminus C)$ y $(A \cup B) \setminus (A \cup C)$.

En primer lugar, tomamos tres conjuntos A, B y C y vemos si podemos encontrar alguna relación. Por ejemplo:

Sean $A = \{1, 2, 3, 4, 5\}$, $B = \{3, 4, 6, 7, 8\}$ y $C = \{4, 7, 8, 9, 10\}$.

Entonces $B \setminus C = \{3, 6\}$, luego $A \cup (B \setminus C) = \{1, 2, 3, 4, 5, 6\}$, mientras que $A \cup B = \{1, 2, 3, 4, 5, 6, 7, 8\}$, $A \cup C = \{1, 2, 3, 4, 5, 7, 8, 9, 10\}$ y $(A \cup B) \setminus (A \cup C) = \{6\}$.

Vemos entonces que los conjuntos no son iguales. Pero podría darse el caso de que $(A \cup B) \setminus (A \cup C) \subseteq A \cup (B \setminus C)$.

Vamos a comprobar que efectivamente, se tiene esa inclusión.

Supongamos que $x \in (A \cup B) \setminus (A \cup C)$. Entonces, $x \in (A \cup B)$ y $x \notin A \cup C$. Por tanto, x no puede pertences a A y tampoco a C. Es decir, $x \notin C$, y claramente $x \in B$, de donde deducimos que $x \in B \setminus C$. Entonces se tiene que $x \in A \cup (B \setminus C)$.

También podemos comprobarlo usando las tablas de pertenencia.

A	B	C	$A \cup B$	$A \cup C$	$\mathbf{(A \cup B) \setminus (A \cup C)}$	$B \setminus C$	$\mathbf{A \cup (B \setminus C)}$
0	0	0	0	0	**0**	0	**0**
0	0	1	0	1	**0**	0	**0**
0	1	0	1	0	**1**	1	**1**
0	1	1	1	1	**0**	0	**0**
1	0	0	1	1	**0**	0	**1**
1	0	1	1	1	**0**	0	**1**
1	1	0	1	1	**0**	1	**1**
1	1	1	1	1	**0**	0	**1**

Y vemos como en las filas en las que hay un uno en la columna correspondiente a $(A \cup B) \setminus (A \cup C)$ *(en este caso, sólo la tercera fila), también hay un uno en la columna a* $A \cup (B \setminus C)$.

Vamos a fijarnos un poco más en esta tabla, y en los conjuntos que hemos puesto como ejemplo.

Vemos que el conjunto $(A \cup B) \setminus (A \cup C)$ *tenía un solo elemento, el 6. Este elemento se corresponde con el único elemento que pertenece a* B*, y que no pertenece ni a* A *y a* C*. Esto es así porque el único uno de la columna* $(A \cup B) \setminus (A \cup C)$ *se encuentra en la tercera fila, en la que tenemos un cero en la columna* A*, un uno en la columna* B *y un cero en la columna* C.

En cambio, el conjunto $A \cup (B \setminus C)$ *tiene seis elementos, que son el* 1*, el* 2*, el* 3*, el* 4*, el* 5 *y el* 6.

El 1 *y el* 2 *pertenecen sólo a* A *(no pertenecen ni a* B *ni a* C*, y se corresponden con el 1 que aparece en la quinta fila. El* 5 *se corresponde con el uno de la sexta fila (el* 5 *pertenece a* A *y a* C*, pero no a* B*). El* 3 *se corresponde con el uno de la séptima fila (pertenece a* A *y* B*, pero no a* C*. Y el* 4 *se corresponde con el uno de la última fila (pertenece a* A*, a* B *y a* C*).*

1.1.3. Producto cartesiano

Definición 9. *Dados dos conjuntos* A *y* B *definimos el conjunto producto cartesiano* $A \times B$ *como el conjunto cuyos elementos son parejas, donde la primera componente pertenece a* A *y la segunda componente pertenece a* B*. Es decir:*

$$A \times B = \{(a, b) : a \in A; b \in B\}$$

Ejemplo 1.1.8. *Por ejemplo, si* $A = \{0, 2, 4\}$ *y* $B = \{1, 2\}$ *entonces*

$$A \times B = \{(0, 1),\ (2, 1),\ (4, 1),\ (0, 2),\ (2, 2),\ (4, 2)\}$$

De forma análoga puede definirse el producto cartesiano de tres o más conjuntos. Incluso podría definirse el producto cartesiano de infinitos conjuntos.

Normalmente, el producto cartesiano de un conjunto A por sí mismo será denotado como A^2; el producto $A \times A \times A$ como A^3, y A^k el producto cartesiano de A consigo mismo k veces. Por ejemplo:

$$A^2 = \{(0, 0),\ (0, 2),\ (0, 4),\ (2, 0),\ (2, 2),\ (2, 4),\ (4, 0),\ (4, 2),\ (4, 4)\}$$

$$B^3 = \{(1, 1, 1),\ (1, 1, 2),\ (1, 2, 1),\ (1, 2, 2),\ (2, 1, 1),\ (2, 1, 2),\ (2, 2, 1),\ (2, 2, 2)\}$$

Si $X = \emptyset$ o $Y = \emptyset$ entonces $X \times Y = \emptyset$.

Si A es un conjunto, consideramos el producto cartesiano $A^2 = A \times A$. Definimos la diagonal como el subconjunto de A^2 siguiente:

$$\Delta_A = \{(a, a) : a \in A\}$$

Es decir, Δ_A es el conjunto de parejas de A donde las dos coordenadas son iguales. Por ejemplo, si $A = \{1, 2, 3, 5, 7\}$ entonces $\Delta_A = \{(1, 1),\ (2, 2),\ (3, 3),\ (5, 5),\ (7, 7)\}$.

Cuando no haya lugar a la confusión, escribiremos Δ en lugar de Δ_A.

Algunas propiedades referentes al producto cartesiano de conjuntos:

Propiedades:

Sean X e Y dos conjuntos, y $A, C \subseteq X$, y $B, D \subseteq Y$. Entonces:

1. $A \times B \subseteq X \times Y$.
2. $(A \cup C) \times Y = (A \times Y) \cup (C \times Y)$ y $X \times (B \cup D) = (X \times B) \cup (X \times D)$.
3. $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.
4. $(A \cap C) \times Y = (A \times Y) \cap (C \times Y)$ y $X \times (B \cap D) = (X \times B) \cap (X \times D)$
5. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

La inclusión del apartado tercero puede ser estricta. Da un ejemplo en el que no se de la igualdad.

1.2. Aplicaciones

1.2.1. Definición y ejemplos.

Supongamos que tenemos dos conjuntos X e Y, y que para cada elemento $x \in X$, hemos elegido un elemento (y sólo uno) $y \in Y$. Eso es lo que vamos a llamar una una aplicación de X en Y.

Definición 10. *Sean X e Y dos conjuntos. Una aplicación de X en Y es una forma de asignar a cada elemento de X, un elemento (y sólo uno) de Y.*

Si llamamos f a una aplicación de X en Y, y $x \in X$, el elemento $y \in Y$ que le asignamos a este elemento lo denotaremos como $f(x)$, y leeremos f de x. *Diremos que este elemento es la imagen por (la aplicación) f del elemento x.*

Cuando tengamos una aplicación f, de X en Y, escribiremos $f : X \to Y$, o $X \xrightarrow{f} Y$.

Al conjunto X se le llama dominio *de la aplicación, mientras que al conjunto Y* codominio.

Ejemplo 1.2.1. *Cuando somos pequeñitos, y nos bautizan, o nos inscriben en el registro civil, nos asignan una palabra (o más) que dicen que es nuestro nombre (vamos a suponer que todos tenemos nombres simples). Esta asignación, salvo casos excepcionales, nos marca de por vida. Tenemos de esta forma una aplicación del conjunto de las personas en el conjunto de palabras.*

Más adelante, se nos asigna un número natural que será el que nos identifique. Así tenemos una aplicación del conjunto de los españoles mayores de 18 años en el conjunto de los números naturales.

A cada número natural le vamos a asignar su doble. Vamos a llamar f a esta asignación. Tenemos entonces que f es una aplicación $\mathbb{N} \to \mathbb{N}$. Para cada número natural n su imagen por f es $2n$, es decir, $f(n) = 2n$. Podríamos haber descrito esta aplicación como sigue: Sea $f : \mathbb{N} \to \mathbb{N}$ la aplicación dada por (o definida por) $f(n) = 2n$ (o definida por $n \mapsto 2n$).

Podemos ver entonces f como una regla, o como una máquina, que transforma cada elemento de X en un elemento de Y (en el ejemplo precedente cada número natural en un número natural). Sobre las posibles reglas no hay restricción alguna. Podemos elegir una regla, como la de asignar a cada número su doble, o simplemente, ir eligiendo una a una la imagen de cada elemento, sin ningún criterio aparente. Así, podemos tener la aplicación que asigne al cero el valor 35, al uno el valor 26, al dos el valor 99, al tres el valor 638, al cuatro el valor 2411. Y así podríamos seguir definiendo la imagen de cualquier otro número. Claro, que de esta forma únicamente tenemos definida la aplicación para aquellos valores de los que hemos dicho explícitamente su imagen.

> Podría decirse que la aplicación anterior es la que asigna a cada número natural n menor o igual que cuatro, el número $16n^4 - 32n^3 + 25n^2 - 18n + 35$. En tal caso, podríamos considerar la aplicación $\mathbb{N} \xrightarrow{f} \mathbb{N}$ dada por $f(n) = 16n^4 - 32n^3 + 25n^2 - 18n + 35$ o cualquier otra expresión que satisfaga las cinco condiciones dadas (habría en este caso que comprobar que si $n \in \mathbb{N}$ entonces $16n^4 - 32n^3 + 25n^2 - 18n + 35 \in \mathbb{N}$).
>
> También podría haberse definido la aplicación como $f(0) = 35$, $f(1) = 26$, $f(2) = 99$, $f(3) = 638$, $f(4) = 2411$ y $f(n) = n$ si $n \geq 5$.

Para dar una aplicación $X \to Y$, podemos, bien dar explícitamente la imagen de cada uno de los elementos X, bien dando una regla (o varias) que nos digan cómo calcular la imagen de cada elemento del dominio.

Ejemplo 1.2.2.

1. *Sea $X = \{1, 2, 3, 4, 5\}$, $Y = \{1, 2, 3, 4, 5\}$ y $f : X \to Y$ la aplicación dada por $f(1) = 5$, $f(2) = 2$, $f(3) = 1$, $f(4) = 2$ y $f(5) = 5$.*

   En este caso, hemos dado explícitamente la imagen de cada uno de los elementos del dominio. También podríamos haberlo escrito diciendo que f es la aplicación definida por $1 \mapsto 5$, $2 \mapsto 2$, $3 \mapsto 1$, $4 \mapsto 2$, $5 \mapsto 5$.

2. *La misma aplicación que acabamos de dar, la podríamos haber descrito como la aplicación $f : X \to Y$ dada por $f(x) = x^2 - 6x + 10$. En este caso, hemos dado la aplicación mediante una regla que nos permite calcular $f(x)$ a partir de cualquier elemento $x \in X$.*

3. *Sea $G : \mathbb{N} \to \mathbb{N}$ la aplicación*

$$g(n) = \begin{cases} n+1 & \text{si } n \text{ es par.} \\ n-1 & \text{si } n \text{ es impar.} \end{cases}$$

Es decir, $g(0) = 1$, $g(1) = 0$, $g(2) = 3$, $g(3) = 2$, etc.

En este caso, la aplicación la hemos definido mediante dos reglas. Una que nos permite calcular la imagen de los números pares, y otra que nos permite calcular la imagen de los números impares.

Esta misma aplicación la podríamos haber definido mediante una única regla, que sería $g(n) = n + (-1)^n$.

Definición 11. *Si $f : X \to Y$ es una aplicación, se define el grafo de f como el conjunto:*

$$G(f) = \{(x, f(x)) : x \in X\}$$

es decir, las parejas formadas por un elemento y su imagen.

