# Lógica 1

Enrique Casanovas

Curso 1999 - 2000

# Índice general

**1. Axiomas de la Teoría de Conjuntos** **3**

**2. Operaciones Booleanas** **11**

**3. Relaciones** **18**

**4. Equivalencia y Orden** **26**

**5. Funciones** **36**

**6. Números Naturales** **46**

**7. Conjuntos Finitos y Conjuntos Infinitos** **56**

**Bibliografía** **64**

**Índice de Materias** **65**

# Capítulo 1

# Axiomas de la Teoría de Conjuntos

La Teoría de Conjuntos es una de las partes principales de la Lógica. Tiene un papel muy importante en la discusión de los fundamentos de la Matemática y en el estudio de las nociones de *infinito* y de *número*. Desde ese punto de vista es una disciplina útil para la Filosofía de la Lógica y de la Matemática.

La teoría es fundamentalmente creación de un autor, G. Cantor, y su fecha de nacimiento puede cifrarse en los finales del siglo XIX. Pero hay ciertos precedentes y hay numerosas contribuciones de otros lógicos y matemáticos posteriores. También debe ser mencionado que en la segunda mitad del siglo XX la Teoría de Conjuntos ha experimentado avances espectaculares.

Una de las nociones centrales de la Teoría de Conjuntos es la de *cardinalidad* de un conjunto. Es una medida del tamaño aplicable también a conjuntos infinitos. Se dice que dos conjuntos tienen la misma cardinalidad cuando existe una aplicación biyectiva entre ellos. Los *números cardinales* representan las distintas cardinalidades de los conjuntos. Estos números están ordenados de tal modo que cada uno tiene un sucesor, un número inmediatamente superior. Los números naturales $0, 1, 2, \ldots$ son las cardinalidades de los conjuntos finitos. Tras ellos aparece el primer cardinalidad infinito $\aleph_0$, que es la cardinalidad del conjunto de los números naturales. A este número cardinal le siguen $\aleph_1, \aleph_2, \ldots$. El proceso sigue mucho más allá de lo que uno pueda imaginarse en principio. Cantor demostró que el conjunto de los números racionales tiene cardinalidad $\aleph_0$ y que la misma cardinalidad tiene el conjunto de los números reales algebraicos. Por otro lado demostró que la cardinalidad del conjunto de los números reales es mayor que $\aleph_0$. Existe una operación de exponenciación entre números cardinales que permite describir la cardinalidad del conjunto de los números reales como $2^{\aleph_0}$. Una pregunta que surge naturalmente es si $2^{\aleph_0} = \aleph_1$ o no. Esta ecuación se conoce con el nombre de *Hipótesis del Continuo*. Cantor dedicó muchos esfuerzo a intentar demostrarla pero no lo consiguió. En 1938 K. Gödel demostró que la Hipótesis del Continuo es irrefutable, es decir, que en Teoría de Conjuntos no se puede demostrar que es falsa a no ser que la Teoría de Conjuntos sea una teoría contradictoria y permita demostrar cualquier enunciado. En 1964 P. Cohen demostró que la Hipótesis del Continuo no es un teorema de la Teoría de Conjuntos a no ser, de nuevo, que la Teoría de Conjuntos sea contradictoria. Esto estableció el estatus de la Hipótesis del Continuo como enunciado indecidible en base a los axiomas comúnmente admitidos. Pero además los métodos de Gödel y Cohen abrieron la puerta a la Teoría de Conjuntos contemporánea, donde a menudo no se demuestran teoremas sino que se demuestra que ciertos enunciados son indemostrables o irrefutables. Pero estas cuestiones no pueden ser tratadas en esta asignatura. Aquí sólo se va a efectuar una introducción a la axiomática y al tratamiento de las nociones de infinito y de número cardinal.

La parte de la Teoría de Conjuntos que se enseña en esta asignatura es bastante elemental. Se introducen nociones y se exponen resultados que son necesarios para poder desarrollar posteriormente otras partes de la Lógica, en particular la Semántica de la Lógica de Primer Orden. Por otro lado esta asignatura está destinada a enseñar a hacer demostraciones, de manera que se concede una especial importancia a la manera en que los teoremas se van justificando.

La Teoría de Conjuntos habla esencialmente de *conjuntos*. Sin embargo no se debe esperar encontrar una definición de qué es un conjunto, no es frecuente que las teorías definan los objetos de los que hablan y normalmente sólo dan una descripción parcial de ellos. De hecho aquí hablaremos no sólo de conjuntos, sino que hablaremos más generalmente de *objetos*. Ciertos objetos serán conjuntos y otros no. Estos últimos se llamarán *objetos primitivos*. Los conjuntos se formarán con objetos primitivos y con conjuntos ya formados. Puede hacerse Teoría de Conjuntos sin considerar más objetos que los conjuntos, es decir, sin objetos primitivos. En ocasiones se llama Teoría de Conjuntos Puros. De hecho en la mayoría de los libros de texto se encuentra expuesta la Teoría de Conjuntos Puros. La razón es que la eliminación de los objetos primitivos simplifica la escritura de los enunciados y además se puede justificar fácilmente que no hay realmente una gran pérdida eliminando estos objetos primitivos pues pueden ser convenientemente simulados mediante conjuntos puros. Aquí mantendremos los objetos primitivos en la presentación de la teoría aunque no tendrán un papel muy relevante.

Entre los objetos de los que la teoría habla hay una relación establecida, la relación de *pertenencia*. Se dice que un objeto es *elemento* de otro si le pertenece, es decir, si está relacionado con él mediante esa relación de pertenencia. Los objetos primitivos no tienen elementos pero pueden ser elementos de otros objetos. Los conjuntos pueden tener o no tener elementos. Veremos que hay un único conjunto sin elementos. Por otro lado los conjuntos pueden ser elementos de otros objetos, es decir, tendremos conjuntos de conjuntos, conjuntos de conjuntos de conjuntos, etc.

La Teoría de Conjuntos es una *teoría* y como tal es un conjunto de enunciados de un cierto lenguaje. En este caso el lenguaje es el de la Lógica de Primer Orden con un símbolo "$\in$" para la relación de pertenencia. Usamos por tanto el símbolo de igualdad, conectores lógicos, cuantificadores, paréntesis y variables. Para distinguir los conjuntos entre los objetos de los que hablamos usamos dos tipos de variables: minúsculas $x, y, z, \ldots$ para objetos cualesquiera y mayúsculas $A, B, C, \ldots$ para conjuntos. En la práctica este lenguaje se ampliará en distintas direcciones:

- introduciremos nuevos símbolos mediante *definiciones*,
- introduciremos más tipos de variables para ciertos tipos de conjuntos,
- usaremos el lenguaje natural mezclado con el lenguaje formal para poder expresar los hechos de modo más natural y comprensible.

Esta ampliación del lenguaje es inesencial. Todo enunciado del lenguaje ampliado tiene una traducción al lenguaje formal inicial.

Los enunciados de la teoría de conjuntos están organizados en tres categorías: *axiomas, definiciones* y *teoremas*. Los axiomas caracterizan a la teoría. No precisan ser demostrados aunque su significado puede ser explicado y discutido. Las definiciones tampoco se demuestran, sirven sólo para ampliar el lenguaje y facilitar así la expresión breve de enunciados complejos. Los teoremas deben ser demostrados a partir de los axiomas, las definiciones y otros teoremas previamente demostrados. Los *lemas*, las *proposiciones* y los *corolarios* son teoremas. Se llaman de estas maneras diversas según su importancia, el motivo por el que se enuncian o la facilidad con que se demuestran a partir de otros teoremas.

Los axiomas de la Teoría de Conjuntos se irán introduciendo poco a poco y se intercalarán definiciones y teoremas en ese proceso. La teoría no estará totalmente presentada hasta el final.

**Axioma 1.1 (Axioma de Extensionalidad)** *Conjuntos con los mismos elementos son iguales.*

El hecho de que los conjuntos $A$ y $B$ tienen los mismos elementos se expresa con la fórmula

$$\forall x(x \in A \leftrightarrow x \in B)$$

o, si se prefiere, mediante

$$\forall x(x \in A \rightarrow x \in B) \wedge \forall x(x \in B \rightarrow x \in A).$$

Por tanto el Axioma de Extensionalidad se enuncia en el lenguaje formal como sigue:

$$\forall A \forall B(\forall x(x \in A \leftrightarrow x \in B) \rightarrow A = B).$$

Una manera alternativa de expresarlo consiste en decir que si $A$ y $B$ son conjuntos distintos, entonces no tienen los mismos elementos, es decir $A$ tiene un elemento que $B$ no tiene o $B$ tiene un elemento que $A$ no tiene:

$$A \neq B \rightarrow \exists x(x \in A \wedge x \notin B) \vee \exists x(x \in B \wedge x \notin A).$$

Obsérvese que, con independencia del Axioma de Extensionalidad y por motivos puramente lógicos, es cierto que

$$A = B \rightarrow \forall x(x \in A \leftrightarrow x \in B).$$

Si juntamos esto con el Axioma de Extensionalidad obtenemos que

**Proposición 1.2** $\forall x(x \in A \leftrightarrow x \in B) \leftrightarrow A = B$

Esto nos permite eliminar la igualdad en $A = B$ utilizando en su lugar la expresión $\forall x(x \in A \leftrightarrow x \in B)$.

**Definición** Decimos que $A$ *está incluido en* $B$ o que $A$ *es un subconjunto de* $B$ y escribimos $A \subseteq B$ si todos los elementos de $A$ son elementos de $B$, esto es,

$$A \subseteq B \leftrightarrow \forall x(x \in A \rightarrow x \in B).$$

Para decir que $A$ no está incluido en $B$ escribimos $A \nsubseteq B$. Obsérvese que $A \nsubseteq B$ significa que algún elemento de $A$ no es elemento de $B$ pero no significa que todos los elementos de $A$ estén fuera de $B$.

**Observaciones 1.3** *1.* $A \subseteq A$

*2.* $A \subseteq B \wedge B \subseteq A \rightarrow A = B$

*3.* $A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$

Es importante distinguir bien entre pertenencia ($\in$) e inclusión ($\subseteq$). La inclusión es una relación entre conjuntos, la pertenencia es una relación entre objetos y conjuntos. La inclusión es transitiva pero la pertenencia no. Hay casos en que un cierto conjunto pertenece a otro y al mismo tiempo está incluido en él, pero no es ésta la situación habitual. El modo más frecuente en que interaccionan en las demostraciones estas dos relaciones está resumido en los dos siguientes principios:

- De $A \subseteq B$ y $x \in A$ se infiere que $x \in B$.
- De $A \subseteq B$ y $x \notin B$ se infiere que $x \notin A$.

Introducimos ahora una notación de uso frecuente en teoría de conjuntos: el *abstractor*. Supongamos que $P$ es una propiedad y que por algún motivo se sabe ya que existe un conjunto $A$ cuyos elementos son precisamente los objetos que tienen esa propiedad, es decir

$$\forall x (x \in A \leftrightarrow P(x)),$$

donde $P(x)$ significa que $x$ tiene la propiedad $P$. En ese caso decimos que la propiedad $P$ determina un conjunto y nos referimos a ese conjunto $A$ con la notación

$$\{x : P(x)\}.$$

Obsérvese que esto es legítimo dado que por el Axioma de Extensionalidad sabemos que sólo puede existir un tal conjunto $A$, es decir si $B$ es otro conjunto y también

$$\forall x (x \in B \leftrightarrow P(x))$$

entonces $A = B$.

**Observaciones 1.4** *Supóngase que las propiedades $P$ y $Q$ determinan conjuntos. Entonces*

*1.* $\forall z (z \in \{x : P(x)\} \leftrightarrow P(z))$

*2.* $A = \{x : P(x)\} \leftrightarrow \forall x (x \in A \leftrightarrow P(x))$

*3.* $\{x : P(x)\} = \{x : Q(x)\} \leftrightarrow \forall x (P(x) \leftrightarrow Q(x))$

*4.* $\{x : P(x)\} = \{y : P(y)\}$.

De hecho si se sabe que $P$ determina un conjunto y $Q$ es otra propiedad tal que $\forall x (P(x) \leftrightarrow Q(x))$, entonces también $Q$ determina un conjunto y determina precisamente el mismo conjunto que $P$, es decir, $\{x : P(x)\} = \{x : Q(x)\}$.

Ciertas propiedades determinan un conjunto. Por ejemplo la propiedad $x \in A$ determina el conjunto $A$. Así pues, $A = \{x : x \in A\}$. Pero no toda propiedad determina un conjunto. Este hecho fue observado por B. Russell para el caso particular de la propiedad $x \notin x$ y esta observación se conoce con el nombre de *Paradoja de Russell*.

**Proposición 1.5** *No hay ningún conjunto $A$ tal que $\forall x(x \in A \leftrightarrow x \notin x)$, es decir, $\{x : x \notin x\}$ no existe.*

**Prueba**. Efectuando una prueba indirecta supongamos lo contrario, es decir, que existe un conjunto $A$ tal que

$$\forall x(x \in A \leftrightarrow x \notin x).$$

Esto vale en particular para el caso $x = A$, de modo que

$$A \in A \leftrightarrow A \notin A$$

lo cual es una contradicción.