Notemos que $G(f)$ es un subconjunto de $X \times Y$. Muchos autores definen una aplicación a partir de su grafo. Una aplicación de X en Y sería un subconjunto G de $X \times Y$ de forma que para cualquier $x \in X$ existe un único elemento $y \in Y$ tal que $(x, y) \in G$.

Ejemplo 1.2.3. *Por ejemplo, si $X = \{1, 2, 3\}$, $Y = \{a, b, c, d\}$ y $f : X \to Y$ es la aplicación dada por $f(1) = b$, $f(2) = c$ y $f(3) = b$, entonces $G(f) = \{(1, b),\ (2, c),\ (3, b)\}$. Notemos que el conjunto $\{(1, b),\ (2, c),\ (3, b)\}$ determina totalmente a la aplicación f.*

Para cualquier conjunto X tenemos una aplicación $X \to X$ dada por $x \mapsto x$. Esta aplicación se conoce como aplicación identidad*, y se denota como Id_X o 1_X. En este caso, el grafo de la aplicación es el conjunto diagonal Δ_X.*

Si A es un subconjunto de un conjunto X, tenemos la aplicación $i : A \to X$ definida como $i(x) = x$. Esta aplicación se conoce como aplicación inclusión.

Como caso especial, consideramos que para cualquier conjunto X hay una aplicación $\emptyset \to X$. Su grafo es el único subconjunto de $\emptyset \times X = \emptyset$.

La siguiente regla $\frac{a}{b} \mapsto a + b$ no define ninguna aplicación $\mathbb{Q} \to \mathbb{Z}$, ya que no determina de forma única la imagen de un elemento. Por ejemplo, $\frac{1}{2}$ podría tener como imagen a 3, a 6 (pues $\frac{1}{2} = \frac{2}{4}$), a -3 y en general a cualquier múltiplo no nulo de 3. El único elemento que tendría determinada su imagen es -1.

1.2.2. Imagen directa e imagen inversa.

Definición 12. *Sea $f : X \to Y$. Definimos entonces dos nuevas aplicaciones.*

$$f_* : \mathcal{P}(X) \to \mathcal{P}(Y) \qquad f_*(A) = \{f(x) : x \in A\}$$
$$f^* : \mathcal{P}(Y) \to \mathcal{P}(X) \qquad f^*(B) = \{x \in X | f(x) \in B\}$$

Es decir, si A es un subconjunto de X, entonces $f_*(A)$ es el conjunto formado por todas las imágenes de los elementos de A, mientras que $f^*(B)$ está formado por todos los elementos de X cuyas imágenes pertenecen a B. Las aplicaciones f_* y f^* se conocen como aplicaciones *imagen directa* e *imagen iversa* respectivamente.

Al conjunto $f_*(X)$ se le conoce como la *imagen* de f. Será denotado como $Im(f)$.

Algunos autores escriben $f(A)$ en lugar de $f_*(A)$ y $f^{-1}(B)$ en lugar de $f^*(B)$.

Ejemplo 1.2.4.

1. *Sea E el conjunto de todos los ciudadanos españoles, y $f : E \to \mathbb{N}$ la aplicación que asocia a cada persona su edad en años.*

   Sea $B = \{18, 19, \cdots, 111\}$. Entonces $f^*(B)$ es el conjunto de todos los españoles cuya edad está comprendida entre 18 y 111 años. Si suponemos que no hay nadie que tenga 112 años o más, entonces $f^*(B)$ es el conjunto de todos los españoles mayores de edad, y por tanto que tienen derecho a voto.

2. *Sea $g : \mathbb{Z} \to \mathbb{N}$ la aplicación dada por $g(x) = x^2$. Sean $A_1 = \{0, 1, 2\}$, $A_2 = \{-3, -1, 0, 3\}$, $B_1 = \{1, 2, 3, 4\}$ y $B_2 = \{3, 5, 7\}$. Entonces:*

   $g_*(A_1) = \{0, 1, 4\}$, pues $g(0) = 0$, $g(1) = 1$ y $g(2) = 4$.

   $g_*(A_2) = \{0, 1, 9\}$, pues $g(0) = 0$, $g(-1) = 1$ y $g(-3) = g(3) = 9$.

   $g^*(B_1) = \{1, -1, 2, -2\}$ pues $g(1) = g(-1) = 1 \in B_1$, $g(2) = g(-2) = 4 \in B_1$, y no hay ningún otro número entero cuya imagen por g pertenezca a B_1.

   $g^*(B_2) = \emptyset$, pues no hay ningún número entero cuyo cuadrado sea 3, 5 ó 7.

Propiedades.
Sean X e Y dos conjuntos, $A_1, A_2 \subseteq X$ y $B_1, B_2 \subseteq Y$ y $f : X \to Y$ una aplicación. Entonces:

1. $f_*(A_1 \cup A_2) = f_*(A_1) \cup f_*(A_2)$.

2. $f_*(A_1 \cap A_2) \subseteq f_*(A_1) \cap f_*(A_2)$.

3. $f^*(B_1 \cup B_2) = f^*(B_1) \cup f^*(B_2)$.

4. $f^*(B_1 \cap B_2) = f^*(B_1) \cap f^*(B_2)$.

5. $f^*(\overline{B_1}) = \overline{f^*(B_1)}$.

6. $A_1 \subseteq f^*(f_*(A_1))$.

7. $f^*(f_*(B_1)) \subseteq B_1$.

Vamos a demostrar, por ejemplo, la número 4. Como es una igualdad lo haremos por doble inclusión.

Sea $x \in f^*(B_1 \cap B_2)$. Entonces $f(x) \in B_1 \cap B_2$, luego $f(x) \in B_1$ y $f(x) \in B_2$. Ahora bien, si $f(x) \in B_1$ entonces $x \in f^*(B_1)$ (pues su imagen está en B_1), y de la misma forma $x \in f^*(B_2)$, luego x pertenece a la intersección de ambos, es decir, $x \in f^*(B_1) \cap f^*(B_2)$.

Recíprocamente, si $x \in f^*(B_1) \cap f^*(B_2)$ entonces $x \in f^*(B_1)$ y $x \in f^*(B_2)$, luego $f(x) \in B_1$ y $f(x) \in B_2$, es decir, $f(x) \in B_1 \cap B_2$ lo que nos dice que $x \in f^*(B_1 \cap B_2)$.

En los casos en que se ha puesto una inclusión es porque la otra inclusión no tiene porqué darse. Así, si consideramos la aplicación del ejemplo anterior, tenemos que

$$A_1 \cap A_2 = \{0\}; \quad f_*(A_1 \cap A_2) = \{0\} \quad \text{mientras que } f_*(A_1) \cap f_*(A_2) = \{0, 1, 9\} \cap \{0, 1, 4\} = \{0, 1\}$$

Aunque vemos en el ejemplo que la inclusión es estricta, no podemos poner como propiedad que $f_*(A_1 \cap A_2) \subsetneq f_*(A_1) \cap f_*(A_2)$, ya que hay casos en los que sí se da la igualdad (toma el mismo ejemplo, pero incluyendo en A_2 el elemento 1).

1.2.3. Composición de aplicaciones.

Supongamos que tenemos una aplicación $f : X \to Y$ y otra aplicación $g : Y \to Z$. Si tomamos un elemento $x \in X$, por la aplicación f le asignamos el elemento $y = f(x)$. Como este elemento pertenece a Y, por la aplicación g se le asigna el elemento $g(y) = g(f(x)) \in Z$. Tenemos entonces una forma de hacerle corresponder a cada elemento de X un elemento de Z, es decir, tenemos una aplicación $X \to Z$. Esta aplicación se conoce como la composición de f y g. Formalmente:

Definición 13. *Sean X, Y, Z conjuntos, y $f : X \to Y$ y $g : Y \to Z$ dos aplicaciones. Se define la aplicación composición de f y g como la aplicación $g \circ f : X \to Z$ dada por $(g \circ f)(x) = g(f(x))$.*

Ejemplo 1.2.5. *Por ejemplo. Sean $f : \mathbb{N} \to \mathbb{N}$ y $g : \mathbb{N} \to \mathbb{N}$ las aplicaciones dadas por $f(n) = n + 1$, y $g(n) = n^2$. Entonces $(g \circ f)(n) = g(f(n)) = g(n+1) = (n+1)^2$, mientras que $(f \circ g)(n) = f(n^2) = n^2 + 1$. Como en general $n^2 + 1 \neq (n + 1)^2$ podemos concluir que $g \circ f \neq f \circ g$.*

Vemos con el ejemplo anterior que la composición de aplicaciones no es conmutativa. De hecho, pudiera ocurrir que $g \circ f$ existiera, pero que $f \circ g$ no estuviera definida. Por ejemplo, si $f : X \to Y$ y $g : Y \to Z$ y $X \neq Z$, entonces la composición $f \circ g$ no tiene sentido.

También puede ocurrir que existiendo ambas, dominio y codominio fueran diferentes. Por ejemplo, tenemos $f : X \to Y$ y $g : Y \to X$. En tal caso, tenemos $g \circ f : X \to X$ y $f \circ g : Y \to Y$. Si $Y \neq X$, el dominio y codominio de $g \circ f$ es distinto del dominio y codominio de $f \circ g$.

Pero aún en el caso de que existan ambas composiciones, y que dominio y codominio coincidieran, las dos composiciones pueden ser diferentes, como hemos visto en el ejemplo precedente.

Propiedades.

Para cualquier aplicación $f : X \to Y$ se verifica que $f \circ Id_X = Id_Y \circ f = f$.

La composición de aplicaciones es asociativa, es decir, si tenemos $f : X \to Y$, $g : Y \to Z$ y $h : Z \to W$ entonces $h \circ (g \circ f) = (h \circ g) \circ f$.

Ejemplo 1.2.6. *Sean $f : \mathbb{N} \to \mathbb{Z}$, $g : \mathbb{Z} \to \mathbb{N}$ y $h : \mathbb{N} \to \mathbb{N}$ las aplicaciones dadas por $f(n) = n^2 - 5$, $g(n) = n^2 + 1$ y $h(n) = n + 1$. Entonces:*

- $(g \circ f)(n) = g(f(n)) = g(n^2 - 5) = (n^2 - 5)^2 + 1 = n^4 - 10n^2 + 25 + 1 = n^4 - 10n^2 + 26$.
- $(h \circ (g \circ f))(n) = h((g \circ f)(n)) = h(n^4 - 10n^2 + 26) = n^4 - 10n^2 + 27$.
- $(h \circ g)(n) = h(n^2 + 1) = n^2 + 2$.
- $((h \circ g) \circ f)(n) = (h \circ g)(f(n)) = (h \circ g)(n^2 - 5) = (n^2 - 5)^2 + 2 = n^4 - 10n^2 + 25 + 2 = n^4 - 10n^2 + 27$.

Dada una aplicación $f : X \to X$, denotaremos como f^2 a la composición $f \circ f$. Más en general, definimos:

$$f^0 = Id_X \qquad f^{n+1} = f^n \circ f$$

Ejemplo 1.2.7. *Si $f : \mathbb{N} \to \mathbb{N}$ es la aplicación dada por $f(n) = 2n + 1$, entonces $f^2(n) = f(f(n)) = f(2n+1) = 2(2n+1) + 1 = 4n + 3$, $f^3(n) = f^2(f(n)) = f^2(2n+1) = 4(2n+1) + 3 = 8n + 7$. En general, puede verse que $f^k(n) = 2^k n + 2^k - 1$.*

1.2.4. Aplicaciones inyectivas, sobreyectivas y biyectivas.

Aplicaciones inyectivas.

Definición 14. *Una aplicación $f : X \to Y$ se dice inyectiva cuando elementos distintos del dominio dan lugar a imágenes distintas. Es decir, dados $x_1, x_2 \in X$, $x_1 \neq x_2 \Longrightarrow f(x_1) \neq f(x_2)$. O lo que es lo mismo, $f(x_1) = f(x_2) \Longrightarrow x_1 = x_2$.*

También podría haberse definido una aplicación inyectiva como aquella aplicación tal que para cada $y \in Y$ el conjunto $f^*(\{y\})$ tiene a lo sumo un elemento.

Ejemplo 1.2.8.

1. *La aplicación $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = 2n$ es inyectiva, pues dos números distintos no pueden tener el mismo doble. Es decir, $n \neq n' \Longrightarrow 2n \neq 2n'$.*

2. *La aplicación $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = n^2$ es inyectiva, mientras que $g : \mathbb{Z} \to \mathbb{Z}$ dada por $g(n) = n^2$ no lo es, pues $g(1) = g(-1)$ (es decir, dos elementos distintos tienen la misma imagen). Notemos que en este caso se tiene que $g^*(\{1\})$ tiene dos elementos, pues $g^*(\{1\}) = \{-1, 1\}$.*

3. *Sea B el conjunto de todos los estudiantes matriculados en la asignatura ALEM de 1ºD del grado en Ingeniería Informática en la Universidad de Granada, y D el conjunto de los 366 días del año. Sea $n : B \to D$ la aplicación que a cada estudiante le hace corresponder el día que nació.*

   Apostaría 20 euros a que la aplicación n no es inyectiva, es decir, hay dos estudiantes que han nacido el mismo día (aunque posiblemente de distinto año).

Propiedades.

Para cualquier conjunto X, la aplicación Id_X es inyectiva.

La composición de aplicaciones inyectivas es inyectiva.

Si $g \circ f$ es inyectiva, entonces podemos asegurar que f lo es, pero g podría serlo o no.

Ejemplo 1.2.9. *Sean $X = \{1, 2, 3\}$, $Y = \{a, b, c, d\}$ y $Z = \{0, 2, 4, 6, 8\}$. Consideramos las aplicaciones $f : X \to Y$ dada por $f(1) = a$, $f(2) = c$ y $f(3) = d$ y $g : Y \to Z$ dada por $g(a) = 0$, $g(b) = 4$, $g(c) = 4$, $g(d) = 8$. Entonces $g \circ f$ es inyectiva (la imagen de 1 es 0, la imagen de 2 es 4 y la imagen de 3 es 8), mientras que g no lo es, ya que $g(b) = g(c)$.*

Aplicaciones sobreyectivas.

Definición 15. *Sea $f : X \to Y$. Se dice que f es sobreyectiva si para cualquier $y \in Y$ existe $x \in X$ tal que $f(x) = y$ (es decir, para cualquier $y \in Y$ el conjunto $f^*(\{y\})$ tiene al menos un elementos - es distinto del conjunto vacío -).*

Ejemplo 1.2.10.

1. *La aplicación $f : \mathbb{Z} \to \mathbb{N}$ dada por $f(x) = |x|$ es sobreyectiva, pues para cualquier número natural n hay un número entero (el propio n, o $-n$) cuyo valor absoluto es n. Esta aplicación no es inyectiva, pues $f(2) = f(-2)$.*

2. *La aplicación $f : \mathbb{Z} \to \mathbb{Z}$ $x \mapsto x+1$ es sobreyectiva, pues dado un número entero y, hay otro número entero $x = y - 1$ tal que $f(x) = y$.*

   Sin embargo, la aplicación $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = n+1$ no es sobreyectiva, pues no hay ningún número natural que al sumarle 1 nos de 0 ($f^*(\{0\} = \emptyset$).

3. *La aplicación $n : B \to D$ definida en el ejemplo 1.2.8 no es sobreyectiva, pues al ser el número de estudiantes de primero B menor de 366, tiene que haber días del año en que no haya nacido ninguno de estos estudiantes.*

Propiedades.
Para cualquier conjunto X, la aplicación Id_X es sobreyectiva.
La composición de aplicaciones sobreyectivas es sobreyectiva.
Si $f : X \to Y$, $g : Y \to Z$ son aplicaciones tales que $g \circ f$ es sobreyectiva, entonces también lo es g, pues dado $z \in Z$ sabemos que existe $x \in X$ tal que $g(f(x)) = z$. Basta tomar $y = f(x)$ y se tiene que $g(y) = z$.

Ejemplo 1.2.11. *Tomamos, por ejemplo, $f : \mathbb{N} \to \mathbb{N}$ la aplicación $n \mapsto 2n$, y $g : \mathbb{N} \to \mathbb{N}$ la aplicación $n \mapsto E(n/2)$ (donde $E(x)$ denota la parte entera de x). Entonces $(g \circ f)(n) = g(f(n)) = g(2n) = E(2n/2) = E(n) = n$, luego $g \circ f = Id_{\mathbb{N}}$ que es sobreyectiva. Es claro que f no lo es.*

Aplicaciones biyectivas. Aplicación inversa.

Definición 16. *Una aplicación $f : X \to Y$ se dice que es biyectiva si es inyectiva y sobreyectiva. O lo que es lo mismo, para cada $y \in Y$, el conjunto $f^*(\{y\})$ tiene exactamente un elemento.*

Ejemplo 1.2.12. *La aplicación $f : \mathbb{Z} \to \mathbb{Z}$ dada por $f(x) = x+2$ es biyectiva, mientras que la aplicación $f : \mathbb{N} \to \mathbb{N}$ $n \mapsto n+2$ no lo es, pues no es sobreyectiva.*

La aplicación $f : \mathbb{Q} \to \mathbb{Q}$ definida como $f(x) = 2x$ es biyectiva. La misma expresión, pero tomando como dominio y codominio $\mathbb{Z}$ define una aplicación que no es biyectiva (pues no es sobreyectiva).

Propiedades.
Para cualquier conjunto X la aplicación Id_X es biyectiva.
La composición de aplicaciones biyectivas es una aplicación biyectiva.
Si $f : X \to Y$ y $g : Y \to Z$ son aplicaciones tales que $g \circ f$ es biyectiva, lo más que podemos asegurar es que f es inyectiva y que g es sobreyectiva.

Definición 17. *Sea $f : X \to Y$ una aplicación. Se dice que f tiene inversa si existe $g : Y \to X$ tal que $g \circ f = Id_X$ y $f \circ g = Id_Y$.*

Ejemplo 1.2.13. *La aplicación $f : \mathbb{Z} \to \mathbb{Z}$ $x \mapsto x + 2$ tiene como inversa la aplicación $g : \mathbb{Z} \to \mathbb{Z}$ $x \mapsto x - 2$.*

Para cualquier conjunto X la aplicación $Id_X : X \to X$ tiene como inversa a ella misma.

Propiedad.

Dada una aplicación $f : X \to Y$ se tiene que f tiene inversa si, y sólo si, f es biyectiva.

Vamos a demostrarlo. Supongamos que f tiene inversa. Sea $g : Y \to X$ una inversa. Entonces $f \circ g = Id_Y$, luego $f \circ g$ es sobreyectiva. Vimos antes que en ese caso f es sobreyectiva. También $g \circ f = Id_X$, luego $g \circ f$ es inyectiva, lo que implica que f es inyectiva. Por tanto, f es inyectiva y sobreyectiva.

Recíprocamente, supongamos ahora que f es biyectiva. Vamos a definir $g : Y \to X$. Para esto, sea $y \in Y$. Por ser f sobreyectiva, $f^*(\{y\})$ es distinto del vacío, y por ser f inyectiva, $f^*(\{y\})$ tiene a lo sumo un elemento, luego $f^*(\{y\})$ tiene exactamente un elemento. Definimos $g(y)$ como el único elemento que pertenece a $f^*(\{y\})$.

Es fácil comprobar que g, así definida, es una inversa para f.

Ejemplo 1.2.14. *Consideramos $f : \mathbb{N} \to \mathbb{N}$ la aplicación definida como $f(n) = 2n$. Esta aplicación es inyectiva, pero no sobreyectiva (pues el 1 no pertenece a la imagen de f). Vimos que si tomamos la aplicación $g : \mathbb{N} \to \mathbb{N}$ $n \mapsto E(n/2)$ se tiene que $g \circ f = Id_{\mathbb{N}}$.*

Esta aplicación no es una inversa para f, aunque $g \circ f = Id_{\mathbb{N}}$, ya que $f \circ g \neq Id_{\mathbb{N}}$ (por ejemplo, $(f \circ g)(3) = f(g(3)) = f(1) = 2$).

La aplicación g se dice que es una inversa por la izquierda *de f. De la misma forma se dice que la aplicación f es una* inversa por la derecha *de g.*

Puede demostrarse que una aplicación f es inyectiva si, y sólo si, tiene inversas por la izquierda, y es sobreyectiva si, y sólo si, tiene inversas por la derecha.

Una aplicación $f : X \to Y$ puede tener varias inversas por la izquierda o varias inversas por la derecha. Pero si tiene inversa por la izquierda y por la derecha, entonces ambas deben coincidir, pues si $g : Y \to X$ es una inversa por la derecha y $h : Y \to X$ es una inversa por la izquierda, se tiene que $g = Id_X \circ g = (h \circ f) \circ g = h \circ (f \circ g) = h \circ Id_Y = h$. De aquí deducimos que si una aplicación tiene inversa, entonces sólo puede tener una. A esta aplicación la denotaremos como f^{-1}.

Ejemplo 1.2.15. *Sean $X = \{1, 2\}$ e $Y = \{a, b, c\}$, y $f : X \to Y$ la aplicación dada por $f(1) = b$, $f(2) = a$. Entonces f es inyectiva, y por lo dicho antes tiene inversa por la izquierda. En este caso tiene 2 inversas por la izquierda, que son:*

$$\begin{array}{c} Y \xrightarrow{g_1} X \\ a \mapsto 2 \\ b \mapsto 1 \\ c \mapsto 1 \end{array} \qquad \begin{array}{c} Y \xrightarrow{g_2} X \\ a \mapsto 2 \\ b \mapsto 1 \\ c \mapsto 2 \end{array}$$

La aplicación g_1 es sobreyectiva. Por tanto tiene inversa por la derecha. Una de ellas es f, pero tiene otra, que es la dada por $1 \mapsto c$, $2 \mapsto a$.

También g_2 tiene dos inversas por la derecha. Aparte de f, la dada por $1 \mapsto b$, $2 \mapsto c$.

La aplicación $f : \mathbb{N} \to \mathbb{N}$ definida como $f(n) = 2n$ tiene infinitas inversas por la izquierda (y por tanto no puede tener inversa por la derecha).

Supongamos que $f : X \to Y$ y $g : Y \to Z$ son dos aplicaciones biyectivas. Sabemos entonces que tanto f como g tienen inversa. Sabemos también que la composición $g \circ f$ es biyectiva, luego tiene inversa. En tal caso se tiene que $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Ejemplo 1.2.16. *Sea $f : \mathbb{Q} \to \mathbb{Q}$ la aplicación $f(x) = x - 2$, y $g : \mathbb{Q} \to \mathbb{Q}$ la aplicación dada por $g(x) = 3x$. Tanto f como g son biyectivas, y sus inversas vienen dadas por $f^{-1}(x) = x + 2$ y $g^{-1}(x) = \frac{x}{3}$.*

Si realizamos la composición $g \circ f$ nos queda que $(g \circ f)(x) = g(x - 2) = 3x - 6$. Esta aplicación es biyectiva, y su inversa es la aplicación $x \mapsto \frac{x+6}{3}$.

Por otra parte, se tiene que
$(f^{-1} \circ g^{-1})(x) = f^{-1}(g^{-1}(x)) = f^{-1}(\frac{x}{3}) = \frac{x}{3} + 2 = \frac{x+6}{3}$
es decir, $f^{-1} \circ g^{-1}$ es la aplicación inversa de $g \circ f$.

Si realizamos la composición en el otro sentido, nos queda
$(g^{-1} \circ f^{-1})(x) = g^{-1}(x + 2) = \frac{x+2}{3}$
que no es la inversa de $g \circ f$.

Dado un conjunto X, definimos la aplicación $f : \mathcal{P}(X) \to \mathcal{P}(X)$ como $f(A) = \overline{A}$. En ese caso, se tiene que $(f \circ f)(A) = f(f(A)) = f(\overline{A}) = \overline{\overline{A}} = A$. Por tanto, $f \circ f = Id_{\mathcal{P}(X)}$, y por tanto f es una biyección cuya inversa es ella misma.