Si bien es cierto que no toda propiedad determina un conjunto, también es verdad que es habitual en la teoría intuitiva de conjuntos utilizar propiedades para formar conjuntos tomando los elementos de un cierto conjunto previamente formado que tengan la propiedad en cuestión, es decir *separando* los elementos del conjunto que tienen la propiedad de los que no la tienen. En la teoría axiomática también podemos hacer eso.

**Axioma 1.6 (Esquema de Separación)** *Si $P$ es una propiedad expresable en el lenguaje de la teoría de conjuntos, para cada conjunto $X$ existe el conjunto $\{x : x \in X \wedge P(x)\}$, es decir hay un conjunto $A$ tal que $\forall x(x \in A \leftrightarrow x \in X \wedge P(x))$.*

Obsérvese que el Esquema de Separación no es un simple axioma sino una infinidad de axiomas: a cada propiedad $P$ le corresponde un axioma de separación, el axioma

$$\forall X \exists A \forall x(x \in A \leftrightarrow x \in X \wedge P(x)).$$

Obsérvese también que el Esquema de Separación no sirve para obtener conjuntos a no ser que se tengan ya conjuntos. Pero en algún momento habrá que empezar a tener conjuntos por algún otro medio. Para ello serán necesarios otros axiomas.

El hecho de que exijamos que la propiedad $P$ sea expresable en el lenguaje de la teoría de conjuntos no es retórico. Se obtienen contradicciones en la teoría si este punto no se respeta. Un ejemplo de ello es la llamada *paradoja de Richard*. Consiste en lo siguiente. Consideremos el conjunto $\mathbb{N}$ de los números naturales. La existencia de ese conjunto puede garantizarse con los axiomas de la teoría de conjuntos. Consideremos ahora la propiedad $P$ que consiste en ser un objeto definible en castellano utilizando menos de 23 palabras. No está nada claro que esa propiedad pueda expresarse en el lenguaje de la teoría de conjuntos. Puede haber discusiones acerca de cuáles son exactamente las palabras del castellano. Imaginemos que hemos fijado un determinado fragmento con rigor y que ese fragmento contiene sólo un número finito de palabras, por ejemplo todas las que alguna vez hayan aparecido escritas. Eliminada esta ambigüedad comenzamos la discusión. Supongamos que existe el conjunto $A = \{x : x \in \mathbb{N} \wedge P(x)\}$. Veremos que ello conduce a contradicciones. Como no tenemos más que un número finito de palabras, no hay más que un número finito de propiedades expresadas mediante 23 palabras en castellano. Eso quiere decir que el conjunto $A$ es finito y con ello que su complemento $\mathbb{N} \setminus A$ es infinito y en particular no es un conjunto vacío. Es un hecho que todo conjunto no vacío de números naturales tiene un menor elemento. Por tanto $\mathbb{N} \setminus A$ tiene un menor elemento $n$. Obsérvese que $n \notin A$. Pero $n$ es el menor número natural que no pertenece al conjunto de los números naturales definibles en castellano mediante menos de 23 palabras. Ésta es una definición de $n$ que usa menos de 23 palabras. Como $n$ es entonces definible con menos de 23 palabras, $n \in A$. Esto es una contradicción.

Enunciamos ahora un axioma que nos garantiza que hay conjuntos. Este axioma resulta redundante si se hace Teoría de Conjuntos Puros, es decir si todos los objetos considerados son conjuntos.

**Axioma 1.7 (Axioma de Existencia de Conjuntos)** *Hay conjuntos, esto es,* $\exists A\, A = A$.

**Proposición 1.8** *Existe un conjunto sin elementos, es decir,* $\exists A \forall x\, x \notin A$.

**Prueba**. Por el Axioma de Existencia de Conjuntos sabemos que hay al menos un conjunto $B$. Aplicamos el esquema de separación al conjunto $B$ y a la propiedad $x \neq x$ obteniendo con ello que $A = \{x : x \in B \wedge x \neq x\}$ es un conjunto. Obviamente $A$ no puede tener elementos, pues si $x \in A$ entonces $x \neq x$.

**Proposición 1.9** *Hay a lo sumo un conjunto sin elementos. Formalmente,*

$$\forall x\, x \notin A \wedge \forall x\, x \notin B \rightarrow A = B.$$

**Prueba**. Sean $A$ y $B$ conjuntos sin elementos. Entonces $A$ y $B$ tienen los mismos elementos, esto es, $\forall x(x \in A \leftrightarrow x \in B)$. Por el Axioma de Extensionalidad, $A = B$.

En virtud de las dos últimas proposiciones sabemos que hay un único conjunto sin elementos. Esto nos permite hacer la siguiente definición.

**Definición** El *conjunto vacío*, $\emptyset$, es el único conjunto que no tiene elementos.

La propiedad $x \neq x$ determina entonces un conjunto, el conjunto vacío. Podemos escribir

$$\emptyset = \{x : x \neq x\}.$$

**Observaciones 1.10** *1.* $\forall x\, x \notin \emptyset$

*2.* $\forall x\, x \notin A \rightarrow A = \emptyset$

*3.* *para cualquier propiedad* $P$, $\forall x(x \in \emptyset \rightarrow P(x))$

*4.* $\emptyset \subseteq A$

*5.* $A \subseteq \emptyset \rightarrow A = \emptyset$

Si bien hay un conjunto mínimo, el conjunto vacío, veremos ahora que no hay un conjunto máximo. El proceso de construcción de conjuntos no puede darse nunca por acabado.

**Proposición 1.11** *No hay un conjunto universal, es decir, un conjunto al que pertenezcan todos los objetos. Formalmente,* $\neg\exists A \forall x\, x \in A$

**Prueba**. Supongamos que existe un conjunto $A$ con la propiedad de que $\forall x x \in A$. Aplicamos el esquema de separación al conjunto $A$ y a la propiedad $x \notin x$ obteniendo de ese modo el conjunto $B = \{x : x \in A \wedge x \notin x\}$. Sin embargo la propiedad $x \in A \wedge x \notin x$ es sustituible por la propiedad $x \notin x$, pues la condición $x \in A$ ya la verifican todos los objetos $x$. Al efectuar esta sustitución se obtiene que existe el conjunto $A = \{x : x \notin x\}$. Per esto contradice a la proposición 1.5.

A continuación introducimos una serie de axiomas que garantizan la existencia de los conjuntos finitos de objetos. De hecho bastaría con uno sólo de esos axiomas garantizando la existencia de pares, pues los restantes se podrían introducir con el auxilio de la operación de unión, pero esa operación todavía no la podemos usar.

**Axioma 1.12 (Axiomas de Existencia de Conjuntos Finitos)** *Para cada secuencia de objetos $x_1, \ldots, x_n$ existe un conjunto cuyos elementos son $x_1, \ldots, x_n$ y nada más. Formalmente,*

$$\forall x_1 \cdots x_n \exists A \forall x (x \in A \leftrightarrow x = x_1 \vee \cdots \vee x = x_n).$$

**Definición** Designamos con $\{x_1, \ldots, x_n\}$ al conjunto cuyos elementos son precisamente los objetos $x_1, \ldots, x_n$. En el caso $n = 1$ llamamos *unitario* de $x_1$ al conjunto $\{x_1\}$ así obtenido. Para el caso $n = 2$, llamamos *par* de $x_1, x_2$ al correspondiente conjunto $\{x_1, x_2\}$.

**Observaciones 1.13** *1.* $x \in \{x\}$

*2.* $x \in \{x, y\} \wedge y \in \{x, y\}$

*3.* $\forall u(u \in \{x\} \leftrightarrow u = x)$

*4.* $\forall u(u \in \{x, y\} \leftrightarrow u = x \vee u = y)$

*5.* $\{x, x\} = \{x\}$

*6.* $\{x\} = \{y\} \leftrightarrow x = y$

*7.* $\{x, y\} = \{u, v\} \leftrightarrow (x = u \wedge y = v) \vee (x = v \wedge y = u)$

*8.* $\{x, y\} = \{y, x\}$

*9.* $\forall x(x \in A \leftrightarrow \{x\} \subseteq A)$

Si $a$ es un objeto, la propiedad $x = a$ determina un conjunto, concretamente determina el conjunto $\{a\}$, pues $\{a\} = \{x : x = a\}$. Si $b$ es otro objeto, la propiedad $(x = a \vee x = b)$ también determina un conjunto, el conjunto $\{a, b\}$, pues $\{a, b\} = \{x : x = a \vee x = b\}$. Lo mismo se puede decir en general de la propiedad $(x = a_1 \vee \cdots \vee x = a_n)$, que determina el conjunto $\{a_1, \ldots, a_n\}$, esto es,

$$\{a_1, \ldots, a_n\} = \{x : x = a_1 \vee \cdots \vee x = a_n\}.$$

Con los axiomas introducidos hasta el momento podemos garantizar la existencia de los conjuntos $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\{\emptyset\}\}$, etc. Es conveniente darse cuenta de que todos estos conjuntos son distintos. Por ejemplo, $\emptyset$ no tiene elementos, pero los demás sí. Tanto $\{\emptyset\}$ como $\{\{\emptyset\}\}$ son conjuntos con un sólo elemento, pero el elemento en cuestión no es el mismo y por ello los conjuntos son distintos. El elemento de $\{\emptyset\}$ es $\emptyset$ mientras que el elemento de

$\{\{\emptyset\}\}$ es $\{\emptyset\}$. Por su parte $\{\emptyset, \{\emptyset\}\}$ es un conjunto con dos elementos y por ello no puede ser igual a los anteriores. El conjunto vacío pertenece a algunos conjuntos pero no a todos. Sin embargo está incluido en todos. Puede ayudar a comprender estas nociones el descifrar qué relaciones de pertenencia e inclusión se dan entre los siguientes conjuntos: $A = \emptyset$, $B = \{\emptyset\}$, $C = \{\{\emptyset\}\}$, $D = \{\emptyset, \{\emptyset\}\}$, $E = \{\emptyset, \{\{\emptyset\}\}\}$, $F = \{\{\emptyset\}, \{\{\emptyset\}\}\}$ y $G = \{\{\emptyset, \{\emptyset\}\}\}$.

# Capítulo 2

# Operaciones Booleanas

En este capítulo vamos a tratar de las operaciones de unión, intersección y diferencia de conjuntos. Se introducirán algunos nuevos axiomas. Las operaciones de intersección y diferencia de conjuntos pueden obtenerse aplicando el esquema de separación. Lo explicamos a continuación.

**Proposición 2.1** *1. Dados dos conjuntos $A$ y $B$ existe siempre un tercer conjunto $C$ cuyos elementos son los elementos comunes a $A$ y a $B$, esto es*

$$\forall AB\exists C\forall x(x \in C \leftrightarrow x \in A \wedge x \in B)$$

*2. Dados dos conjuntos $A$ y $B$ existe siempre un tercer conjunto $C$ cuyos elementos son los elementos de $A$ que no son elementos de $B$, esto es,*

$$\forall AB\exists C\forall x(x \in C \leftrightarrow x \in A \wedge x \notin B)$$

**Prueba**. El primer conjunto se obtiene aplicando el esquema de separación al conjunto $A$ y a la propiedad $x \in B$. El segundo se obtiene aplicándolo al conjunto $A$ y a la propiedad $x \notin B$.

**Definición** La proposición anterior nos asegura que tanto $\{x : x \in A \wedge x \in B\}$ como $\{x : x \in A \wedge x \notin B\}$ existen. El primer conjunto se llama *intersección de $A$ y $B$* y se denota con $A \cap B$. El segundo conjunto se llama *diferencia de $A$ y $B$* y se denota $A \setminus B$.

La operación de unión no puede obtenerse de ese modo. Necesitamos un axioma específico que garantice su existencia. Introducimos de momento una versión débil de este axioma.

**Axioma 2.2 (Axioma de Uniones. Primera versión)** *Dados dos conjuntos $A$ y $B$ existe siempre un tercer conjunto $C$ cuyos elementos se obtienen añadiendo a los elementos de $A$ los de $B$, es decir*

$$\forall AB\exists C\forall x(x \in C \leftrightarrow x \in A \vee x \in B)$$

**Definición** El axioma anterior nos asegura que $\{x : x \in A \vee x \in B\}$ existe. El conjunto $\{x : x \in A \vee x \in B\}$ se llama *unión de $A$ y $B$* y se denota con $A \cup B$.

**Observaciones 2.3** *1.* $\forall x(x \in A \cap B \leftrightarrow x \in A \wedge x \in B)$

*2.* $\forall x(x \in A \setminus B \leftrightarrow x \in A \wedge x \notin B)$

*3.* $\forall x(x \in A \cup B \leftrightarrow x \in A \vee x \in B)$

La siguiente es una lista de las propiedades básicas de estas operaciones.

**Proposición 2.4** *Cualesquiera conjuntos $A, B, C$ cumplen las siguientes ecuaciones:*

1. $A \cap B = B \cap A$ *(Conmutatividad de la intersección)*
2. $A \cap (B \cap C) = (A \cap B) \cap C$ *(Asociatividad de la intersección)*
3. $A \cap A = A$ *(Idempotencia de la intersección)*
4. $A \cap \emptyset = \emptyset$
5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *(Distributividad de la intersección respecto a la unión)*
6. $A \cup B = B \cup A$ *(Conmutatividad de la unión)*
7. $A \cup (B \cup C) = (A \cup B) \cup C$ *(Asociatividad de la unión)*
8. $A \cup A = A$ *(Idempotencia de la unión)*
9. $A \cup \emptyset = A$
10. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(Distributividad de la unión respecto a la intersección)*
11. $A \setminus A = \emptyset$
12. $A \setminus \emptyset = A$
13. $\emptyset \setminus A = \emptyset$
14. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
15. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
16. $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$
17. $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$

**Ejercicio 2.5** *1.* *Demostrar las siguientes ecuaciones.*

   a) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$
   b) $(A \setminus B) \setminus C = A \setminus (B \cup C)$
   c) $A \cap B = A \setminus (A \setminus B)$

*2.* *Decidir si los siguientes enunciados son verdaderos. En caso afirmativo dar una demostración y en caso negativo un contraejemplo.*

   a) $A \setminus B = C \setminus B \rightarrow A = C$
   b) $A \cup B = B \cup C \rightarrow A \setminus C = B \setminus C$

c) $A \setminus C = B \setminus C \to A \cup C = B \cup C$

d) $A \setminus B = B \setminus A \leftrightarrow A = B$

Las relaciones más importantes que hay entre estas operaciones de unión, intersección y diferencia por un lado y la inclusión por el otro están resumidas en la siguiente proposición. Se muestra que cada una de estas operaciones permite caracterizar la inclusión y que a su vez todas ellas son caracterizables en términos de la inclusión.

**Proposición 2.6** *1.* $A \subseteq B$ *si y sólo si* $A \cup B = B$.

*2.* $A \subseteq B$ *si y sólo si* $A \cap B = A$.

*3.* $A \subseteq B$ *si y sólo si* $A \setminus B = \emptyset$.

*4.* $A \cup B$ *es el menor conjunto que incluye a* $A$ *y a* $B$*, es decir*

a) $A \subseteq A \cup B$ *y* $B \subseteq A \cup B$.

b) *Si* $C$ *es un conjunto que cumple las condiciones* $A \subseteq C$ *y* $B \subseteq C$*, entonces* $A \cup B \subseteq C$.

*5.* $A \cap B$ *es el mayor conjunto que está incluido en* $A$ *y en* $B$*, es decir*

a) $A \cap B \subseteq A$ *y* $A \cap B \subseteq B$.

b) *Si* $C$ *es un conjunto que cumple las condiciones* $C \subseteq A$ *y* $C \subseteq B$*, entonces* $C \subseteq A \cap B$.

*6.* $A \setminus B$ *es el mayor conjunto que está incluido a* $A$ *y es disjunto de* $B$*, es decir*

a) $A \setminus B \subseteq A$ *y* $(A \setminus B) \cap B = \emptyset$.

b) *Si* $C$ *es un conjunto que cumple las condiciones* $C \subseteq A$ *y* $C \cap B = \emptyset$*, entonces* $C \subseteq A \setminus B$.

**Ejercicio 2.7** *Demostrar lo siguiente:*

*1.* $A \subseteq B \to C \setminus B \subseteq C \setminus A$

*2.* $A \subseteq B \wedge C \subseteq D \to A \cup C \subseteq B \cup D$

*3.* $A \subseteq B \wedge C \subseteq D \to A \cap C \subseteq B \cap D$

**Definición** La *diferencia simétrica* de los conjuntos $A$ y $B$ es el conjunto $A \,\Delta\, B$ formado por los elementos en los que difieren, es decir,

$$A \,\Delta\, B = (A \setminus B) \cup (B \setminus A).$$

**Ejercicio 2.8** *Demostrar que se cumple lo siguiente:*

*1.* $A \,\Delta\, B = (A \cup B) \setminus (A \cap B)$

*2.* $A \,\Delta\, B = \emptyset \leftrightarrow A = B$

*3.* $A \,\Delta\, A = \emptyset$

*4.* $A \,\Delta\, B = B \,\Delta\, A$

*5.* $A \,\Delta\, (B \,\Delta\, C) = (A \,\Delta\, B) \,\Delta\, C$

**Definición** Sea $U$ un conjunto. Si $A$ es un subconjunto de $U$, definimos el *complemento* de $A$ respecto a $U$ como $\overline{A} = U \setminus A$. Hay que ser cuidadosos con esta notación porque es relativa al conjunto $U$ que hay que fijar de antemano en cualquier discusión con complementos.

**Observaciones 2.9** *Sea $U$ un conjunto y sean $A$ y $B$ subconjuntos de $U$. Consideramos complementos respecto a $U$. Se cumple lo siguiente:*

| | | |
|---|---|---|
| 1. $\overline{\overline{A}} = A$ | 6. $A \setminus B = A \cap \overline{B}$ | 11. $\overline{A \cup B} = \overline{A} \cap \overline{B}$ |
| 2. $\overline{\emptyset} = U$ | 7. $A \subseteq B \leftrightarrow \overline{B} \subseteq \overline{A}$ | 12. $A \cup B = \overline{\overline{A} \cap \overline{B}}$ |
| 3. $\overline{U} = \emptyset$ | 8. $A = B \leftrightarrow \overline{A} = \overline{B}$ | 13. $A \cap B = \emptyset \leftrightarrow A \subseteq \overline{B}$ |
| 4. $A \cap \overline{A} = \emptyset$ | 9. $\overline{A \cap B} = \overline{A} \cup \overline{B}$ | 14. $A \cup B = U \leftrightarrow \overline{A} \subseteq B$ |
| 5. $A \cup \overline{A} = U$ | 10. $A \cap B = \overline{\overline{A} \cup \overline{B}}$ | 15. $A = \overline{B} \leftrightarrow A \cup B = U \wedge A \cap B = \emptyset$ |

**Axioma 2.10 (Axioma del Conjunto Potencia)** *Para cada conjunto $A$ existe un conjunto $B$ cuyos elementos son los subconjuntos de $A$, esto es,*

$$\forall A \exists B \forall x (x \in B \leftrightarrow x \subseteq A).$$

**Definición** El *conjunto potencia* de $A$ , $\mathcal{P}(A)$, es el conjunto formado por los subconjuntos de $A$, es decir, $\mathcal{P}(A) = \{x : x \subseteq A\}$.

Para entender bien esta noción resulta útil calcular $\mathcal{P}(\{0,1,2\})$ y calcular $\mathcal{P}(\emptyset)$, $\mathcal{P}(\mathcal{P}(\emptyset))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$, etc.

**Observaciones 2.11** *1.* $A \subseteq B \leftrightarrow A \in \mathcal{P}(B)$.

*2.* $\emptyset \in \mathcal{P}(A)$

*3.* $A \in \mathcal{P}(A)$

*4.* $\forall x (x \in A \leftrightarrow \{x\} \subseteq A)$

*5.* $A \in \mathcal{P}(C) \wedge B \in \mathcal{P}(C) \rightarrow A \cap B \in \mathcal{P}(C)$

*6.* $A \in \mathcal{P}(C) \wedge B \in \mathcal{P}(C) \rightarrow A \setminus B \in \mathcal{P}(C)$.

*7.* $A \in \mathcal{P}(C) \wedge B \in \mathcal{P}(C) \leftrightarrow A \cup B \in \mathcal{P}(C)$.

**Ejercicio 2.12** *Decidir si los siguientes enunciados son verdaderos. En caso afirmativo dar una demostración y en caso negativo un contraejemplo.*

*1.* $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$

*2.* $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$

*3.* $\mathcal{P}(A \setminus B) = \mathcal{P}(A) \setminus \mathcal{P}(B)$

Con las operaciones que hemos introducido podemos efectuar la unión y la intersección de cualquier colección finita de conjuntos, simplemente hay que repetir el proceso de unir o intersectar dos cada vez. Pero esto no puede generalizarse al caso de una familia arbitraria de conjuntos. Necesitamos otras operaciones. Para el caso de la intersección la correspondiente operación se obtiene aplicando el esquema de separación, pero para la unión necesitamos un axioma nuevo, una versión definitiva del Axioma de Uniones. Estas operaciones se aplican a conjuntos cuyos elementos son conjuntos, es decir, a colecciones o familias de conjuntos. Usaremos para ellas las variables $\Phi, \Psi, \ldots$

**Axioma 2.13 (Axioma de Uniones. Segunda versión)** *Para cada colección de conjuntos $\Phi$ existe un conjunto $A$ cuyos elementos son los elementos de los elementos de $\Phi$, esto es,*

$$\forall\Phi\exists A\forall x(x \in A \leftrightarrow \exists y(x \in y \wedge y \in \Phi)).$$

**Definición** La *gran unión* de $\Phi$, $\bigcup\Phi$, es el conjunto formado por los elementos de los elementos de $\Phi$, es decir,

$$\bigcup\Phi = \{x : \exists y(x \in y \wedge y \in \Phi)\}.$$

**Observaciones 2.14** *1.* $\bigcup\emptyset = \emptyset$

*2.* $\bigcup\{A, B\} = A \cup B$

*3.* $\bigcup\{A\} = A$

*4.* $\bigcup\{A_1, \ldots, A_n\} = A_1 \cup \cdots \cup A_n$

*5.* $\bigcup\mathcal{P}(A) = A$

**Proposición 2.15** *Para cada colección no vacía de conjuntos $\Phi$ existe un conjunto $A$ cuyos elementos son los elementos que pertenecen a todos los elementos de $\Phi$, esto es,*

$$\forall\Phi(\Phi \neq \emptyset \rightarrow \exists A\forall x(x \in A \leftrightarrow \forall y(y \in \Phi \rightarrow x \in y))).$$

**Prueba**. Sea $\Phi$ una colección no vacía de conjuntos. Esto significa que hay un conjunto $B$ tal que $B \in \Phi$. Aplicamos el esquema de separación al conjunto $B$ y a la propiedad que consiste en pertenecer a todos los elementos de $\Phi$, es decir, a la propiedad $\forall y(y \in \Phi \rightarrow x \in y)$. Obtenemos así un conjunto $A$ cuyos elementos son los elementos de $B$ que tienen esa propiedad, esto es $A = \{x : x \in B \wedge \forall y(y \in \Phi \rightarrow x \in y)\}$. Como

$$\forall x(x \in B \wedge \forall y(y \in \Phi \rightarrow x \in y) \leftrightarrow \forall y(y \in \Phi \rightarrow x \in y)),$$

vemos que de hecho $A = \{x : \forall y(y \in \Phi \rightarrow x \in y)\}$.

**Definición** La *gran intersección* de una colección no vacía de conjuntos $\Phi$, $\bigcap\Phi$, es el conjunto formado por los elementos que pertenecen a todos los elementos de $\Phi$, es decir,

$$\bigcap\Phi = \{x : \forall y(y \in \Phi \rightarrow x \in y)\}.$$

La gran intersección del vacío no está definida. Nunca hablaremos de $\bigcap\emptyset$ y cuando usemos la notación $\bigcap\Phi$ tendremos que estar seguros de que $\Phi$ es una colección no vacía. Obsérvese que si uno se empeñara en decir que existe el conjunto

$$\bigcap\emptyset = \{x : \forall y(y \in \emptyset \to x \in y)\}$$

caería en contradicciones pues ese conjunto sería un conjunto universal.

**Observaciones 2.16** *1.* $\bigcap\{A, B\} = A \cap B$

*2.* $\bigcap\{A\} = A$

*3.* $\bigcap\{A_1, \ldots, A_n\} = A_1 \cap \cdots \cap A_n$

*4.* $\bigcap\mathcal{P}(A) = \emptyset$

En relación con las operaciones de gran unión y gran intersección se utiliza en ocasiones la notación de *cuantificación acotada*. La notación $(\exists x \in y)\varphi$ abrevia $\exists x(x \in y \wedge \varphi)$ y la notación $(\forall x \in y)\varphi$ abrevia $\forall x(x \in y \to \varphi)$. Obsérvese que $\neg(\exists x \in y)\varphi$ es lógicamente equivalente a $(\forall x \in y)\neg\varphi$ y que $\neg(\forall x \in y)\varphi$ lo es a $(\exists x \in y)\neg\varphi$. Usando la cuantificación acotada se pueden expresar la gran unión y la gran intersección de modo muy breve:

$$\bigcup\Phi = \{x : (\exists y \in \Phi)x \in y\} \text{ y } \bigcap\Phi = \{x : (\forall y \in \Phi)x \in y\}.$$

Para poder enunciar de modo sencillo las generalizaciones de las propiedades básicas de la unión y la intersección a estas operaciones de gran unión y gran intersección, es conveniente introducir una notación nueva. Si $A$ es un conjunto y $\Phi$ una colección de conjuntos, entonces mediante $\{A \cap X : X \in \Phi\}$ nos referimos al conjunto formado por todos los objetos de la forma $A \cap X$ que se pueden obtener utilizando elementos $X$ de $\Phi$, es decir,

$$\{A \cap X : X \in \Phi\} = \{B : \exists X(X \in \Phi \wedge B = A \cap X)\}.$$

Otras notaciones análogas son $\{A \cup X : X \in \Phi\}$ y $\{A \smallsetminus X : X \in \Phi\}$. Y si $\Phi$ y $\Psi$ son colecciones de conjuntos, con $\{X \cap Y : X \in \Phi \wedge Y \in \Psi\}$ denotamos el conjunto formado por todas las intersecciones que se pueden hacer entre elementos de $\Phi$ y elementos de $\Psi$. Formalmente

$$\{X \cap Y : X \in \Phi \wedge Y \in \Psi\} = \{Z : \exists XY(Z = X \cap Y \wedge X \in \Phi \wedge Y \in \Psi)\}.$$

La notación $\{X \cup Y : X \in \Phi \wedge Y \in \Psi\}$ se entiende de modo similar. Un problema que se plantea al usar estas notaciones es que previamente debería asegurarse que el conjunto en cuestión existe. Esto puede garantizarse sin dificultades en cada caso concreto, pero no lo vamos a ir haciendo. Otra cuestión es que si se usa, por ejemplo, la notación $\bigcap\{A \cap X : X \in \Phi\}$ previamente debería saberse que $\{A \cap X : X \in \Phi\}$ no es vacío. Eso se cumple cuando $\Phi$ es una colección no vacía. Tampoco iremos repitiendo este tipo de comentarios continuamente.