Si X es un conjunto y A un subconjunto de X, definimos la aplicación $f_A : \mathcal{P}(X) \to \mathcal{P}(X)$ como $f_A(B) = A\Delta B$. Entonces f es una biyección. Como ejercicio, encuentra su inversa.

1.2.5. Cardinales.

Sea $f : X \to Y$ una aplicación inyectiva. Eso significa que dos elementos distintos de X dan lugar (por la aplicación f) a dos elementos distintos de Y. Por tanto, el conjunto Y debe tener más elementos (o quizá los mismos) que X.

De la misma forma, si $f : X \to Y$ es una aplicación sobreyectiva, entonces el número de elementos de X debe ser mayor o igual que el número de elementos de Y, pues por cada elemento $y \in Y$ tenemos uno o más elementos de X (los que pertenecen a $f^*(\{y\})$).

Por tanto, si $f : X \to Y$ es una aplicación biyectiva, el número de elementos de X debe ser igual al número de elementos de Y.

Sea n un número natural. Vamos a llamar $\mathbf{n}$ al conjunto $\mathbf{n} = \{0, 1, 2, \cdots, n-1\}$ (el conjunto $\mathbf{0}$ es el conjunto vacío). El número de elementos de $\mathbf{n}$ es n.

Definición 18. *Sea X un conjunto. Diremos que X tiene cardinal n (es decir, que X tiene n elementos) si existe una biyección $\mathbf{n} \to X$. En tal caso escribiremos $|X| = n$.*

Notemos que cuando damos una biyección $\mathbf{n} \to X$ lo que estamos haciendo es contar los elementos de X (empezando por cero) tal y como nosotros hemos contado siempre los elementos de un conjunto.

Esta definición es coherente, en el sentido que si tuviéramos dos biyecciones $\mathbf{m} \to X$ y $\mathbf{n} \to X$ entonces $m = n$ (es decir, a la hora de contar los elementos de un conjunto da igual por cual empecemos y el orden en que los contemos. Siempre llegaremos al mismo resultado).

La afirmación anterior, aunque intuitivamente muy clara tiene una demostración un poco complicada.

Cardinal de la unión de conjuntos.

Si A y B son dos conjuntos disjuntos, entonces $|A \cup B| = |A| + |B|$.

La idea está clara. Al contar los elementos de $A \cup B$, y no haber ninguno en común, sale exactamente la suma del número de elementos de A y el número de elementos de B.

Si m es el cardinal de A y n el cardinal de B, cuando contamos los elementos de la unión, primero contamos los de A (y llegamos hasta $m-1$), y a continuación contamos los de B (pero siguiendo por m). LLegaremos entonces hasta $m+n-1$. Luego $|A \cup B| = m + n = |A| + |B|$.

Más formalmente, si $f : \mathbf{m} \to A$ y $g : \mathbf{n} \to B$ son dos biyecciones. Entonces la aplicación $h : \mathbf{m} + \mathbf{n} \to A \cup B$

$$h(x) = \begin{cases} f(x) & \text{si } x < m \\ g(x-m) & \text{si } x \geq m \end{cases}$$

es una biyección.

Vamos ahora a calcular cuando vale $|A \cup B|$ sin que necesariamente $A \cap B$ sea igual al conjunto vacío. Intuitivamente, si sumamos el cardinal de A y el cardinal de B, los elementos de $A \cap B$ los estamos contando dos veces, luego habrá que restarlos una vez para haber contado todos los elementos de $A \cup B$ exactamente una vez. Por tanto, $|A \cup B| = |A| + |B| - |A \cap B|$.

Una demostración de esto podría ser como sigue. En primer lugar, se tiene que es fácil comprobar que $A = (A \setminus B) \cup (A \cap B)$, y que $(A \setminus B) \cap (A \cap B) = \emptyset$. Por tanto, $|A| = |A \setminus B| + |A \cap B|$, luego $|A \setminus B| = |A| - |A \cap B|$. De la misma forma, $|B \setminus A| = |B| - |A \cap B|$.

Puesto que $A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B)$ y la intersección de dos cualesquiera de estos conjuntos es el conjunto vacío se tiene que

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

Cardinal del producto cartesiano.

En cuanto al producto cartesiano, se tiene que $|A \times B| = |A| \cdot |B|$. Si $A = \{a_1, \cdots, a_m\}$ y $B = \{b_1, \cdots, b_n\}$, por cada elemento $a_i \in A$ tenemos n elementos $(a_i, b_1), \cdots, (a_i, b_n)$ de $A \times B$. Por tanto, el cardinal del producto cartesiano debe ser el producto de cada uno de los factores, es decir:

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

Para comprobarlo, vamos a ver que existe una biyección $f : \mathbf{m} \times \mathbf{n} \to \mathbf{p}$, donde $p = m \cdot n$.
Esta biyección viene dada por $f(x, y) = x + m \cdot y$.

$$
\begin{array}{llcl}
f(0,0) = 0 & f(1,0) = 1 & & f(m-1,0) = m-1 \\
f(0,1) = m & f(1,1) = m+1 & \cdots\cdots\cdots & f(m-1,1) = 2m-1 \\
\cdots\cdots\cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots\cdots\cdots\cdots & & \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
f(0,n-1) = mn-m & f(1,n-1) = mn-m+1 & & f(m-1,n-1) = mn-1
\end{array}
$$

La inversa de f sería la aplicación $g : \mathbf{p} \to \mathbf{m} \times \mathbf{n}$ $z \mapsto (z \bmod m, z \operatorname{div} m)$

Cardinal de un conjunto de aplicaciones.

Por último vamos a calcular el número de aplicaciones de X en Y en función del número de elementos de X y de Y. Supongamos que $X = \{a_1, \cdots, a_m\}$ e $Y = \{b_1, \cdots, b_n\}$. Entonces, para dar una aplicación $X \to Y$ debemos elegir el valor de $f(a_1)$, para lo cual tenemos n posibilidades; el valor de $f(a_2)$, para lo cual tenemos otras n posibilidades, y así hasta $f(a_m)$, para lo cual volvemos a tener n posibilidades. En total, podemos hacer un total de $n \cdot n \cdots n = n^m$ posibles aplicaciones.

> Una forma de demostrar esto, sería dar una biyección entre el conjunto $Z = \{\alpha : \mathbf{m} \to \mathbf{n} | \alpha \text{ es aplicación}\}$ y el conjunto $\mathbf{p}$, donde $p = n^m$. Esta biyección podría ser:
>
> $$h(\alpha) = \alpha(0) + \alpha(1) \cdot n + \cdots + \alpha(m-1) \cdot n^{m-1}$$
>
> La inversa vendría dada como sigue: para un elemento x tal que $0 \leq x < p$, calculamos su expresión en base n, y nos quedaría $x = (a_{m-1} \cdots a_1 a_0)_n$ (donde a_{m-1} podría valer 0). Al elemento x le haríamos corresponder la aplicación $\alpha : \mathbf{m} \to \mathbf{n}$ dada por $\alpha(i) = a_i$.

En base a esto, es usual, dado dos conjuntos X e Y, denotar como Y^X al conjunto de todas las aplicaciones $f : X \to Y$.

Cardinal del conjunto potencia.

Finalmente, vamos a calcular el cardinal del conjunto $\mathcal{P}(X)$ en función del cardinal de X.

Sea X un conjunto de cardinal n. Supongamos que $X = \{a_1, a_2, \cdots, a_n\}$. Para cada subconjunto $A \subseteq X$ definimos la aplicación característica $\chi_A : X \to \{0, 1\}$ como:

$$\chi_A(a_i) = \begin{cases} 1 & \text{si } a_i \in A \\ 0 & \text{si } a_i \notin A \end{cases}$$

Por ejemplo, $\chi_\emptyset$ es la aplicación constante 0, mientras que χ_X es la aplicación constante 1. Se tiene que $A \subseteq B$ si, y sólo si, para cualquier $a \in X$, $\chi_A(a) \leq \chi_B(a)$.

De esta forma, hemos definido una aplicación

$$\begin{array}{ccc} \mathcal{P}(X) & \longrightarrow & \{0,1\}^X \\ A & \mapsto & \chi_A \end{array}$$

que es biyectiva. Es inyectiva pues dos subconjuntos de X diferentes dan lugar a aplicaciones características diferentes, y es sobreyectiva pues cualquier aplicación $X \to \{0, 1\}$ es la aplicación característica de algún subconjunto de X (basta tomar la imagen inversa de $\{1\}$).

Por tanto, ambos conjuntos tienen igual cardinal. Como el cardinal del segundo conjunto es $2^{|X|}$ deducimos que $|\mathcal{P}(X)| = 2^{|X|}$.

Por ejemplo, vamos a tomar $X = \{a, b, c\}$. Vamos a escribir todas las aplicaciones $X \to \{0, 1\}$, y el subconjunto de X con el que se corresponden:

$$
\begin{array}{cccccccc}
a \mapsto 0 & a \mapsto 0 & a \mapsto 0 & a \mapsto 0 & a \mapsto 1 & a \mapsto 1 & a \mapsto 1 & a \mapsto 1 \\
b \mapsto 0 & b \mapsto 0 & b \mapsto 1 & b \mapsto 1 & b \mapsto 0 & b \mapsto 0 & b \mapsto 1 & b \mapsto 1 \\
c \mapsto 0 & c \mapsto 1 & c \mapsto 0 & c \mapsto 1 & c \mapsto 0 & c \mapsto 1 & c \mapsto 0 & c \mapsto 1 \\
\\
A = \emptyset & A = \{c\} & A = \{b\} & A = \{b,c\} & A = \{a\} & A = \{a,c\} & A = \{a,b\} & A = \{a,b,c\}
\end{array}
$$

1.3. Relaciones

Definición 19. *Sea X un conjunto. Una relación en X es un subconjunto de $X \times X$.*

Si R es una relación en X, y $(x, y) \in R$, escribiremos normalmente xRy, y diremos x está relacionado con y *(con la relación R).*

Si el elemento (x, y) no pertenece a R, escribiremos $x \not R y$.

Para dar una relación en un conjunto X, podemos, bien enumerar las parejas de elementos que están relacionados, bien dar las condiciones que deben cumplir dos elementos para estar relacionados.

Ejemplo 1.3.1.

1. *Sea $X = \{0, 1, 2, 3, 4\}$, y la relación $R = \{(0, 0),\ (0, 2),\ (0, 4),\ (2, 1),\ (2, 3),\ (4, 0),\ (4, 2),\ (4, 4)\}$. Entonces $0R0$, $2R1$, $1 \not R 2$, $3 \not R 2$, $4R2$, $4 \not R 3$.*

   En este caso que 0 está relacionado con 0, 2 está relacionado con 1, pero 1 no está relacionado con 2.

   También podríamos haber definido R como xRy si $x + 2y$ es múltiplo de 4.

   De la primera forma hemos enumerado todas las parejas que están relacionadas, mientras que en la segunda hemos dicho la condición que deben cumplir dos elementos para estar relacionados.

2. *En el mismo conjunto X, definimos la relación R' como $xR'y$ si $x \leq y$. O si queremos,*

$$R' = \{(0, 0),\ (0, 1),\ (0, 2),\ (0, 3),\ (0, 4),\ (1, 1),\ (1, 2),\ (1, 3),\ (1, 4),\ (2, 2),\ (2, 3),\ (2, 4),\ (3, 3),\ (3, 4),\ (4, 4)\}$$

Definición 20. *Si X es un conjunto, definimos la relación Δ como $\Delta = \{(x, x) : x \in X\}$. O si preferimos: $x\Delta y$ si, y sólo si, $x = y$.*

Si X es un conjunto y R una relación en X, definimos la relación inversa R^{-1} como $xR^{-1}y$ si yRx.

Si X es un conjunto, y R y S dos relaciones en X, definimos la relación $R \circ S$ como $x(R \circ S)Y$ si existe z tal que xRz y zRy.

Ejemplo 1.3.2.

1. *Si R es la relación del ejemplo anterior, entonces*

   $R^{-1} = \{(0, 0),\ (2, 0),\ (4{,}0),\ (1, 2),\ (3, 2),\ (0, 4),\ (2, 4),\ (4, 4)\}$

   $R \circ R = \{(0, 0),\ (0, 1),\ (0, 3),\ (0, 2),\ (0, 4),\ (4, 0),\ (4, 1),\ (4, 2),\ (4, 3),\ (4, 4)\}$.

   Por ejemplo, $0(R \circ R)2$ pues $0R0$ y $0R2$ (hemos tomado $z = 0$). $4(R \circ R)1$ ya que $4R2$ y $2R1$ (aquí hemos tomado $z = 2$).

2. *En el caso de la relación R', se tiene que*

$$(R')^{-1} = \{(0, 0),\ (1, 0),\ (2, 0),\ (3, 0),\ (4, 0),\ (1, 1),\ (2, 1),\ (3, 1),\ (4, 1),\ (2, 2),\ (3, 2),\ (4, 2),\ (3, 3),\ (4, 3),\ (4, 4)\}$$

   Mientras que $R \circ R = R$.

Definición 21. *Sea X un conjunto y R una relación en X. Para cada $x \in X$ definimos la clase de x como*

$[x] = \{y \in X : xRy\}$.

Ejemplo 1.3.3.

1. *Para la relación R del ejemplo anterior tenemos que*

   - $[0] = [4] = \{0, 2, 4\}$.
   - $[1] = [3] = \emptyset$.

- $[2] = \{1, 3\}$.

2. *Para la relación R', se tiene:*

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

3. *Si X es un conjunto, y consideramos la relación Δ, entonces, para cada $x \in X$, $[x] = \{x\}$.*

Definición 22. *Sea X un conjunto. Una relación R sobre X se dice:*

- Reflexiva: *si para cualquier $x \in X$ se tiene que xRx (o equivalentemente, $\Delta \subseteq R$).*
- Simétrica: *si siempre que xRy se tiene que yRx (es decir, $R \subseteq R^{-1}$)*
- Antisimétrica: *si xRy e yRx implica que $x = y$ (es decir, $R \cap R^{-1} \subseteq \Delta$).*
- Transitiva: *si xRy e yRz implica que xRz (es decir, $R \circ R \subseteq R$).*

Ejemplo 1.3.4.

1. *La relación R del ejemplo anterior no es reflexiva, pues $1 \not R 1$ ($(1, 1) \in \Delta$ pero $(1, 1) \notin R$).*
   No es simétrica, pues $1R2$ pero $2 \not R 1$ ($(1, 2) \in R$ pero $(1, 2) \notin R^{-1}$)
   No es antisimétrica, pues $0R4$ y $4R0$ y sin embargo, $0 \neq 4$ ($(0, 4) \in R \cap R^{-1}$ y $(0, 4) \notin \Delta$).
   No es transitiva, pues $0R2$, $2R3$ y sin embargo, $0 \not R 3$ ($(0, 3) \in R \circ R$ pero $(0, 3) \notin R$).

2. *Para cualquier conjunto X, la relación Δ es una relación reflexiva, simétrica, antisimétrica y transitiva.*

3. *En $\mathbb{N}$, la relación xRy si $x + y$ es par es:*
   - Reflexiva, pues para cualquier x, $x + x = 2x$ es par.
   - Simétrica, pues si $x + y$ es par también lo es $y + x$.
   - Transitiva, pues si $x + y$ es par e $y + z$ es par, entonces $x + z = (x + y) + (y + z) - 2y$, que es par.
   No es antisimétrica, pues $2R4$ y $4R2$.
   Podemos ver que $[0] = \{0, 2, 4, 6, \cdots\} = 2\mathbb{N}$, y esta clase es igual a la de cualquier número par, y si x es un número impar, entonces $[x] = \{1, 3, 5, 7, \cdots\}$.

4. *En $\mathbb{N}$ la relación xRy si $x < y$ es transitiva y antisimétrica, pero no es ni reflexiva, ni simétrica.*
   Para cualquier número natural x, la clase de x está formada por todos los números mayores que x.

5. *Si X es un conjunto, la relación en $\mathcal{P}(X)$ definida como ARB si $A \subseteq B$ es reflexiva, antisimétrica y transitiva.*

Propiedad.
Una relación que sea simétrica y transitiva es reflexiva, pues si xRy, por ser simétrica se tiene que yRx, y al ser transitiva deducimos que xRx.

Ejemplo 1.3.5. *En $\mathbb{N}$ definimos la relación mRn si $m \cdot n \neq 0$. Esta relación es simétrica (pues si $m \cdot n \neq 0$ entonces $n \cdot m \neq 0$) y es transitiva (ya que si $m \cdot n \neq 0$ y $n \cdot p \neq 0$ entonces $m \neq 0$ y $p \neq 0$, luego $m \cdot p \neq 0$. Sin embargo no es reflexiva.*
Cuestión: *Este ejemplo no es coherente con lo que acabamos de decir. ¿Qué falla?.*

Vamos a estudiar con un poco más de detalle dos tipos de relaciones: las relaciones de equivalencia y las relaciones de orden.

1.3.1. Relaciones de equivalencia.

Una relación de equivalencia viene a ser una generalización del concepto de igualdad.

Definición 23. *Sea X un conjunto. Una relación de equivalencia en X es una relación reflexiva, simétrica y transitiva.*

Ejemplo 1.3.6.

- *Para cualquier conjunto X, la relación de igualdad (xRy si $x = y$) es una relación de equivalencia.*
- *La relación xRy si $x + y$ es par definida en $\mathbb{N}$ es una relación de equivalencia.*
- *Sea m un número natural. Definimos en $\mathbb{Z}$ la relación $\equiv_m$ como:*

  $$x \equiv_m y \text{ si } m|(y - x)$$

  Es decir, x está relacionado con y si $(y - x)$ es múltiplo de m.

  Esta relación es de equivalencia, pues es:

  Reflexiva. Ya que para cualquier $x \in \mathbb{Z}$ se tiene que $x \equiv_m x$, ya que $x - x = 0$ que es múltiplo de m (sea quien sea m).

  Simétrica. Pues si $x \equiv_m y$ significa que $(y - x)$ es múltiplo de m, luego, luego $(x - y)$ es también múltiplo de m, ya que $(x - y) = -(y - x)$.

  Transitiva. Si $x \equiv_m y$ e $y \equiv_m z$ significa que tanto $y - x$ como $z - y$ son múltiplos de m, luego también lo es $(y - x) + (z - y) = z - x$. Es decir, $x \equiv_m z$.

  Esta es la relación de congruencia módulo m.

- *Si $f : X \to Y$ es una aplicación, definimos en X la relación R_f como sigue: xR_fy si $f(x) = f(y)$. Esta relación es una relación de equivalencia.*
- *En $\mathbb{R}^2$ se define la relación $(x, y)R(x', y')$ si $|x| + |y| = |x'| + |y'|$.*

  Esta relación es de equivalencia.

- *Sea $X = \{1, 2, 3, 4, 5\}$. La relación*

  $$R = \{(1, 1),\ (1, 2),\ (2, 1),\ (2, 2),\ (3, 3),\ (3, 4),\ (3, 5),\ (4, 3),\ (4, 4),\ (4, 5),\ (5, 3),\ (5, 4),\ (5, 5)\}$$

  es de equivalencia.

Si X es un conjunto y R una relación de equivalencia en X, a la clase de un elemento $x \in X$ la llamaremos *clase de equivalencia* del elemento x.

Una relación de equivalencia en un conjunto X clasifica a los elementos del conjunto X. Esta clasificación viene dada por las clases de equivalencia.

Ejemplo 1.3.7.

1. *Para cualquier relación de equivalencia en un conjunto X, la clase de equivalencia de un elemento es distinta del vacío (pues el propio elemento pertenece a su clase, al ser la relación reflexiva).*
2. *Consideramos la relación de igualdad en un conjunto X, que vimos que es de equivalencia. Entonces, para cualquier $x \in X$ se tiene que $[x] = \{x\}$.*
3. *Vamos a calcular las clases de equivalencia para la relación de congruencia módulo m. Vamos a escribir $[a]_m$ para denotar la clase de equivalencia de a bajo la relación $\equiv_m$. Empezamos para $m = 2$. Tenemos que*

   $$0 \equiv_2 x \Longleftrightarrow 2|(x - 0) \Longleftrightarrow 2|x \Longleftrightarrow x \text{ es par}$$

Por tanto, $[0]_2 = \{x \in \mathbb{Z} : 0 \equiv_2 x\} = \{\cdots, -4, -2, 0, 2, 4, 6, \cdots\}$.

De la misma forma se comprueba que $[1]_2 = \{x \in \mathbb{Z} : 1 \equiv_2 x\} = \{\cdots, -5, -3, -1, 1, 3, 5, \cdots\}$.

Podemos ver que si $x \in \mathbb{Z}$ *y* x *es par, entonces* $[x]_2 = [0]_2$*, mientras que si* x *es impar entonces* $[x]_2 = [1]_2$.

Si ahora lo hacemos para $m = 3$ *tenemos que*

$$0 \equiv_3 x \Longleftrightarrow 3|(x-0) \Longleftrightarrow x = 3k \text{ para algún } k \in \mathbb{Z}$$

Luego $[0]_3 = \{\cdots, -6, -3, 0, 3, 6, \cdots\}$.

De la misma forma se comprueba que $[1]_3 = \{\cdots, -8, -5, -2, 1, 4, 7, \cdots\}$

y que $[2]_3 = \{\cdots, -7, -4, -1, 2, 5, 8, \cdots\}$.

Para cualquier $n \in \mathbb{Z}$*, su clase de equivalencia coincide con alguna de estas tres.*

En general, se tiene que

$[0]_m = \{\cdots, -3m, -2m, -m, 0, m, 2m, \cdots\} = \{n \in \mathbb{Z} | n \text{ mód } m = 0\}$[2]

$[1]_m = \{\cdots, -3m+1, -2m+1, -m+1, 1, m+1, 2m+1, \cdots\} = \{n \in \mathbb{Z} | n \text{ mód } m = 1\}$

$[2]_m = \{\cdots, -3m+2, -2m+2, -m+2, 2, m+2, 2m+2, \cdots\} = \{n \in \mathbb{Z} | n \text{ mód } m = 2\}$

$[m-1]_m = \{\cdots, -2m-1, -m-1, -1, m-1, 2m-1, 3m-1, \cdots\} = \{n \in \mathbb{Z} | n \text{ mód } m = m-1\}$

$[n]_m = [n \text{ mód } m]_m$.

4. *Si* $X = \{1, 2, 3, 4, 5\}$ *y* R *la relación dada en el ejemplo 1.3.6 entonces se tiene que*

   $[1] = [2] = \{1, 2\}$ *y* $[3] = [4] = [5] = \{3, 4, 5\}$.

   Podemos considerar la aplicación $f : X \to X$ *dada por* $1 \mapsto 1$, $2 \mapsto 1$, $3 \mapsto 3$, $4 \mapsto 3$, $5 \mapsto 3$. *Entonces* $R = R_f$.

5. *Para la relación* R *definida en* $\mathbb{R}^2$ *como* $(x, y)R(x', y')$ *si* $|x| + |y| = |x'| + |y'|$*, la clase de equivalencia de un elemento* $(x, y) \in \mathbb{R}^2$ *es un cuadrado que tiene los vértices en los ejes coordenados, concretamente en los puntos* $(z, 0)$*,* $(0, z)$*,* $(-z, 0)$*,* $(0, -z)$*, donde* $z = |x| + |y|$.

Vemos en estos ejemplos que si tenemos un conjunto X y una relación de equivalencia en X, dados dos elementos de X, o sus clases de equivalencia no tienen ningún elemento en común, o los tienen todos (es decir, o son disjuntas o son iguales).

Proposición 1.3.1. *Sea* X *un conjunto, y* R *una relación de equivalencia en* X*. Sean* $x, y \in X$*. Entonces:*

1. *Si* xRy *se tiene que* $[x] = [y]$.
2. *Si* $x \not R y$ *entonces* $[x] \cap [y] = \emptyset$.