**Proposición 2.17** *Sean $\Phi$ y $\Psi$ colecciones de conjuntos y sea $A$ un conjunto. Se supone además que las colecciones afectadas por la gran intersección no son vacías.*

*1.* $(\bigcup\Phi) \cup (\bigcup\Psi) = \bigcup(\Phi \cup \Psi)$ *y* $(\bigcap\Phi) \cap (\bigcap\Psi) = \bigcap(\Phi \cup \Psi)$.

*2.* $A \cup \bigcup\Phi = \bigcup(\Phi \cup \{A\})$ *y* $A \cap (\bigcap\Phi) = \bigcap(\Phi \cup \{A\})$.

3. $A \cup (\bigcap \Phi) = \bigcap\{A \cup X : X \in \Phi\}$ *y* $A \cap \bigcup \Phi = \bigcup\{A \cap X : X \in \Phi\}$.
4. $(\bigcup \Phi) \cap (\bigcup \Psi) = \bigcup\{X \cap Y : X \in \Phi \wedge Y \in \Psi\}$
5. $(\bigcap \Phi) \cup (\bigcap \Psi) = \bigcap\{X \cup Y : X \in \Phi \wedge Y \in \Psi\}$
6. $A \smallsetminus \bigcup \Phi = \bigcap\{A \smallsetminus X : X \in \Phi\}$ *y* $A \smallsetminus \bigcap \Phi = \bigcup\{A \smallsetminus X : X \in \Phi\}$.
7. $(\bigcup \Phi) \smallsetminus A = \bigcup\{X \smallsetminus A : X \in \Phi\}$ *y* $(\bigcap \Phi) \smallsetminus A = \bigcap\{X \smallsetminus A : X \in \Phi\}$.

**Observaciones 2.18** *Sea $U$ un conjunto y sea $\Phi$ una colección no vacía de subconjuntos de $U$. Consideramos complementos respecto a $U$. Se cumple lo siguiente:*

1. $\overline{\bigcup \Phi} = \bigcap\{\overline{X} : X \in \Phi\}$
2. $\overline{\bigcap \Phi} = \bigcup\{\overline{X} : X \in \Phi\}$
3. $\bigcup \Phi = \overline{\bigcap\{\overline{X} : X \in \Phi\}}$
4. $\bigcap \Phi = \overline{\bigcup\{\overline{X} : X \in \Phi\}}$

**Ejercicio 2.19** *Sea $\Phi$ una colección de conjuntos. Demostrar lo siguiente.*

1. $\bigcup \Phi$ *es el menor conjunto que incluye a todos los elementos de $\Phi$, es decir,*
   a) *Para cada $A \in \Phi$, $A \subseteq \bigcup \Phi$*
   b) *Si $C$ es un conjunto tal que para cada $A \in \Phi$, $A \subseteq C$, entonces $\bigcup \Phi \subseteq C$.*
2. *Supóngase que $\Phi \neq \emptyset$. Entonces $\bigcap \Phi$ es el mayor conjunto que está incluido en todos los elementos de $\Phi$, es decir,*
   a) *Para cada $A \in \Phi$, $\bigcap \Phi \subseteq A$*
   b) *Si $C$ es un conjunto tal que para cada $A \in \Phi$, $C \subseteq A$, entonces $C \subseteq \bigcap \Phi$.*

# Capítulo 3

# Relaciones

**Definición** Definimos el *par ordenado* de $x$ e $y$ como el conjunto

$$\langle x, y\rangle = \{\{x\}, \{x, y\}\}.$$

Se dice que $x$ es la primera componente o primera coordenada de $\langle x, y\rangle$ y que $y$ es la segunda.

Esta definición tiene una cierta dosis de arbitrariedad. De lo que se trata es de encontrar un conjunto $\langle x, y\rangle$ asociado a $x$ e $y$, dados en ese orden, que los represente en esa ordenación. No importa qué elementos tenga $\langle x, y\rangle$, lo único que importa es que verifique la siguiente condición

$$\langle x, y\rangle = \langle u, v\rangle \leftrightarrow x = u \wedge y = v$$

Existen otras soluciones a este problema, es decir, podríamos definir el par ordenado de otras manera cumpliendo todavía esta última condición. La definición que hemos dado se debe a Kuratowski y es la habitual. Una alternativa, propuesta por Wiener, consiste en definir $\langle x, y\rangle$ como el conjunto $\{\{x\}, \{y, \emptyset\}\}$.

**Proposición 3.1** $\langle x, y\rangle = \langle u, v\rangle \leftrightarrow x = u \wedge y = v$

**Prueba**. Es claro que de $x = u \wedge y = v$ ya se sigue que $\langle x, y\rangle = \langle u, v\rangle$. Supongamos ahora que $\langle x, y\rangle = \langle u, v\rangle$ y veamos que $x = u \wedge y = v$. Tenemos que

$$\{\{x\}\{x, y\}\} = \{\{u\}\{u, v\}\}.$$

Por las observaciones de 1.13 sabemos que se pueden plantear dos casos

1. $\{x\} = \{u\} \wedge \{x, y\} = \{u, v\}$
2. $\{x\} = \{u, v\} \wedge \{x, y\} = \{u\}$

Consideremos el caso 1. Como $\{x\} = \{u\}$, ya tenemos que $x = u$. La igualdad $\{x, y\} = \{u, v\}$ implica que aparecen dos nuevos subcasos. El primero de ellos consiste en que $x = u \wedge y = v$. En este caso ya obtenemos lo que buscábamos. El segundo consiste en que $x = v \wedge y = u$. En esta situación $x = y = u = v$ y por tanto $x = u \wedge y = v$. Consideremos ahora el caso 2. Como $\{x\} = \{u, v\}$, resulta que $x = u = v$. Y como $\{x, y\} = \{u\}$, resulta que $x = y = u$. Por tanto $x = y = u = v$ y en especial $x = u \wedge y = v$.

**Ejercicio 3.2** *Mostrar que si se definiera* $\langle x, y\rangle = \{x, \{y\}\}$ *no se cumpliría la Proposición 3.1.*

**Definición** El *producto cartesiano* de los conjuntos $A$ y $B$, $A \times B$, es el conjunto formado por todos los pares ordenados cuya primera componente pertenece a $A$ y cuya segunda componente pertenece a $B$. Así pues

$$A \times B = \{\langle x, y\rangle : x \in A \wedge y \in B\}.$$

Hay que observar que en la definición de $A \times B$ estamos usando la misma notación abreviada que, por ejemplo, en $\{A \cap X : X \in \Phi\}$. Sin usarla tenemos que

$$A \times B = \{z : \exists x \exists y (z = \langle x, y\rangle \wedge x \in A \wedge y \in B)\}.$$

Por tanto, para decidir si un objeto pertenece o no a $A \times B$ hay que usar lo siguiente:

$$\forall z (z \in A \times B \leftrightarrow \exists x \exists y (z = \langle x, y\rangle \wedge x \in A \wedge y \in B)).$$

Sin embargo si la pregunta es si un par ordenado $\langle x, y\rangle$ pertenece o no a $A \times B$, entonces se puede usar el siguiente criterio:

$$\forall x \forall y (\langle x, y\rangle \in A \times B \leftrightarrow x \in A \wedge y \in B).$$

Otra cuestión es que, previamente a la definición de $A \times B$, deberíamos haber demostrado que existe un conjunto $C$ cuyos elementos son todos los pares ordenados cuya primera componente es de $A$ y cuya segunda componente es de $B$, es decir,

$$\forall A \forall B \exists C \forall z (z \in C \leftrightarrow \exists x \exists y (z = \langle x, y\rangle \wedge x \in A \wedge y \in B)).$$

El conjunto $C$ puede obtenerse aplicando el esquema de separación a la propiedad $\exists x \exists y (z = \langle x, y\rangle \wedge x \in A \wedge y \in B)$ y al conjunto $\mathcal{P}\mathcal{P}(A \cup B)$. En posteriores definiciones no siempre entraremos en estos detalles.

**Observaciones 3.3** *1.* $A \times \emptyset = \emptyset \times A = \emptyset$

*2.* $A \times B = B \times A \leftrightarrow A = B \vee A = \emptyset \vee B = \emptyset$

*3.* $A \times (B \cup C) = (A \times B) \cup (A \times C)$ *y* $(A \cup B) \times C = (A \times C) \cup (B \times C)$

*4.* $A \times (B \cap C) = (A \times B) \cap (A \times C)$ *y* $(A \cap B) \times C = (A \times C) \cap (B \times C)$

*5.* $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$ *y* $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$

*6.* $A \subseteq B \wedge C \subseteq D \rightarrow A \times C \subseteq B \times D$

**Ejercicio 3.4** *El siguiente enunciado es falso.*

$$A \times C \subseteq B \times D \rightarrow A \subseteq B \wedge C \subseteq D.$$

*Mostrar que es falso mediante un contraejemplo y añadir alguna condición adicional que lo haga verdadero.*

**Ejercicio 3.5** *Demostrar los siguientes enunciados.*

1. $A \times \bigcup \Phi = \bigcup \{A \times X : X \in \Phi\}$

2. *Si* $\Phi \neq \emptyset$, *entonces* $A \times \bigcap \Phi = \bigcap \{A \times X : X \in \Phi\}$.

**Definición** Una *relación* es un conjunto de pares ordenados. Usamos las variables $R, S, T$, con subíndices si es preciso, para relaciones. Se dice que $R$ es una *relación en el conjunto* $A$ si $R$ es un conjunto de pares ordenados formados por elementos de $A$, es decir, si $R$ es un subconjunto de $A \times A$. Formalmente,

- $R$ es una relación $\leftrightarrow \forall x(x \in R \rightarrow \exists u \exists v\ x = \langle u, v\rangle)$
- $R$ es una relación en $A \leftrightarrow R \subseteq A \times A$.

Obsérvese que si $R$ es una relación en $A$, entonces $R$ es una relación. La notación $xRy$ es una abreviación de $\langle x, y\rangle \in R$. Se lee "$x$ está relacionado con $y$ mediante $R$".

El siguiente enunciado incluye una versión del Axioma de Extensionalidad para las relaciones.

**Proposición 3.6** 1. *Si* $\forall xy(xRy \rightarrow xSy)$ *entonces* $R \subseteq S$.

2. *Si* $\forall xy(xRy \leftrightarrow xSy)$, *entonces* $R = S$.

**Prueba**. Basta con mostrar el punto *1*, pues el punto *2* se sigue de él. Para ver que $R \subseteq S$ tenemos que mostrar que todos los elementos de $R$ son elementos de $S$, es decir, que $\forall z(z \in R \rightarrow z \in S)$. Sea $z \in R$ y veamos que $z \in S$. Como $R$ es una relación y $z \in R$, $z$ es un par ordenado, es decir, hay $x, y$ tales que $z = \langle x, y\rangle$. Tenemos entonces que $\langle x, y\rangle \in R$. Con la nueva notación, $xRy$. Utilizando ahora la hipótesis, vemos que $xSy$. Esto significa que $\langle x, y\rangle \in S$, es decir, que $z \in S$.

**Definición** El *dominio* de una relación $R$ es el conjunto $\operatorname{dom} R$ formado por las primeras componentes de los pares de $R$ y el *recorrido* de $R$ es el conjunto $\operatorname{rec} R$ formado por las segundas componentes de los pares de $R$. Así pues

$$\operatorname{dom} R = \{x : \exists y xRy\} \text{ y } \operatorname{rec} R = \{y : \exists x xRy\}.$$

El *campo* de $R$ es el conjunto $\operatorname{campo} R$ formado por las componentes de los pares de $R$. Por tanto,

$$\operatorname{campo} R = \operatorname{dom} R \cup \operatorname{rec} R.$$

Para garantizar la existencia de $\operatorname{dom} R$ se aplica el Axioma de Separación a la propiedad $\exists y\langle x, y\rangle \in R$ y al conjunto $\bigcup\bigcup R$. Para $\operatorname{rec} R$ se usa la propiedad $\exists y\langle y, x\rangle \in R$ y el mismo conjunto.

**Observaciones 3.7** 1. *$R$ es una relación si y sólo si existen $A$ y $B$ tales que $R \subseteq A \times B$.*

2. *Si $R$ es una relación, entonces existe un conjunto $A$ tal que $R$ es una relación en $A$.*

3. *Para cada relación $R$, $R$ es una relación en $A$ si y sólo si* $\operatorname{campo}(R) \subseteq A$.

4. *$\emptyset$ es una relación en $A$.*
5. *$A \times A$ es una relación en $A$.*
6. *Si $R$ es una relación en $A$, entonces $\emptyset \subseteq R \subseteq A \times A$.*
7. *Si $R, S$ son relaciones en $A$, entonces también $R \cup S$, $R \cap S$ y $R \setminus S$ son relaciones en $A$.*

Hasta el momento las operaciones que realizamos con las relaciones provienen del álgebra booleana de conjuntos. Pero hay otras operaciones que no tiene sentido aplicar a conjuntos cualesquiera pero sí a relaciones. Las introducimos a continuación.

**Definición** La relación de *identidad* en un conjunto $A$ es la relación

$$I_A = \{\langle x, x\rangle : x \in A\}.$$

También puede definirse como

$$I_A = \{\langle x, y\rangle : x \in A \wedge x = y\}.$$

Obviamente se trata de una relación en $A$. La *inversa* de una relación $R$ es la relación $\breve{R}$ obtenida cambiando el orden de las componentes de los pares de $R$, esto es,

$$\breve{R} = \{\langle x, y\rangle : \langle y, x\rangle \in R\}.$$

También es una relación en $A$ si $R$ lo es. La *composición* de las relaciones $R$ y $S$ es la relación

$$R \mid S = \{\langle x, z\rangle : \exists y(\langle x, y\rangle \in R \wedge \langle y, z\rangle \in S)\}.$$

Si $R$ y $S$ son relaciones en $A$ también $R \mid S$ lo es.

**Lema 3.8** *Las siguientes condiciones son equivalentes para la relación $R$:*

1. *$\forall xy(xRy \to x = y)$.*
2. *$R = I_{\text{campo}\,(R)}$.*
3. *Hay un conjunto $A$ tal que $R = I_A$.*
4. *Hay un conjunto $A$ tal que $R \subseteq I_A$.*

**Prueba**. Comenzamos mostrando que *1* implica *2*. Supongamos que se da *1*. Mostramos primero que $R \subseteq I_{\text{campo}\,(R)}$. Supongamos para ello que $xRy$. Por nuestra hipótesis tenemos que $x = y$. Pero por otro lado es claro que $x \in \text{campo}\,(R) \wedge y \in \text{campo}\,(R)$. Por tanto $\langle x, y\rangle \in I_{\text{campo}\,(R)}$. Queda por justificar que $I_{\text{campo}\,(R)} \subseteq R$. Sea $\langle x, y\rangle \in I_{\text{campo}\,(R)}$ y veamos que $\langle x, y\rangle \in R$. Como $\langle x, y\rangle \in I_{\text{campo}\,(R)}$, resulta que $x = y \wedge x \in \text{campo}\,(R)$. Entonces hay un $z$ tal que $xRz$ o hay un $z$ tal que $zRx$. En cualquiera de los dos casos se obtiene de *1* que $x = z$. Entonces tenemos que $x = y = z$ y que $\langle x, z\rangle \in R$, de manera que $\langle x, y\rangle \in R$.

Establecido esta implicación observamos a continuación que es obvio que de *2* se sigue *3* y que de *3* se sigue *4*. Por tanto todo lo que nos queda es mostrar que *4* implica *1*. Pero esto es sencillo, pues si $xRy$ entonces, por *2*, $xI_Ay$ para un cierto conjunto $A$ y, por consiguiente, $x = y$.

**Observaciones 3.9** *1.* $\breve{\emptyset} = \emptyset$, $(A \times B)\breve{} = (B \times A)$ *y* $\breve{I}_A = I_A$.

2. $\breve{\breve{R}} = R$

3. $(R \cap S)\breve{} = \breve{R} \cap \breve{S}$, $(R \cup S)\breve{} = \breve{R} \cup \breve{S}$ *y* $(R \setminus S)\breve{} = \breve{R} \setminus \breve{S}$.

4. $R \mid (S \mid T) = (R \mid S) \mid T$

5. $(R \mid S)\breve{} = \breve{S} \mid \breve{R}$

6. *Si* $R$ *es una relación en* $A$, *entonces* $R \mid I_A = I_A \mid R = R$.

7. $R \mid \emptyset = \emptyset \mid R = \emptyset$.

**Ejercicio 3.10** *Decidir si los siguientes enunciados son verdaderos. En caso afirmativo dar una demostración y en caso negativo un contraejemplo.*

1. $(R \cup S) \mid T = (R \mid T) \cup (S \mid T)$

2. $(R \cap S) \mid T = (R \mid T) \cap (S \mid T)$

3. $(R \setminus S) \mid T = (R \mid T) \setminus (S \mid T)$

**Observaciones 3.11** *1.* $\operatorname{dom} \emptyset = \emptyset = \operatorname{rec} \emptyset$.

2. $\operatorname{dom} I_A = A = \operatorname{rec} I_A$.

3. $\operatorname{dom} A \times B = A$ *si* $B \neq \emptyset$ *y* $\operatorname{rec} A \times B = B$ *si* $A \neq \emptyset$.

4. $\operatorname{dom} \breve{R} = \operatorname{rec} R$ *y* $\operatorname{rec} \breve{R} = \operatorname{dom} R$.

5. $\operatorname{dom} (R \mid S) \subseteq \operatorname{dom} R$ *y* $\operatorname{rec} (R \mid S) \subseteq \operatorname{rec} S$.

6. *Si* $\operatorname{rec} R \subseteq \operatorname{dom} S$, *entonces* $\operatorname{dom} (R \mid S) = \operatorname{dom} R$.

7. *Si* $\operatorname{dom} S \subseteq \operatorname{rec} R$, *entonces* $\operatorname{rec} (R \mid S) = \operatorname{rec} R$.

**Ejercicio 3.12** *Decidir si los siguientes enunciados son verdaderos. En caso afirmativo dar una demostración y en caso negativo un contraejemplo.*

1. *Si* $\operatorname{dom} (R \mid S) = \operatorname{dom} R$, *entonces* $\operatorname{rec} R \subseteq \operatorname{dom} S$.

2. *Si* $\operatorname{rec} (R \mid S) = \operatorname{rec} S$, *entonces* $\operatorname{dom} S \subseteq \operatorname{rec} R$.

**Ejercicio 3.13** *Decidir si los siguientes enunciados son verdaderos. En caso afirmativo dar una demostración y en caso negativo un contraejemplo.*

1. $\operatorname{dom} (R \cup S) = \operatorname{dom} R \cup \operatorname{dom} S$

2. $\operatorname{dom} (R \cap S) = \operatorname{dom} R \cap \operatorname{dom} S$

3. $\operatorname{dom} (R \setminus S) = \operatorname{dom} R \setminus \operatorname{dom} S$

En la última parte de este capítulo se introducen y discuten las propiedades de las relaciones que se necesitan posteriormente para estudiar las relaciones de equivalencia y de orden.

**Definición** Decimos que la relación $R$ es *reflexiva en el conjunto* $A$ si para cada $x \in A$, $xRx$ y que $R$ es *reflexiva* si $R$ es reflexiva en su campo. Decimos que $R$ es *irreflexiva* si no hay ningún $x$ tal que $xRx$.

**Observaciones 3.14** *1. Cualquier relación es reflexiva en $\emptyset$.*

*2. Si $R$ es reflexiva en $A$ y $B \subseteq A$, entonces $R$ también es reflexiva en $B$.*

*3. $\emptyset$ es reflexiva en $A$ si y sólo si $A = \emptyset$.*

*4. La única relación que es al tiempo reflexiva e irreflexiva es $\emptyset$, pero hay relaciones que no son ni reflexivas ni irreflexivas.*

*5. $R$ es reflexiva en $A$ si y sólo si $I_A \subseteq R$.*

*6. $R$ es irreflexiva si y sólo si $I_{\text{campo}\,(R)} \cap R = \emptyset$.*

**Definición** Decimos que la relación $R$ es *simétrica* si

$$\forall xy(xRy \to yRx),$$

decimos que es *asimétrica* si

$$\forall xy(xRy \to \neg yRx),$$

es decir, si no existen $x, y$ tales que $xRy \wedge yRx$. Por último, decimos que $R$ es *antisimétrica* si

$$\forall xy(xRy \wedge yRx \to x = y),$$

es decir, si no hay $x, y$ distintos y tales que $xRy \wedge yRx$.

**Observaciones 3.15** *1. $R$ es simétrica si y sólo si $R \subseteq \breve{R}$ si y sólo si $R = \breve{R}$.*

*2. $R$ es asimétrica si y sólo si $R \cap \breve{R} = \emptyset$.*

*3. $R$ es antisimétrica si y sólo si $R \cap \breve{R} \subseteq I_{\text{campo}\,(R)}$.*

*4. $R$ es asimétrica si y sólo si $R$ es antisimétrica e irreflexiva.*

*5. $R$ es simétrica y asimétrica si y sólo si $R = \emptyset$.*

*6. $R$ es simétrica y antisimétrica si y sólo si hay un conjunto $A$ tal que $R = I_A$.*

**Prueba**. *1.* Sea $R$ simétrica y veamos que $R \subseteq \breve{R}$. Para ello supongamos que $xRy$. Como $R$ es simétrica, tenemos que $yRx$. Pero esto significa que $x\breve{R}y$. Esto establece la inclusión. Ahora vemos que de la inclusión se sigue ya la igualdad. Para ello falta demostrar que $\breve{R} \subseteq R$. Supongamos que $x\breve{R}y$. Entonces $yRx$ y, como $R \subseteq \breve{R}$, también $y\breve{R}x$. Por definición de $\breve{R}$ concluimos que $xRy$. Finalmente mostramos que $R \subseteq \breve{R}$ implica que $R$ es simétrica. Supongamos que $xRy$ y veamos que $yRx$. Como $R \subseteq \breve{R}$, tenemos que $x\breve{R}y$ y entonces, por definición de $\breve{R}$, se concluye que $yRx$.

*2.* Que $R$ sea asimétrica significa que no hay $x, y$ tales que $xRy \wedge yRx$. Pero la condición $xRy \wedge yRx$ es equivalente a $\langle x, y\rangle \in R \cap \breve{R}$. Por tanto la asimetría de $R$ significa que no hay $x, y$ tales que $\langle x, y\rangle \in R \cap \breve{R}$, es decir, a que $R \cap \breve{R} = \emptyset$.

*3*. Que $R$ sea antisimétrica quiere decir que para cada $x, y$, si $xRy \wedge yRx$, entonces $x = y$. Como se acaba de indicar, esto se puede reformular diciendo que para cada $x, y$, si $\langle x, y\rangle \in R \cap \breve{R}$, entonces $x = y$. Pero si $x, y$ cumplen el antecedente de este condicional, entonces son elementos del campo de $R$ y por ello la condición $x = y$ es equivalente a $\langle x, y\rangle \in I_{\text{campo}\,(R)}$. Uniendo todo esto, la antisimetría de $R$ significa que para cada $x, y$, si $\langle x, y\rangle \in R \cap \breve{R}$, entonces $\langle x, y\rangle \in I_{\text{campo}\,(R)}$, lo cual simplemente quiere decir que $R \cap \breve{R} \subseteq I_{\text{campo}\,(R)}$.

*4*. Supongamos que $R$ es asimétrica. Esto significa que no hay $x, y$ tales que $xRy \wedge yRx$. En particular no hay $x, y$ tales que $xRy \wedge yRx \wedge x \neq y$, de manera que $R$ es antisimétrica. Pero además $R$ debe ser irreflexiva, pues en caso contrario existiría un $x$ tal que $xRx$, pero entonces tomando $y = x$ resulta que $xRy \wedge yRx$. Mostramos a continuación que las relaciones que son antisimétricas e irreflexivas deben ser asimétricas. Sea $R$ antisimétrica e irreflexiva y supongamos que $R$ no es asimétrica. Esto significa que existen $x, y$ tales que $xRy \wedge yRx$. Si $x = y$ se tiene $xRx$, lo cual contradice a la irreflexividad. Y si $x \neq y$ se tiene $xRy \wedge yRx \wedge x \neq y$, lo cual contradice a la antisimetría.

*5*. Es fácil comprobar que la relación vacía es tanto simétrica como asimétrica. Vamos a mostrar que ninguna relación distinta del vacío puede tener estas dos propiedades. Para ello supongamos lo contrario, es decir, que hay una relación $R$ simétrica y asimétrica en la que hay al menos un par $\langle x, y\rangle$. Por simetría deber ser entonces $\langle y, x\rangle \in R$, pero por asimetría eso es imposible.