Demostración:

Para demostrarlo, vamos a ver, en primer lugar, que ocurre si xRy.

Sea $z \in [x]$. Entonces xRz. Puesto que xRy y R es simétrica tenemos que yRx. Y al ser R transitiva, podemos deducir que yRz, es decir $z \in [y]$. Por tanto hemos probado que $[x] \subseteq [y]$.

De la misma forma se prueba que $[y] \subseteq [x]$.

En el caso de que $x \not R y$, si hubiera un elemento $z \in [x] \cap [y]$ tendríamos xRz e yRz, luego zRy y por tanto xRy lo cual es imposible. Por tanto, ese elemento no existe y la intersección es vacía. ■

Definición 24. *Sea* X *un conjunto, y* R *una relación de equivalencia. Definimos el conjunto cociente* X/R *como el conjunto formado por las clases de equivalencia, es decir:*

$$X/R = \{[x] : x \in X\}$$

[2]Si m, n son dos números enteros, con $m > 0$, entonces podemos encontrar c y r tales que $n = m \cdot c + r$ y $0 \leq r < m$. El número r es lo que llamaremos n mód m. En el caso de que n sea positivo no es más que el resto de la división de n entre m. En el capítulo dedicado a los números enteros, veremos esto con más detalle.

Ejemplo 1.3.8.

- *Vamos a llamar* $\mathbb{Z}_m$ *al conjunto* $\mathbb{Z}/\equiv_m$. *Entonces:*

  $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$. *Tiene exactamente 2 elementos.*

  $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$. *Tiene exactamente 3 elementos.*

  $\mathbb{Z}_m = \{[0]_m, [1]_m, \cdots [m-1]_m\}$. *Tiene exactamente m elementos.*

  Puesto que $[0]_3 = [-12]_3$, $[1]_3 = [25]_3$ *y* $[2]_3 = [50]_3$, *podemos escribir que* $\mathbb{Z}_3 = \{[-12]_3, [25]_3, [50]_3\}$.

  En general, para abreviar la notación escribiremos a en lugar de $[a]_m$. *El contexto nos aclarará si estamos considerando a como un número entero o como un elemento de* $\mathbb{Z}_m$. *Con esta notación tenemos que* $\mathbb{Z}_m = \{0, 1, 2, \cdots, m-1\}$.

- *En la relación definida sobre el conjunto* $X = \{1, 2, 3, 4, 5\}$ *que hemos visto en los ejemplos anteriores, se tiene que el conjunto cociente tiene cardinal 2. Sus dos elementos son* $[1]$ *y* $[3]$.

- *Definimos en* $X = \{0, 1, 2, 3, 4\}$ *la relación*

  $$R = \{(0,0),\ (3,0),\ (4,0),\ (1,1),\ (3,1),\ (0,2),\ (3,2),\ (4,2),\ (0,4),\ (1,4),\ (4,4)\}$$

  Esta relación no es de equivalencia. No es reflexiva pues $(3,3) \notin R$, *no es simétrica pues* $(3,0) \in R$ *pero* $(0,3) \notin R$, *y tampoco es transitiva pues* $(3,1) \in R$, $(1,4) \in R$ *pero* $(3,4) \notin R$.

  Las clases de los distintos elementos son:

  $[0] = \{0, 2, 4\}$

  $[1] = \{1, 4\}$

  $[2] = \emptyset$.

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

  $[4] = \{0, 2, 4\}$.

  Vemos como hay una clase que es vacía. Las clases $[0]$ *y* $[1]$ *no son disjuntas ni iguales. Igual ocurre con* $[0]$ *y* $[3]$, *con* $[1]$ *y* $[3]$, *con* $[1]$ *y* $[4]$ *o con* $[3]$ *y* $[4]$. *El* 3 *no pertenece a ninguna clase. Las clases* $[0]$ *y* $[4]$ *sí son iguales.*

Si X es un conjunto, y R es una relación de equivalencia en X, tenemos una aplicación $p : X \to X/R$ definida como $p(x) = [x]$. Esta aplicación se conoce como la *proyección canónica.*

Esta aplicación es siempre sobreyectiva

Ejemplo 1.3.9. *Consideramos en* $\mathbb{Z}$ *la relación de congruencia módulo 3. En tal caso, el conjunto cociente es* $\mathbb{Z}_3$. *La proyección canóncia* $\mathbb{Z} \to \mathbb{Z}_3$ *es la aplicación* $x \mapsto x \textit{ mód } 3$.

Para terminar este apartado dedicado a las relaciones de equivalencia, vamos a ver la descomposición canónica de una aplicación.

Sea $f : X \to Y$ una aplicación. Entonces f se escribe como composición de tres aplicaciones de la forma $f = i \circ b \circ p$, donde p es sobreyectiva, b es biyectiva e i es inyectiva.

Veamos ahora cuales son estas aplicaciones.

La aplicación p es la proyección $p : X \to X/R_f$.

La aplicación b tiene como dominio X/R_f y codominio $Imag(f)$. Esta aplicación viene dada por $b([x]) = f(x)$. Es fácil comprobar que b está bien definida (si $[x] = [x']$, $b([x]) = b([x'])$, y que es una biyección.

Por último, la aplicación $i : Imag(f) \to Y$ es la inclusión (ya que $Imag(f)$ es un subconjunto de Y).

Ejemplo 1.3.10. *Sea* $f : \{0, 1, 2, 3, 4, 5\} \to \{0, 1, 2, 3, 4, 5\}$ *la aplicación dada por* $f(x) = 2x \textit{ mód } 6$. *Vamos a dar la descomposición canónica de* f.

Podemos ver que $f(0) = f(3) = 0$, $f(1) = f(4) = 2$ *y* $f(2) = f(5) = 4$. *Por tanto,* X/R_f *tiene tres elementos, que son:*

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

Por otra parte, $Imag(f) = \{f(0), f(1), f(2), f(3), f(4), f(5)\} = \{0, 2, 4\}$.

Entonces, las tres aplicaciones que aparecen en la descomposición de f *son:*

- $p : \{0,1,2,3,4,5\} \to \{[0],[1],[2]\}$ *definida como* $p(0) = [0]$, $p(1) = [1]$, $p(2) = [2]$, $p(3) = [0]$, $p(4) = [1]$, $p(5) = [2]$.
- $b : \{[0],[1],[2]\} \to \{0,2,4\}$ *definida como* $b([0]) = f(0) = 0$, $b([1]) = f(1) = 2$, $b([2]) = f(2) = 4$.
- $i : \{0,2,4\} \to \{0,1,2,3,4,5\}$ *definida como* $i(0) = 0$, $i(2) = 2$, $i(4) = 4$.

Es fácil comprobar que $f = i \circ b \circ p$, *que* p *es sobreyectiva, que* b *es biyectiva y que* i *es inyectiva.*

1.3.2. Relaciones de orden.

Definición 25. *Sea* X *un conjunto, y* $\leq$ *una relación binaria en* X*. Se dice que* $\leq$ *es una relación de orden si se verifican las siguientes propiedades.*

Reflexiva: $x \leq x$ *para todo* $x \in X$.

Antisimétrica: Si $x \leq y$ *e* $y \leq x$ *entonces* $x = y$.

Transitiva: Si $x \leq y$ *e* $y \leq z$ *entonces* $x \leq z$.

Si X *es un conjunto en el que tenemos definida una relación de orden* $\leq$*, se dice que* $(X, \leq)$ *es un conjunto ordenado (o, si está claro cual es la relación* $\leq$ *se dice simplemente que* X *es un conjunto ordenado).*

Si $\leq$ *es una relación de orden en* X *que satisface la propiedad adicional de que dados* $x, y \in X$ *entonces* $x \leq y$ *ó* $y \leq x$*, se dice entonces que* $\leq$ *es una relación de orden total, y que* $(X, \leq)$ *(o* X*) es un conjunto totalmente ordenado (en ocasiones, para destacar que* $(X, \leq)$ *es una relación de orden, pero que no es total se dice que* $\leq$ *es una relación de orden parcial y que* $(X, \leq)$ *es un conjunto parcialmente ordenado).*

Ejemplo 1.3.11.

1. *El conjunto de los números naturales, con el orden natural (*$m \leq n$ *si existe* $k \in \mathbb{N}$ *tal que* $n = m+k$*) es un conjunto totalmente ordenado. De la misma forma, también lo son* $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$ *y* $(\mathbb{R}, \leq)$.
2. *Dado un conjunto* X*, entonces* $\mathcal{P}(X)$*, con el orden dado por la inclusión es un conjunto ordenado. Si* X *tiene más de un elemento, este orden no es total, pues dados* $x, y \in X$ *distintos se tiene que* $\{x\} \not\subseteq \{y\}$ *y* $\{y\} \not\subseteq \{x\}$.
3. *En el conjunto de los números naturales, la relación de divisibilidad es una relación de orden que no es total. Esta relación viene dada por* $a|b$ *si existe* $c \in \mathbb{N}$ *tal que* $b = a \cdot c$ *(compara con la relación de orden natural). Sin embargo, en el conjunto de los números enteros esta relación no es de orden pues no es antisimétrica, ya que* $2|-2$, $-2|2$ *y sin embargo* $2 \neq -2$.
4. *Para cualquier número natural* n *consideramos el conjunto*
$$D(n) = \{m \in \mathbb{N} : m|n\}$$
Entonces $(D(n), |)$ *es un conjunto (parcialmente) ordenado.*
5. *Sea* $(X, \leq)$ *es un conjunto ordenado, e* Y *un subconjunto de* X*. Definimos en* Y *el orden* $x \preceq y$ *si* $x \leq y$ *(vistos como elementos de* X*). Entonces,* $(Y, \preceq)$ *es un conjunto ordenado. De ahora en adelante, el orden en* Y *lo denotaremos igual que en* X.

   Un ejemplo de esto último podría ser el caso de los divisores de un número natural n.

   Si $(X, \leq)$ *es un conjunto totalmente ordenado, entonces, para cualquier* $Y \subseteq X$ *se tiene que* $(Y, \leq)$ *es un conjunto totalmente ordenado.*

La definición de conjunto ordenado puede hacerse también a partir de la noción de *orden estricto*.

Definición 26. *Sea X un conjunto, y $<$ una relación binaria en X. Se dice que $<$ es un orden estricto si se verifican las siguientes propiedades:*

Antirreflexiva Para cualquier $x \in X$ se tiene que $x \not< x$ (es decir, $R \cap \Delta = \emptyset$).

Transitiva Si $x < y$ e $y < z$ entonces $x < z$.

Es fácil comprobar que si $\leq$ es una relación de orden en un conjunto X, entonces si definimos

$$x < y \text{ si } x \leq y \text{ y } x \neq y$$

se tiene que $<$ es una relación de orden estricto en X.

De la misma forma, si $<$ es una relación de orden estricto en X entonces la relación siguiente:

$$x \leq y \text{ si } x < y \text{ o } x = y$$

es una relación de orden en X.

Vemos entonces que los conceptos de *relación de orden* y *relación de orden estricto* son equivalentes, pues dada una relación de orden tenemos determinada una relación de orden estricto y viceversa. Además, los caminos para pasar de orden a orden estricto, y de orden estricto a orden, son uno el inverso del otro.

A continuación vamos a construir un grafo (dirigido) asociado a una relación de orden. Aún cuando los grafos serán estudiados con posterioridad, la representación de una relación de orden mediante este grafo ayuda a visualizar mejor el orden dado.

Definición 27. *El diagrama de Hasse de un conjunto ordenado $(X, \leq)$ es un grafo dirigido cuyos vértices son los elementos de X, y existe un lado de x a y si $x < y$ y no existe z tal que $x < z < y$.*

El diagrama de Hasse está definido para cualquier conjunto ordenado. Sin embargo, en general dicho diagrama no permite recuperar el orden. Por ejemplo, en el caso del conjunto $(\mathbb{R}, \leq)$, dado cualquier $x \in \mathbb{R}$ no existe ningún $y \in \mathbb{R}$ que esté conectado a x por algún lado.