*6*. Se comprueba sin dificultades que $I_A$ es siempre simétrica y antisimétrica. Supongamos ahora que $R$ es una relación simétrica y antisimétrica y veamos que $R$ es la identidad en un conjunto. De acuerdo con el Lema 3.8, basta mostrar que $\forall xy(xRy \rightarrow x = y)$. Supongamos que $xRy$. Por simetría, $yRx$ y por antisimetría, $x = y$.

**Ejercicio 3.16** *Decidir si los siguientes enunciados son verdaderos. En caso afirmativo dar una demostración y en caso negativo un contraejemplo.*

1. *Si $R$ y $S$ son simétricas, entonces $R \cap S$ es simétrica. Lo mismo para $R \cup S$, $R \setminus S$ y $R \mid S$.*

2. *Si $R$ y $S$ son asimétricas, entonces $R \cap S$ es asimétrica. Lo mismo para $R \cup S$, $R \setminus S$ y $R \mid S$.*

3. *Si $R$ y $S$ son antisimétricas, entonces $R \cap S$ es antisimétrica. Lo mismo para $R \cup S$, $R \setminus S$ y $R \mid S$.*

**Definición** Decimos que la relación $R$ es *transitiva* si

$$\forall xyz(xRy \wedge yRz \rightarrow xRz).$$

**Observaciones 3.17** 1. *$R$ es transitiva si y sólo si $R \mid R \subseteq R$.*

2. *$\emptyset$, $I_A$ y $A \times A$ son relaciones transitivas.*

3. *Si $R$ es transitiva e irreflexiva, entonces $R$ es asimétrica.*

4. *Si $R$ es transitiva y simétrica, entonces $R$ es reflexiva.*

**Prueba**. *1*. Supongamos que $R$ es transitiva y que $x(R \mid R)y$ y veamos que $xRy$. Por definición de composición existe un $z$ tal que $xRz \wedge zRy$. Entonces por transitividad $xRy$. Para demostrar la otra dirección, supongamos ahora que $R \mid R \subseteq R$ y supongamos también que $xRy \wedge yRz$. Queremos mostrar que $xRz$. Por definición de composición $x(R \mid R)z$. Entonces la hipótesis $R \mid R \subseteq R$ nos da el resultado $xRz$.

*2*. Si $\emptyset$ no fuera una relación transitiva existirían $x, y, z$ tales que $\langle x, y\rangle \in \emptyset \wedge \langle y, z\rangle \in \emptyset \wedge \langle x, z\rangle \notin \emptyset$, pero esto es imposible porque $\emptyset$ no tiene elementos. Respecto a $I_A$, supongamos que $xI_Ay \wedge yI_Az$. Entonces $x, y, z$ son elementos de $A$ y $x = y \wedge y = z$. Por tanto $x = z$ y así $xI_Az$. Finalmente, para el caso $A \times A$, supongamos que $x(A \times A)y \wedge y(A \times A)z$. Entonces $x, y, z$ son elementos de $A$ y por tanto $x(A \times A)z$.

*3*. Supongamos que $R$ es transitiva e irreflexiva y veamos que es asimétrica. Haciendo una prueba indirecta, supongamos lo contrario, es decir, supongamos que hay $x, y$ tales que $xRy \wedge yRx$. Como $R$ es transitiva, vemos que $xRx$. Pero esto no es posible si $R$ es irreflexiva.

*4*. Supongamos que $R$ es transitiva y simétrica. Para establecer que $R$ es reflexiva, consideremos un elemento arbitrario $x$ del campo de $R$ y veamos que $xRx$. Como $x \in \operatorname{campo}(R)$, existe un $y$ tal que $xRy$ o existe un $y$ tal que $yRx$. Como $R$ es simétrica, de hecho hay un $y$ tal que $xRy \wedge yRx$. Por transitividad tenemos entonces que $xRx$.

**Ejercicio 3.18** *Decidir si los siguientes enunciados son verdaderos. En caso afirmativo dar una demostración y en caso negativo un contraejemplo.*

1. *Si $R$ y $S$ son transitivas, entonces $R \cap S$ es transitiva. Lo mismo para $R \cup S$, $R \smallsetminus S$ y $R \mid S$.*
2. *Si $R$ es transitiva y $S \subseteq R$, entonces $S$ es transitiva.*
3. *Si $R$ y $S$ son relaciones transitivas y $\operatorname{rec} R \cap \operatorname{dom} S = \operatorname{rec} S \cap \operatorname{dom} R = \emptyset$, entonces $R \cup S$ es transitiva.*

# Capítulo 4

# Equivalencia y Orden

**Definición** Se dice que $R$ es una *relación de equivalencia en $A$* si $R$ es una relación en $A$ que es reflexiva en $A$, simétrica y transitiva. Usamos las letras $E, F$ para relaciones de equivalencia. Las relaciones de equivalencia son relaciones de igualdad abstracta. Ello significa que generalizan los rasgos fundamentales de la relación de igualdad.

**Observaciones 4.1** *1. $I_A$ es una relación de equivalencia en $A$.*

*2. $A \times A$ es una relación de equivalencia en $A$.*

*3. Si $E$ y $F$ son relaciones de equivalencia en $A$, entonces $E \cap F$ es una relación de equivalencia en $A$.*

*4. Más generalmente, si $\Phi$ es una colección no vacía formada por relaciones de equivalencia en el conjunto $A$, entonces también $\bigcap \Phi$ es una relación de equivalencia en $A$.*

**Definición** Sea $E$ una relación de equivalencia en $A$. Si $a \in A$, definimos *la clase de equivalencia de $a$ en $E$* como el conjunto

$$[a]_E = \{x : aEx\}.$$

Llamamos *conjunto cociente de $A$ en $E$* al conjunto $A/E$ formado por todas las clases de equivalencia de los elementos de $A$, esto es,

$$A/E = \{[a]_E : a \in A\}.$$

En ocasiones se usa la notación $a/E$ para la clase de equivalencia de $a$ en $E$.

**Observaciones 4.2** *Sea $E$ una relación de equivalencia en $A$ y $a, b \in A$.*

*1. $[a]_E \subseteq A$*

*2. $a \in [a]_E$*

*3. $[a]_E = \{x : xEa\}$*

*4.* $aEb$ *si y sólo si* $[a]_E = [b]_E$

*5.* $aEb$ *si y sólo si* $[a]_E \cap [b]_E \neq \emptyset$

**Prueba**. El punto *1* se sigue del hecho de que $E$ es una relación en $A$, el punto *2* de la reflexividad de $E$ y el punto *3* de la simetría de $E$. Mostramos *4*. Sea $aEb$ y veamos primero que $[a]_E \subseteq [b]_E$. Para ello supongamos que $x \in [a]_E$. Entonces $xEa$. Por transitividad, $xEb$ y por ello $x \in [b]_E$. Usando la simetría se ve que la prueba de $[b]_E \subseteq [a]_E$ es similar. Queda con ello establecido que $[a]_E = [b]_E$ con la hipótesis de que $aEb$. Veamos ahora la otra dirección de *4*. Como $a \in [a]_E$, de la igualdad $[a]_E = [b]_E$ se sigue que $a \in [b]_E$ y por ello que $aEb$. Finalizamos mostrando *5*. Supongamos primero que $aEb$. Entonces, como ya se ha mostrado, $[a]_E = [b]_E$, y como $a \in [a]_E$, concluimos que $[a]_E \cap [b]_E \neq \emptyset$. A la inversa, supongamos ahora que $[a]_E \cap [b]_E \neq \emptyset$ y veamos que $aEb$. De la hipótesis se obtiene que hay un $c$ tal que $c \in [a]_E \cap [b]_E$, con lo cual $cEa \wedge cEb$. Por simetría y transitividad se concluye entonces que $aEb$.

**Definición** $\Pi$ es una *partición* del conjunto $A$ si $\Pi$ es una colección de subconjuntos no vacíos de $A$ que son disjuntos dos a dos y todo elemento de $A$ pertenece a algún elemento de $\Pi$, es decir,

1. $\forall X(X \in \Pi \rightarrow X \subseteq A)$
2. $\emptyset \notin \Pi$
3. $\forall XY(X \in \Pi \wedge Y \in \Pi \wedge X \neq Y \rightarrow X \cap Y = \emptyset)$
4. $\bigcup \Pi = A$

Las particiones de un conjunto y las relaciones de equivalencia en él son las dos caras de la misma moneda. Toda partición genera una relación de equivalencia y la partición se recupera como el conjunto cociente de la relación de equivalencia. Esto se expone en el siguiente resultado.

**Proposición 4.3** $\Pi$ *es una partición de* $A$ *si y sólo si existe una relación de equivalencia* $E$ *en* $A$ *tal que* $\Pi = A/E$.

**Prueba**. Sea $\Pi$ una partición de $A$. Definimos $E$ como la relación en la que están dos objetos $x, y$ cuando existe algún elemento $X \in \Pi$ tal que $x \in X$ y $y \in X$, esto es,

$$E = \{\langle x, y\rangle : \exists X(X \in \Pi \wedge x \in X \wedge y \in X)\}.$$

Verificamos que $E$ es una relación de equivalencia en $A$ y que el conjunto cociente es $\Pi$:

1. $E$ es una relación en $A$. $E$ es un conjunto de pares ordenados y si $\langle x, y\rangle \in E$, entonces hay un $X \in \Pi$ tal que $x \in X \wedge y \in X$. Como $\Pi$ es una partición de $A$, $X$ debe ser un subconjunto de $A$, con lo cual $x \in A \wedge y \in A$. En definitiva, $E \subseteq A \times A$.
2. $E$ es reflexiva en $A$. Sea $x \in A$ y veamos que $xEx$. Como $\bigcup \Pi = A$ y $x \in A$, $x \in \bigcup \Pi$, con lo cual hay un $X$ tal que $X \in \Pi$ y $x \in X$. Por definición de $E$ eso implica que $\langle x, x\rangle \in E$, esto es $xEx$.

3. $E$ es simétrica. Esto es obvio, pues de la condición $x \in X \wedge y \in X$ se sigue la condición $y \in X \wedge x \in X$.

4. $E$ es transitiva. Supongamos que $xEy \wedge yEz$ y veamos que $xEz$. Como $xEy$, existe un $X \in \Pi$ tal que $x \in X \wedge y \in X$. Del mismo modo, como $yEz$, hay un $Y \in \Pi$ tal que $y \in Y \wedge z \in Y$. Entonces $X$ e $Y$ son dos elementos de la partición $\Pi$ y $X \cap Y \neq \emptyset$. De la definición de partición se obtiene entonces que $X = Y$. Entonces $x \in X \wedge z \in X$, con lo cual $xEz$.

5. $E$ es una relación de equivalencia en $A$. Se sigue de los puntos anteriores.

6. Si $X \in \Pi$ y $x \in X$, entonces $[x]_E = X$. Supongamos que $X \in \Pi$ y que $x \in X$. Si $y \in X$ entonces $xEy$ y por ello $y \in [x]_E$. Por tanto es claro que $X \subseteq [x]_E$. Mostramos a continuación que $[x]_E \subseteq X$. Sea $y \in [x]_E$. Entonces $yEx$, de manera que hay un $Y$ tal que $Y \in \Pi \wedge y \in Y \wedge x \in Y$. En ese caso $X$ e $Y$ son elementos de la partición y $X \cap Y \neq \emptyset$, por lo cual $X = Y$. Como $y \in Y$, se concluye que $y \in X$.

7. Para cada $x \in A$, $[x]_E \in \Pi$. Sea $x \in A$. Por definición de partición $A = \bigcup \Pi$ y existe entonces un $X \in \Pi$ tal que $x \in X$. Por el punto anterior se tiene que $[x]_E = X$, de modo que $[x]_E \in \Pi$.

8. $A/E = \Pi$. Del punto anterior se sigue inmediatamente que $A/E \subseteq \Pi$. Establecemos ahora que $\Pi \subseteq A/E$. Sea $X \in \Pi$. Por definición de partición, $X \neq \emptyset$, por lo cual hay un $x$ tal que $x \in X$. Por el punto *6* vemos entonces que $X = [x]_E$. Como $[x]_E \in A/E$, se concluye que $X \in A/E$.

Esto finaliza la mitad de la demostración. Ahora queda establecer que si $E$ es una relación de equivalencia en $A$ entonces el conjunto cociente $A/E$ es una partición de $A$. Los elementos de $A/E$ son las clases de equivalencia de $E$. Usando las observaciones 4.2 vemos que todo elemento de $A/E$ es un subconjunto de $A$, que ningún elemento de $E/A$ es vacío y que elementos distintos de $A/E$ deben ser disjuntos. Para mostrar que $A/E$ es una partición de $A$ sólo falta justificar que $\bigcup(A/E) = A$. Como $A/E$ es una colección de subconjuntos de $A$ ya sabemos que $\bigcup(A/E) \subseteq A$. Finalizamos la prueba mostrando que $A \subseteq \bigcup(A/E)$. Sea $x \in A$. Entonces $x \in [x]_E$ y $[x]_E \in A/E$. Por tanto, $x \in \bigcup(A/E)$.

El siguiente tipo de relaciones que estudiamos son las relaciones de orden. Por un lado hay relaciones de orden estricto y relaciones de orden reflexivo. La diferencia es más de forma de presentación que de fondo. Una misma ordenación de objetos puede expresarse tanto en forma de orden reflexivo como en forma de orden estricto. En el caso reflexivo se expresa la idea de "ser menor o igual que"mientras que en el caso estricto se expresa la idea de ser simplemente "menor que". Posteriormente distinguiremos entre relaciones de orden total y orden no total. Esta distinción afecta al fondo de la cuestión. En el caso del orden total la ordenación se puede representar en forma lineal mientras que en los órdenes no totales siempre hay ramificaciones.

**Definición** Decimos que $R$ es una *relación de orden (parcial) reflexivo en* $A$ si $R$ es una relación en $A$ que es reflexiva en $A$, antisimétrica y transitiva. Decimos que $R$ es una *relación de orden (parcial) estricto en* $A$ si $R$ es una relación en $A$ que es irreflexiva y transitiva (y, por tanto, también asimétrica).

**Observaciones 4.4** *1.* *$\emptyset$ es una relación de orden estricto en $A$ y $I_A$ es una relación de orden reflexivo en $A$.*

*2.* *Si $R$ y $S$ son órdenes estrictos en $A$, entonces $R \cap S$ es un orden estricto en $A$.*

*3.* *Si $R$ y $S$ son órdenes reflexivos en $A$, entonces $R \cap S$ es un orden reflexivo en $A$.*

*4.* *La relación $\{\langle X, Y\rangle : X \subseteq Y \wedge Y \subseteq A\}$ es una relación de orden reflexivo en $\mathcal{P}(A)$.*

*5.* *Si $R$ es un orden estricto en $A$, también $\breve{R}$ lo es.*

*6.* *Si $R$ es un orden reflexivo en $A$, también $\breve{R}$ lo es.*

**Proposición 4.5** *1.* *Si $R$ una relación de orden reflexivo en $A$, entonces $R \smallsetminus I_A$ es una relación de orden estricto en $A$. Se llama el orden estricto asociado a $R$.*

*2.* *Si $S$ una relación de orden estricto en $A$, entonces $S \cup I_A$ es una relación de orden reflexivo en $A$. Se llama el orden reflexivo asociado a $S$.*

*3.* *Sea $R$ un orden reflexivo en $A$. El orden reflexivo asociado al orden estricto asociado a $R$ es de nuevo $R$.*

*4.* *Sea $S$ un orden estricto en $A$. El orden estricto asociado al orden reflexivo asociado a $S$ es de nuevo $S$.*

*5.* *Sea $R$ un orden reflexivo en $A$ y sea $S$ su orden estricto asociado. Entonces*

   a*)* $\forall xy(xSy \leftrightarrow xRy \wedge x \neq y)$

   b*)* $\forall xy(xRy \leftrightarrow xSy \vee (x \in A \wedge x = y))$.

**Prueba**. *1*. Supongamos que $R$ es un orden reflexivo en $A$ y sea $S = R \smallsetminus I_A$. Obviamente $S$ es una relación en $A$. Como campo $(S) \subseteq A$ y $S \cap I_A = \emptyset$, sabemos que $S \cap I_{\text{campo}\,(S)} = \emptyset$, es decir, $S$ es irreflexiva. Falta sólo mostrar que $S$ es transitiva. Supongamos que $xSy \wedge ySz$. Entonces $x \neq y \wedge xRy \wedge y \neq z \wedge yRz$. Como $R$ es transitiva, $xRz$. Si fuera $x = z$ tendríamos que $zRy \wedge yRz$ y por la antisimetría de $R$, $z = y$. Pero $z \neq y$, de manera que debe ser $x \neq z$ y por tanto $xSz$.

*2*. Supongamos que $S$ es un orden estricto en $A$ y sea $R = S \cup I_A$. Como $R$ es unión de dos relaciones en $A$, es también una relación en $A$. Como $I_A \subseteq R$, $R$ es reflexiva en $A$. Para mostrar que $R$ es antisimétrica, supongamos que $xRy \wedge yRx$ y veamos que $x = y$. Si $x \neq y$, por definición de $R$ debe ser $xSy \wedge ySx$. Pero esto contradice a la asimetría de $S$. Finalmente, mostramos que $R$ es transitiva. Supongamos que $xRy \wedge yRz$. Queremos mostrar que $xRz$. Por definición de $R$ puede ser que $xSy$ o que $x = y$. Del mismo modo, $ySz$ o bien $y = z$. En total surgen así cuatro posibilidades. La primera es que $xSy \wedge ySz$. Por transitividad de $S$ se tiene entonces que $xSz$ y por ello que $xRz$. La segunda posibilidad es que $xSy \wedge y = z$. Eso significa que $xSz$ y por tanto tenemos $xRz$. La tercera posibilidad es similar. Consiste en que $x = y \wedge ySz$. Se tiene entonces que $xSz$ y con ello que $xRz$. La última posibilidad es que $x = y \wedge y = z$. En ese caso $x = z$ y como $x \in A$ tenemos que $xI_Az$ y concluimos también en este caso que $xRz$.

*3*. Sea $R$ un orden reflexivo en $A$, sea $S = R \smallsetminus I_A$ y sea $T = S \cup I_A$. Como $I_A \subseteq R$, quitar y luego añadir $I_A$ a $R$ da como resultado de nuevo $R$, esto es, $T = R$. Esto último se verifica fácilmente usando las propiedades elementales de la unión y la diferencia de conjuntos.

*4.* Sea $S$ un orden estricto en $A$, sea $R = S \cup I_A$ y $T = S \smallsetminus I_A$. En este caso $S$ es una relación disjunta de $I_A$ a la que se añade y luego se quita $I_A$. Entonces $T = (S \cup I_A) \smallsetminus I_A = (S \smallsetminus I_A) \cup (I_A \smallsetminus I_A) = S \cup \emptyset = S$.

Por último, el punto *5* se sigue de las definiciones respectivas sin mayores dificultades.

**Definición** $R$ es un *orden total reflexivo en* $A$ si $R$ es un orden parcial reflexivo en $A$ que verifica la condición $\forall xy(x \in A \wedge y \in A \rightarrow xRy \vee yRx)$. $R$ es un *orden total estricto en* $A$ si $R$ es un orden parcial estricto en $A$ que verifica la condición $\forall xy(x \in A \wedge y \in A \rightarrow xRy \vee yRx \vee x = y)$.

**Proposición 4.6** *1. Sea $R$ un orden reflexivo en $A$ y $S$ su orden estricto asociado. Entonces $R$ es un orden total en $A$ si y sólo si $S$ es un orden total en $A$.*

*2. Sea $R$ un orden reflexivo en $A$. Entonces $R$ es total si y sólo si $\breve{R}$ es total.*

*3. Sea $S$ un orden estricto en $A$. Entonces $S$ es total si y sólo si $\breve{S}$ es total.*

**Prueba**. *1.* Supongamos que $R$ es total y veamos que también es total $S$. Sean $x, y$ elementos de $A$. Como $R$ es un orden reflexivo total, tenemos que $xRy \vee yRx$. Pero $xRy$ equivale a $sSy \vee x = y$ y, similarmente, $yRx$ equivale a $ySx \vee y = x$. Tenemos por tanto que $xSy \vee x = y \vee ySx \vee y = x$, es decir, $xSy \vee x = y \vee ySx$. Ahora mostramos la otra dirección. Supongamos que $S$ es un orden estricto total y veamos que $R$ es reflexivo total. Sean $x, y$ elementos de $A$. Entonces $xSy \vee x = y \vee ySx$. Esto puede reformularse como $xSy \vee x = y \vee ySx \vee y = x$ y por tanto como $xRy \vee yRx$.

*2.* Sea $R$ un orden reflexivo. Que $R$ sea total significa que $\forall xy(x \in A \wedge y \in A \rightarrow (xRy \vee yRx))$. Obviamente esto equivale a $\forall xy(x \in A \wedge y \in A \rightarrow (y\breve{R}x \vee x\breve{R}y))$, que expresa que $\breve{R}$ sea total. De modo similar se muestra el punto *3*.

**Ejercicio 4.7** *Decidir si el siguiente enunciado es verdadero. En caso afirmativo dar una demostración y en caso negativo un contraejemplo.*

*Si $R$ y $S$ son ordenes totales estrictos, entonces $R \cap S$ es un orden total estricto.*

Es costumbre emplear la notación $\leq$ para referirse a un orden reflexivo. Si se quiere hablar de varios puede usarse $\leq'$ o $\leq_1, \leq_2, \ldots$. Para el orden estricto asociado se usa $<$. El orden inverso de $\leq$ es $\geq$ y el orden inverso de $<$ es $>$. Obsérvese que $>$ es el orden estricto asociado al orden reflexivo $\geq$. Si son órdenes en el conjunto $A$, sus relaciones para $x, y \in A$ se resumen en los siguientes puntos:

- $x < y \leftrightarrow x \leq y \wedge x \neq y$
- $x \geq y \leftrightarrow y \leq x$
- $x > y \leftrightarrow y < x$
- $x > y \leftrightarrow x \geq y \wedge x \neq y$
- $x \leq y \leftrightarrow x < y \vee x = y$

- $x \geq y \leftrightarrow y \leq x$
- $x \geq y \leftrightarrow x > y \vee x = y$.

**Definición** Sea $<$ un orden estricto en el conjunto $A$ y sea $X \subseteq A$. Decimos que $a$ es un *mínimo* de $X$ o un *menor elemento* de $X$ si $a \in X$ y $\forall x(x \in X \to a \leq x)$. Decimos que $a$ es un *máximo* de $X$ o un *mayor elemento* de $X$ si $a \in X$ y $\forall x(x \in X \to a \geq x)$.

**Lema 4.8** *Sea $<$ un orden estricto en el conjunto $A$ y sea $X \subseteq A$. Si $a$ y $b$ son mínimos de $X$, entonces $a = b$. Y si $a$ y $b$ son máximos de $X$, entonces $a = b$.*

**Prueba**. Sean $a$ y $b$ mínimos de $X$. Entonces $a \in X \wedge \forall x(x \in X \to a \leq x)$. En particular $a \leq b$ pues $b \in X$. Pero por ser $b$ mínimo $\forall x(x \in X \to b \leq x)$ y como $a \in X$ se concluye que $b \leq a$. De $a \leq b \wedge b \leq a$ se sigue entonces por anstisimetría que $a = b$.

De acuerdo con lo anterior, un conjunto tiene a lo sumo un máximo y a lo sumo un mínimo en un orden dado. Pero puede que no tenga ni máximo ni mínimo. Si $X$ tiene máximo se puede hablar de *el máximo* de $X$. Y si tiene mínimo se puede hablar de *el mínimo* de $X$. Un tipo de órdenes muy importantes en la Teoría de Conjuntos son aquellos en los que todos los conjuntos no vacíos tienen siempre mínimo (aunque no necesariamente máximo). Se trata de los buenos órdenes. Los introducimos a continuación.

**Definición** Sea $<$ un buen orden de $A$. Decimos que $<$ es un *buen orden de $A$* si todo subconjunto no vacío de $A$ tiene un menor elemento en el orden $<$.

**Observación 4.9** *Todo buen orden es un orden total.*

**Prueba**. Sea $<$ un orden estricto en $A$ y sean $a, b \in A$. Debemos mostrar que $a \leq b \vee b \leq a$. Sea $X = \{a, b\}$. $X$ es un subconjunto no vacío de $A$ y por tanto tiene un menor elemento $c \in X$. Debe ser $c = a \vee c = b$. En el caso $c = a$ tenemos $a \leq b$ y en el caso $c = b$ tenemos $b \leq a$.

Ejemplos de buenos órdenes son los órdenes totales finitos. También el orden usual de los números naturales es un buen orden. Sin embargo el orden de los enteros no lo es. Los buenos órdenes generalizan en cierto sentido el orden de los números naturales. Los números naturales se van obteniendo a partir del número cero contándolos, es decir obteniendo uno tras otro todos los números naturales con la simple aplicación del proceso de formar *el siguiente a* un número ya obtenido. Este proceso de contar puede generalizarse iterándolo en el infinito si se permite formar *el siguiente a* una colección de números ya formada. Así surgen los *números ordinales*.

La cuestión de si los elementos de cualquier conjunto pueden contarse de esta manera es la cuestión de si todo conjunto puede ordenarse mediante un buen orden. El *Principio del Buen Orden* es el enunciado que afirma que todo conjunto posee un buen orden, es decir, que para cada conjunto $A$ existe una relación $<$ que es un buen orden de $A$. Este principio no puede demostrarse ni refutarse a no ser que la Teoría de Conjuntos resulte ser contradictoria, en cuyo caso todo lo demuestra y todo lo refuta. Usualmente se añade a la lista de axiomas de ZF obteniendo con él el sistema axiomático ZFC. Pero también tiene mucho interés la cuestión de qué resultados pueden establecerse en ZF sin necesidad de usar este principio.