Sin embargo, si el conjunto X es finito, entonces dados $x, y \in X$ se tiene que $x \leq y$ si $x = y$ o existe algún camino que parta de x y termine en y.

Una forma habitual de representar el diagrama de Hasse es dibujar los lados como líneas ascendentes, lo que implica colocar los vértices de forma apropiada.

Ejemplo 1.3.12.

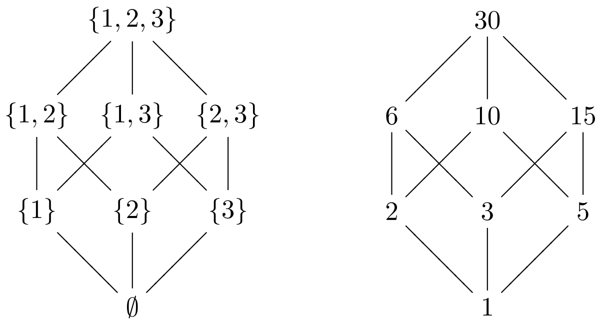
1. *El diagrama de Hasse del conjunto $(\mathbb{N}, \leq)$ sería*

$$\begin{array}{c} \vdots \\ 4 \\ | \\ 3 \\ | \\ 2 \\ | \\ 1 \\ | \\ 0 \end{array}$$

2. *Consideramos el conjunto ordenado $(\mathcal{P}(\{1,2\}, \subseteq)$. Entonces el diagrama de Hasse sería:*

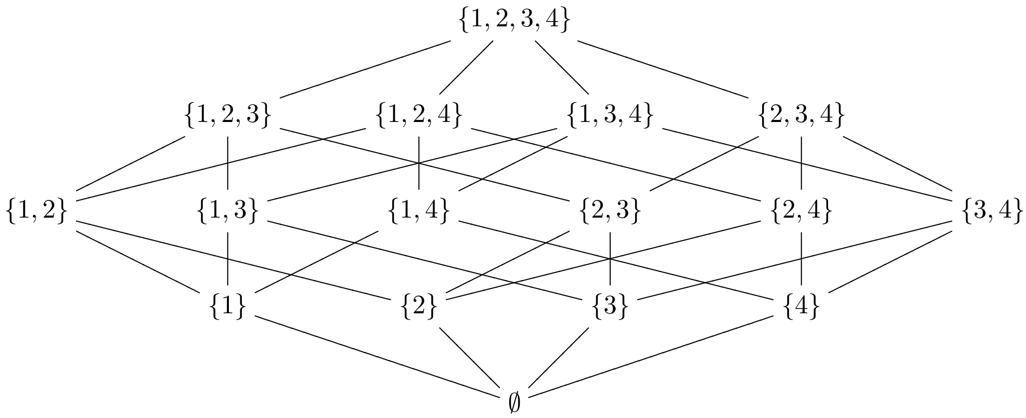
$$\begin{tikzcd}[arrows=-] & \{1,2\} & \\ \{1\} \arrow[ur] & & \{2\} \arrow[ul] \\ & \emptyset \arrow[ul] \arrow[ur] & \end{tikzcd}$$

3. *Vamos a representar los diagramas de Hasse de los conjuntos ordenados* $\mathcal{P}(\{1,2,3\})$ *y* $D(30)$.



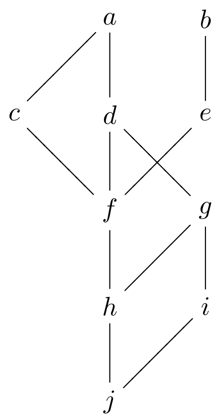
Observa como la estructura de conjunto ordenado es igual en ambos casos.

4. *Vamos a representar el diagrama de Hasse de* $\mathcal{P}(\{1,2,3,4\})$.



Prueba a dibujar el diagrama de Hasse de los divisores de 210 y compáralo con este último.

5. *Si tenemos un grafo dirigido que no contiene caminos cerrados, entonces podemos definir un orden en el conjunto de los vértices.* $x \leq y$ *si* $x = y$ *o existe un camino con inicio* x *y fin* y. *Si en el grafo no hay caminos entre dos vértices adyacentes, entonces el grafo es el diagrama de Hasse de un conjunto ordenado.*



tenemos definido un orden en el conjunto $X = \{a,b,c,d,e,f,g,h,i\}$. *Con este orden se tiene, por ejemplo que,*

$h \leq e$, *pues tenemos un camino* $h - f - e$ *que empieza en* h *y termina en* e.

$i \leq a$, *pues el camino* $i - g - d - a$ *empieza en* i *y termina en* a.

$i \not\leq e$, *pues ningún camino empieza en* i *y termina en* e.

Definición 28. *Sea $(X, \leq)$ un conjunto ordenado.*

1. *Un elemento $x \in X$ se dice que es maximal, si no existe $y \in X$ tal que $x \leq y$ y $x \neq y$.*
2. *Un elemento $x \in X$ se dice que es máximo, si para todo $y \in X$ se verifica que $y \leq x$.*

De la misma forma se puede definir lo que es un elemento minimal y lo que es un mínimo.

Ejemplo 1.3.13. *En el último conjunto ordenado del ejemplo anterior se tiene que a y b son elementos maximales, pues no hay ningún elemento que sea mayor que ellos. Sin embargo, el conjunto X no tiene máximo.*

El elemento j es un elemento minimal, y además es mínimo.

En el conjunto de los divisores de 30 (ver ejemplo anterior) tenemos que 10 *no es un elemento maximal, pues* $10 \leq 30$. *Sí se tiene que* 30 *es un elemento maximal, pues no hay ningún elemento que sea mayor que él. También se tiene que* 30 *es un máximo de ese conjunto.*

En el conjunto $(\mathbb{N}, \leq)$, el cero es el mínimo y es el único elemento minimal. Este conjunto no tiene máximo ni elementos maximales.

Si $(X, \leq)$ es un conjunto ordenado finito, entonces X tiene al menos un elemento maximal y un elemento minimal.

Nótese, que si un conjunto tiene máximo, entonces este es único. Además, en el caso de que tenga máximo, entonces tiene sólo un elemento maximal, que coincide con el máximo.

Idéntica observación vale para mínimo y elemento minimal.

Denotaremos por $\max(X)$ al máximo del conjunto X, en el caso de que exista, y por $\min(X)$ al mínimo.

En el ejemplo que hemos estudiado anteriormente no existe $\max(X)$, mientras que $\min(X) = j$.

Definición 29. *Sea $(X, \leq)$ un conjunto ordenado, e Y un subconjunto de X. Consideramos en Y el orden inducido de X.*

1. *Un elemento $x \in X$ se dice que es* cota superior *de Y si $x \geq y$ para todo $y \in Y$.*
2. *Un elemento $x \in X$ se dice que es* supremo *de Y si es el mínimo del conjunto de las cotas superiores de Y.*

De la misma forma se define lo que es una cota inferior y un ínfimo.

Ejemplo 1.3.14. *Si $X = \{a, b, c, d, e, f, g, h, i, j\}$ con el orden dado anteriormente, e $Y = \{c, d, f, g, h\}$ entonces:*

El conjunto de las cotas superiores de Y es $\{a\}$.

Puesto que este conjunto tiene mínimo, que es a, entonces a es el supremo de Y.

Los elementos c y d son elementos maximales de Y.

El conjunto de las cotas inferiores es $\{h, j\}$.

De éstas, h es el máximo, luego h es el ínfimo de Y.

h es además el único elemento minimal y el mínimo de Y.

Cuando un conjunto tiene supremo éste es único. Podemos entonces hablar de *el supremo de Y*, y lo representaremos mediante $\sup(Y)$.

De la misma forma, denotaremos por $\inf(Y)$ al ínfimo del conjunto Y cuando exista.

Cuando un conjunto tiene máximo, entonces también tiene supremo, y coincide con él. En el último ejemplo vemos como el recíproco no es cierto, pues Y tiene supremo pero no tiene máximo.

Cuando el supremo de un conjunto pertenezca al conjunto, entonces será también el máximo.

Definición 30 (Buen orden). *Sea $(X, \leq)$ un conjunto ordenado. Se dice que $\leq$ es un buen orden si todo subconjunto no vacío de X tiene mínimo. En tal caso, se dice que $(X, \leq)$ (o X) es un conjunto bien ordenado.*

Observación: Todo conjunto bien ordenado es un conjunto totalmente ordenado, pues dados dos elementos $x, y \in X$ el subconjunto $\{x, y\}$ tiene mínimo. Si $\min(\{x, y\}) = x$ entonces $x \leq y$, mientras que si $\min(\{x, y\}) = y$ entonces $y \leq x$.

El recíproco no es cierto. Busca un ejemplo.

Ejemplo 1.3.15. *El conjunto de los números naturales, con el orden usual, es un conjunto bien ordenado.*

Definición 31. *Sean $(X_1, \leq_1)$ y $(X_2, \leq_2)$ dos conjuntos ordenados.*

Se define el orden producto *en $X_1 \times X_2$ como sigue:*

$$(x_1, x_2) \leq_{prod} (y_1, y_2) \text{ si } x_1 \leq_1 y_1 \text{ y } x_2 \leq_2 y_2.$$

Se define el orden lexicográfico *en $X_1 \times X_2$ como sigue:*

$$(x_1, x_2) \leq_{lex} (y_1, y_2) \stackrel{def}{\Longleftrightarrow} \begin{cases} x_1 <_1 y_1 & \text{ó} \\ x_1 = y_1 \text{ y } x_2 \leq_2 y_2. \end{cases}$$

Claramente, si $(x_1, x_2) \leq_{prod} (y_1, y_2)$ entonces $(x_1, x_2) \leq_{lex} (y_1, y_2)$.

Proposición 1.3.2. *Si $(X_1, \leq_1)$ y $(X_2, \leq_2)$ son dos conjuntos ordenados, entonces $(X_1 \times X_2, \leq_{prod})$ y $(X_1 \times X_2, \leq_{lex})$ son conjuntos ordenados.*

Además, si $\leq_1$ y $\leq_2$ son órdenes totales (resp. buenos órdenes) entonces $\leq_{lex}$ es un orden total (resp. buen orden).

Demostración: La demostración de que el orden producto es una relación de orden es fácil, y se deja como ejercicio. Centrémonos pues en el orden lexicográfico.

Notemos en primer lugar que si $(x_1, x_2) \leq_{lex} (y_1, y_2)$ entonces $x_1 \leq_1 y_1$.

Veamos que la relación es de orden.

Reflexiva: Si $(x_1, x_2) \in X_1 \times X_2$ entonces $(x_1, x_2) \leq_{lex} (x_1, x_2)$, pues se da la segunda opción ($x_1 = x_1$ y $x_2 \leq x_2$).

Simétrica: Supongamos que $(x_1, x_2) \leq_{lex} (y_1, y_2)$ y $(y_1, y_2) \leq_{lex} (x_1, x_2)$. Entonces se tiene que $x_1 \leq_1 y_1$ e $y_1 \leq_1 x_1$, de donde $x_1 = y_1$. Deducimos entonces que $x_2 \leq_2 y_2$ e $y_2 \leq_2 x_2$, lo que implica que $x_2 = y_2$.

Transitiva: Supongamos ahora que $(x_1, x_2) \leq_{lex} (y_1, y_2)$ y $(y_1, y_2) \leq_{lex} (z_1, z_2)$. Pueden darse entonces tres opciones(no excluyentes):

- $x_1 <_1 y_1$, en cuyo caso $x_1 <_1 z_1$, luego $(x_1, x_2) \leq_{lex} (z_1, z_2)$.
- $y_1 <_1 z_1$, en cuyo caso $x_1 <_1 z_1$ y concluimos como en la opción anterior.
- $x_1 = y_1$ e $y_1 = z_1$. En tal caso, $x_2 \leq_2 y_2$ e $y_2 \leq_2 z_2$, de donde $x_1 = z_1$ y $x_2 \leq_2 z_2$, es decir, $(x_1, x_2) \leq_{lex} (z_1, z_2)$.

Supongamos ahora que $\leq_1$ y $\leq_2$ son órdenes totales. Sean $(x_1, x_2), (y_1, y_2) \in X_1 \times X_2$. Aquí pueden darse tres opciones (mutuamente excluyentes):

- $x_1 <_1 y_1$. En tal caso $(x_1, x_2) \leq_{lex} (y_1, y_2)$.

- $y_1 <_1 x_1$. En este caso $(y_1, y_2) \leq_{lex} (x_1, x_2)$.
- $x_1 = y_1$. Entonces dependiendo de que $x_2 \leq_2 y_2$ o $y_2 \leq_2 x_2$ se tendrá que $(x_1, x_2) \leq_{lex} (y_1, y_2)$ o que $(y_1, y_2) \leq_{lex} (x_1, x_2)$.

Por último, supongamos que $\leq_1$ y $\leq_2$ son buenos órdenes, y sea $Y \subseteq X_1 \times X_2$ un subconjunto no vacío.

Nos quedamos con el conjunto de todas las primeras coordenadas de los elementos de A, es decir, tomamos

$$Y_1 = \{x_1 \in X_1 : (x_1, x_2) \in A \text{ para algún } x_2 \in X_2\}.$$

Sea $a = \text{mín}(Y_1)$. Tomamos entonces $Y_2 = \{x_2 \in X_2 : (a, x_2) \in A\}$. Como $Y_2 \neq \emptyset$, tiene mínimo. Sea éste b. Entonces $(a, b) = \text{mín}(A)$. ■

Observación: Si tenemos n conjuntos ordenados $X_1, X_2, \ldots, X_n$, podemos definir recursivamente el orden producto y el orden lexicográfico en $X_1 \times X_2 \times \cdots \times X_n$.

Supuesto definido el orden producto $\leq_{prod}$ en $X_1 \times \cdots \times X_{n-1}$ se define en $X_1 \times \cdots \times X_n$:

$$(x_1, \ldots x_{n-1}, x_n) \leq_{prod} (y_1, \ldots, y_{n-1}, y_n) \ si \ (x_1, \ldots, x_{n-1}) \leq_{prod} (y_1, \ldots, y_{n-1}) \text{ y } x_n \leq y_n,$$

es decir, definimos el orden producto en $(X_1 \times \cdots \times X_{n-1}) \times X_n$.

Supuesto definido el orden lexicográfico $\leq_{lex}$ en $X_1 \times \cdots \times X_{n-1}$ se define en $X_1 \times \cdots \times X_n$:

$$(x_1, \ldots x_{n-1}, x_n) \leq_{lex} (y_1, \ldots, y_{n-1}, y_n) \overset{\text{def}}{\Longleftrightarrow} \begin{cases} (x_1, \ldots, x_{n-1}) <_{lex} (y_1, \ldots, y_{n-1}) & \text{ó} \\ (x_1, \ldots, x_{n-1}) = (y_1, \ldots, y_{n-1}) \ y \ x_n \leq y_n. \end{cases}$$

Sea el conjunto

$$\mathcal{A} = \{-, a, b, c, d, e, f, g, h, i, j, l, l, m, n, \tilde{n}, o, p, q, r, s, t, u, v, w, x, y, z\},$$

es decir, las 27 letras del alfabeto junto con el espacio en blanco.

Claramente, $\mathcal{A}$ tiene un orden total de todos conocido.

Supongamos que n es el número de letras de la palabra más larga de la lengua española. Entonces, cada palabra puede representarse como un elemento de $\mathcal{A}^n$ (poniendo tantos espacios al final como sea necesario).

Cuando ordenamos las palabras, tal y como vienen en un diccionario, nos fijamos en la primera letra, y es la que nos da el orden. Cuando ésta coincide, pasamos a la segunda, y es ésta entonces la que nos da el orden. De coincidir también, nos fijamos en la tercera, y así sucesivamente. Es decir, las palabras de la lengua están ordenadas siguiendo el orden lexicográfico.

Ejemplo 1.3.16.

Consideramos en $\mathbb{N} \times \mathbb{N}$ los órdenes producto ($\leq$) y lexicográfico $\leq_{lex}$ deducidos a partir del orden usual en $\mathbb{N}$. Entonces:

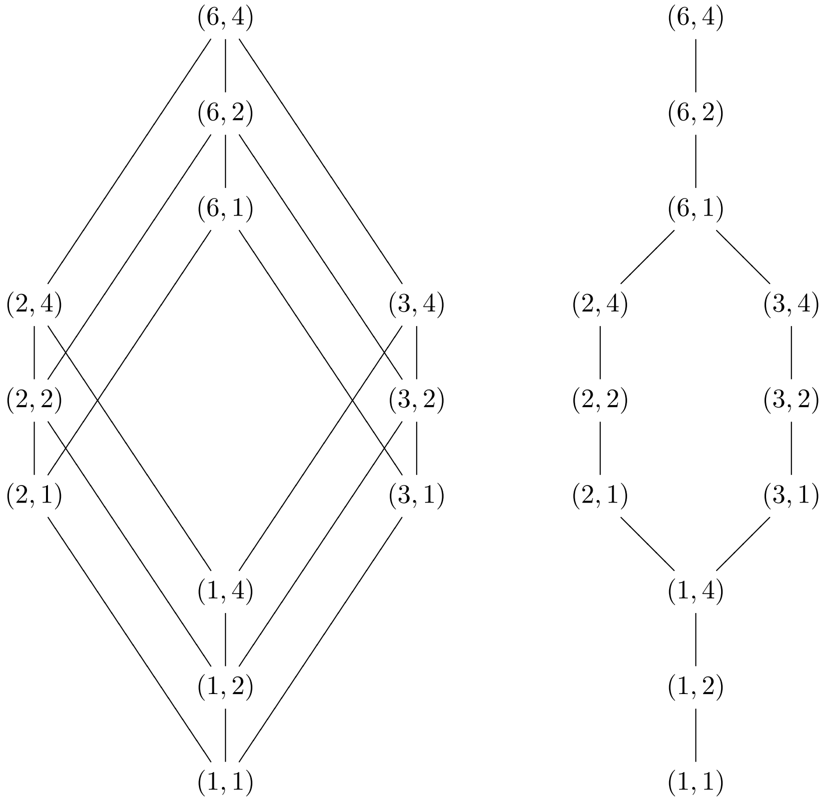
Los elementos $(0, n), (1, n-1), \ldots, (n-1, 1), (n, 0)$ están ordenados según el orden lexicográfico, mientras que con el orden producto ninguna pareja de ellos es comparable.

Se puede ver entonces que la propiedad de ser orden total o buen orden no se mantiene al tomar el orden producto.

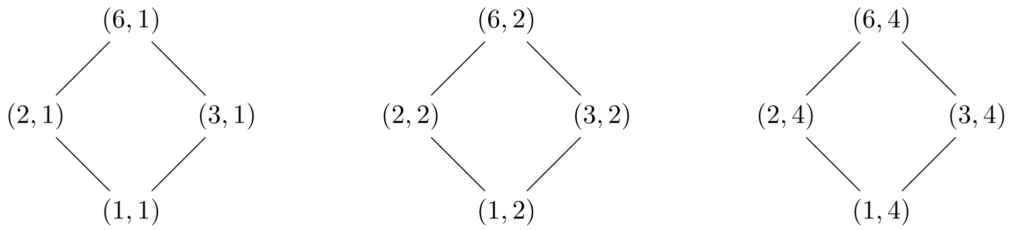
Si $X = \{(0, n), (1, n-1), \ldots, (n-1, 1), (n, 0)\}$ entonces:

- *El conjunto de cotas inferiores con respecto al orden lexicográfico es $\{(0, 0), (0, 1), \ldots, (0, n)\}$, mientras que con respecto al orden producto tiene una única cota inferior, que es $(0, 0)$.*
- *El ínfimo, respecto al orden lexicográfico es $(0, n)$, que es también el mínimo. Con respecto al orden producto es $(0, 0)$, y no tiene mínimo.*
- *Con respecto al orden lexicográfico tiene un elemento minimal, que es $(0, n)$ y un elemento maximal, que es $(n, 0)$. Con respecto al orden producto, todos los elementos son maximales y minimales.*

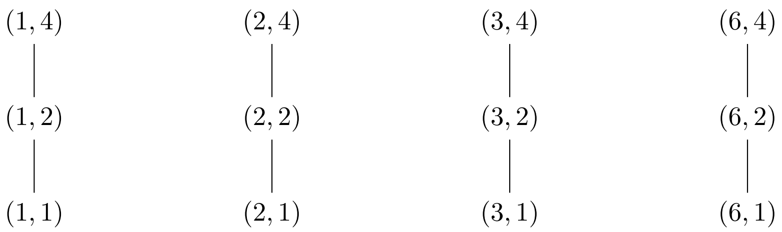
Sean ahora los conjuntos ordenados $(D(6), |)$ *y* $(D(4), |)$*. Entonces los diagramas de Hasse de* $D(6) \times D(4)$ *con el orden producto y el orden lexicográfico son respectivamente:*



Nótese como el diagrama de Hasse de $D(6) \times D(4)$ *con el orden producto consiste en "pegar" tres diagramas como el de* $D(6)$

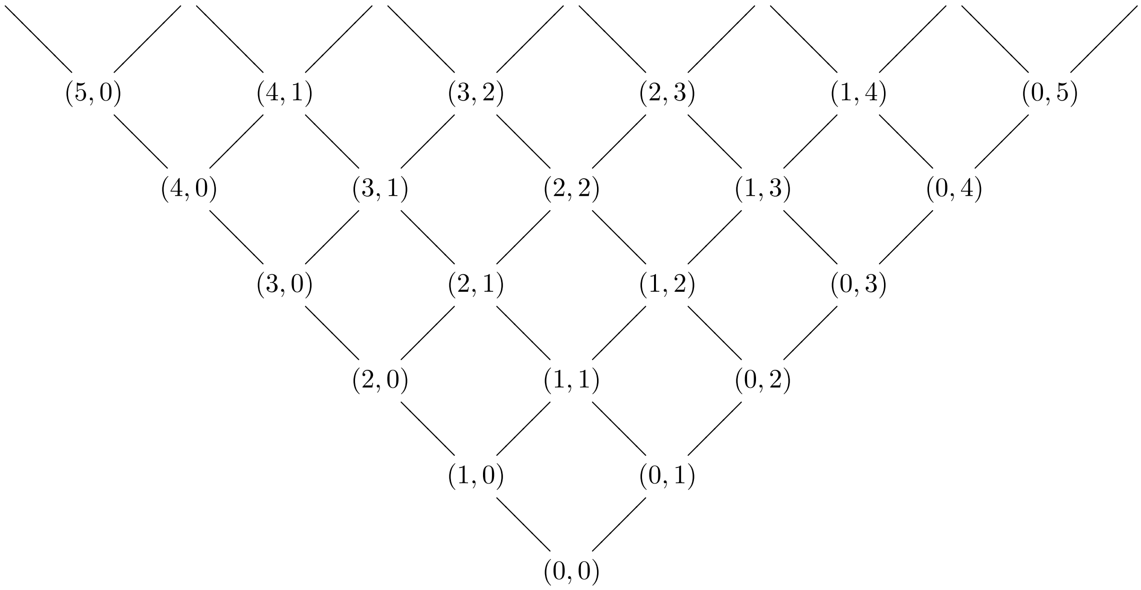


y cuatro diagramas como el de $D(4)$



mientras que el diagrama de Hasse de $D(6) \times D(4)$ *con el orden lexicográfico tiene la "misma forma" que el de* $D(6)$*, salvo que en cada vértice tenemos un diagrama de* $D(4)$*.*

El diagrama de Hasse de $(\mathbb{N}^2, \leq_{prod})$ *sería como sigue:*


(5, 0) (4, 1) (3, 2) (2, 3) (1, 4) (0, 5)
(4, 0) (3, 1) (2, 2) (1, 3) (0, 4)
(3, 0) (2, 1) (1, 2) (0, 3)
(2, 0) (1, 1) (0, 2)
(1, 0) (0, 1)
(0, 0)