**Definición** Sea $<$ un orden parcial estricto en el conjunto $A$ y sea $X$ un subconjunto de $A$. Se dice que $a$ es un *elemento minimal* de $X$ si es un elemento de $X$ y no hay ningún elemento de $X$ menor que él, es decir, si $a \in X \wedge \neg \exists x(x \in X \wedge x < a)$. Similarmente se dice que $a$ es un *elemento maximal* de $X$ si es un elemento de $X$ y no hay ningún elemento de $X$ mayor que él, es decir, si $a \in X \wedge \neg \exists x(x \in X \wedge x > a)$.

A diferencia de lo que ocurre con máximos y mínimos, un conjunto puede tener varios elementos maximales y varios minimales. También puede ser que no tenga ninguno. La importancia de los maximales y minimales surge cuando los órdenes no son totales pues en el caso de los órdenes totales son lo mismo que máximos y mínimos.

**Observaciones 4.10** *Sea $<$ un orden estricto del conjunto $A$ y sea $X \subseteq A$.*

1. *Si $a$ es un máximo de $X$, $a$ es un elemento maximal de $X$. Si $a$ es un mínimo de $X$ entonces $a$ es un elemento minimal de $X$.*
2. *Si $<$ es un orden total, entonces los elementos maximales de $X$ son máximos de $X$ y los elementos minimales de $X$ son mínimos de $X$.*

**Ejercicio 4.11** *Sea $<$ un orden estricto de $A$ y sea $X \subseteq A$. El orden inverso es entonces $>$.*

1. *$a$ es un máximo de $X$ en $<$ si y sólo si $a$ es un mínimo de $X$ en $>$.*
2. *$a$ es un maximal de $X$ en $<$ si y sólo si $a$ es un minimal de $X$ en $>$.*

**Definición** Sea $<$ un orden estricto de $A$ y sea $X \subseteq A$. Decimos que $a$ es una *cota superior* de $X$ si $a$ es un elemento de $A$ que es mayor o igual que todos los elementos de $X$, esto es, $a \in A \wedge \forall x(x \in X \rightarrow x \leq a)$. Se dice que $a$ es una *cota superior estricta* de $X$ si $a$ es un elemento de $A$ que es mayor que todos los elementos de $X$, esto es, $a \in A \wedge \forall x(x \in X \rightarrow x < a)$. Las cotas inferiores y las cotas inferiores estrictas se definen de modo parecido. Se dice que $a$ es una *cota inferior* de $X$ si $a$ es un elemento de $A$ que es menor o igual que todos los elementos de $X$, es decir, $a \in A \wedge \forall x(x \in X \rightarrow a \leq x)$. Finalmente, $a$ es una *cota inferior estricta* de $X$ si $a$ es un elemento de $A$ que es menor que todos los elementos de $X$, esto es, $a \in A \wedge \forall x(x \in X \rightarrow a < x)$.

**Observaciones 4.12** *Sea $<$ un orden estricto del conjunto $A$ y sea $X \subseteq A$.*

1. *$a$ es una cota superior estricta de $X$ si y sólo si $a$ es una cota superior de $X$ y $a \notin X$. Similarmente, $a$ es una cota inferior estricta de $X$ si y sólo si $a$ es una cota inferior de $X$ y $a \notin X$.*
2. *$a$ es una cota superior de $X$ en $<$ si y sólo si $a$ es una cota inferior de $X$ en el orden inverso $>$. Lo mismo ocurre con las cotas estrictas.*

*3. Si $a$ es un máximo de $X$, $a$ es una cota superior de $X$. Y si $a$ es un mínimo de $X$, $a$ es una cota inferior de $X$.*

*4. Si $a$ es una cota superior de $X$ y $a \in X$, entonces $a$ es un máximo de $X$. Y si $a$ es una cota inferior de $X$ y $a \in X$, entonces $a$ es un mínimo de $X$.*

Un conjunto $X$ puede tener varias cotas superiores e inferiores, incluso en un orden total. También puede que no tenga ninguna. En ocasiones existe una menor cota superior. Se llama supremo. Y si hay una menor cota inferior se llama ínfimo. Lo definimos a continuación.

**Definición** Sea $<$ un orden estricto del conjunto $A$ y sea $X \subseteq A$. Si el conjunto formado por las cotas superiores de $X$ tiene un menor elemento, lo llamamos *supremo* de $X$. Se designa con $\sup X$. Y si el conjunto de las cotas inferiores de $X$ tiene un mayor elemento, se le llama *ínfimo* de $X$ y se designa con $\inf X$.

**Observaciones 4.13** *Sea $<$ un orden estricto del conjunto $A$ y sea $X \subseteq A$.*

*1. $a$ es supremo de $X$ en $<$ si y sólo si $a$ es ínfimo de $X$ en el orden inverso $>$.*

*2. Si $X$ tiene un máximo, el máximo de $X$ es supremo de $X$. Si $X$ tiene un mínimo, el mínimo de $X$ es ínfimo de $X$.*

*3. Si $X$ tiene supremo pero no tiene máximo, el supremo de $X$ es una cota superior estricta de $X$. Si $X$ tiene ínfimo pero no tiene mínimo, el ínfimo de $X$ es una cota inferior estricta de $X$.*

*4. Si $X$ tiene supremo y $\sup X \in X$, entonces $\sup X$ es el máximo de $X$. Si $X$ tiene ínfimo y $\inf X \in X$, entonces $\inf X$ es el mínimo de $X$.*

**Ejercicio 4.14** *Sea $A$ un conjunto arbitrario. Consideramos el orden de la inclusión entre subconjuntos de $A$.*

*1. Si $X, Y$ son subconjuntos de $A$, $X \cup Y$ es el supremo de $\{X, Y\}$ y $X \cap Y$ es su ínfimo.*

*2. Si $\Phi$ es una colección de subconjuntos de $X$, $\bigcup \Phi$ es el supremo de $\Phi$. Y si $\Phi \neq \emptyset$, $\cap \Phi$ es su ínfimo.*

**Definición** *Sea $<$ un orden estricto del conjunto $A$ y sea $X \subseteq A$. Se dice que $X$ es una* cadena *(respecto al orden $<$) si los elementos de $X$ están totalmente ordenados por $<$, es decir, si para cualesquiera $x, y$ elementos de $X$, $x \leq y \vee y \leq x$. Esto no significa que $<$ tenga que ser un orden total de $A$. Pero si lo es, todo subconjunto de $A$ es una cadena.*

El *Lema de Zorn* es el siguiente enunciado: si $<$ es un orden estricto del conjunto $A$ en el que toda cadena tiene una cota superior, entonces $A$ tiene un elemento maximal. El Lema de Zorn tiene el mismo estatus que el Principio del Buen Orden. De hecho se puede demostrar en ZF uno a partir del otro. Por tanto es un lema en ZFC pero no en ZF (si ZF no es contradictoria). Es un principio que se utiliza a menudo en Lógica.

Finalizamos este capítulo enunciando sin demostración una serie de hechos importantes que tratan de las ordenaciones habituales de los números naturales, enteros, racionales y reales.

Se dice que un orden total es *denso* si entre cualesquiera dos elementos siempre hay otro. Es decir, el orden total $<$ en el conjunto $A$ es un orden denso si

$$\forall xy(x < y \rightarrow \exists z(z < z \wedge z < y)).$$

El orden de los números racionales es un orden denso pero también es denso el de los números reales. Por el contrario, no son densos ni el orden de los números naturales ni el orden de los números enteros. De hecho, el orden de los números racionales queda caracterizado por los siguientes puntos:

1. Es un orden total denso.
2. No tiene ni mayor ni menor elemento.
3. El conjunto en el que se define el orden tiene el mismo tamaño que el conjunto de los números naturales.

Técnicamente este tipo de caracterizaciones se denominan caracterizaciones salvo isomorfía, pero la noción de isomorfismo no ha sido introducida todavía. Para caracterizar de modo similar el orden de los números reales, necesitamos la noción de que un conjunto sea denso en otro (respecto a un orden). Sea $<$ un orden total de $A$ y sea $X \subseteq A$. Se dice que $X$ es denso en $A$ si entre cada dos elementos de $A$ hay un elemento de $X$, esto es,

$$\forall xy(x < y \rightarrow \exists z(z \in X \wedge x < z \wedge z < y)).$$

Entonces el orden total $<$ de $A$ es denso precisamente cuando $A$ es un subconjunto de $A$ que es denso en $A$. El orden de los números reales se caracteriza por lo siguiente:

1. Es un orden total que posee un subconjunto denso del tamaño del conjunto de los números naturales.
2. No tiene ni mayor ni menor elemento.
3. Todo conjunto con cota superior tiene supremo.

Los órdenes de los números naturales y de los números enteros pueden caracterizarse de diversas maneras. Es mejor introducir algo más de terminología primero. Sea $<$ un orden estricto en $A$ y sea $a \in A$. Los *predecesores* de $a$ en $<$ son los elementos menores que $a$ y los *sucesores* son los elementos mayores que $a$. Se dice que $b$ es *sucesor inmediato* de $a$ si es un sucesor de $b$ y no hay nadie entre ellos, esto es, si

$$a < b \wedge \neg\exists x(a < x \wedge x < b).$$

Esta situación también se describe diciendo que $a$ es un *predecesor inmediato* de $b$. En un orden denso ningún elemento puede tener sucesores inmediatos ni predecesores inmediatos. La situación completamente opuesta es la de un *orden discreto*. Un orden discreto es un orden total en el que todo elemento con sucesores tiene un sucesor inmediato y todo elemento con predecesores tiene un predecesor inmediato.

Los órdenes finitos son siempre discretos. El orden de los números naturales es el único buen orden discreto infinito. El orden de los enteros es discreto y es, en un cierto sentido, el menor orden discreto infinito que no tiene ni mayor ni menor elemento.

Sea $<$ un orden total del conjunto $A$. Un *segmento inicial de* $<$ es un subconjunto $X$ de $A$ con la propiedad de contener a los elementos que son menores que algún elemento de $X$, es decir, con la propiedad de que

$$\forall xy(x \in X \wedge y < x \rightarrow y \in X).$$

Por ejemplo $A$ mismo es un segmento inicial. Pero también el conjunto de predecesores de un elemento de $A$ es un segmento inicial. Se dice que un segmento inicial es propio si no es precisamente todo el conjunto $A$. Un *intervalo* de $A$ es un subconjunto de $A$ formado por los objetos comprendidos entre dos elementos de $A$. Puede ser de alguna de las cuatro formas siguientes: $\{x : a \leq x \wedge x \leq b\}$, $\{x : a < x \wedge x \leq b\}$, $\{x : a \leq x \wedge x < b\}$ o $\{x : a < x \wedge x < b\}$, donde en todos los casos $a, b$ son elementos de $A$.

El orden de los números naturales puede entonces caracterizarse como el único orden total infinito en el que todo segmento inicial propio es finito. Por su parte, el orden de los enteros es el único orden infinito sin mayor ni menor elemento en el que todo intervalo es finito.

# Capítulo 5

# Funciones

Las funciones son procedimientos o reglas para asignar elementos de un conjunto a elementos de un conjunto. Pueden representarse como cierto tipo de relaciones y esto es lo que habitualmente se hace.

**Definición** Una relación $R$ es una *función* si $R$ es unívoca en el siguiente sentido:

$$\forall xyz(xRy \wedge xRz \rightarrow y = z).$$

Usamos las letras $f, g, h, \ldots$ como variables de funciones. Decimos que $f$ es una *función de $A$ en $B$* o una *aplicación de $A$ en $B$* y escribimos $f : A \rightarrow B$ si $f$ es una función, $\operatorname{dom} f = A$ y $\operatorname{rec} f \subseteq B$.

**Observaciones 5.1** *1. Si $f : A \rightarrow B$ y $B \subseteq C$, entonces $f : A \rightarrow C$.*

*2. Si $f$ es una función, entonces $f : \operatorname{dom} f \rightarrow \operatorname{rec} f$.*

*3. $\emptyset : \emptyset \rightarrow B$ para cualquier $B$.*

*4. $I_A : A \rightarrow A$.*

**Ejercicio 5.2** *Mostrar los siguientes enunciados:*

1. *Si $f$ es una función y $g \subseteq f$, también $g$ es una función. Por tanto, la intersección de funciones es una función.*
2. *Si $f, g$ son funciones y $\operatorname{dom} f \cap \operatorname{dom} g = \emptyset$, entonces $f \cup g$ es una función.*

**Definición** Sea $f$ una función. Los *argumentos de $f$* son los elementos del dominio de $f$. Si $a$ es un argumento de $f$, entonces hay un único $b$ tal que $\langle a, b\rangle \in f$. Este único $b$ asociado a $a$ se llama *valor de $a$ en $f$* y se designa con $f(a)$.

**Observaciones 5.3** *Sea $f$ una función.*

1. $\langle a, f(a)\rangle \in f$ *para cada* $a \in \operatorname{dom} f$.

2. *Si* $\langle a, b\rangle \in f$, *entonces* $a$ *es argumento de* $f$ *y* $f(a) = b$.

3. $\operatorname{rec} f = \{f(a) : a \in \operatorname{dom} f\}$.

4. *Si* $f : A \to B$ *y* $a \in A$, *entonces* $f(a) \in B$.

**Prueba**. Los puntos *1* y *2* son una consecuencia inmediata de la definición de $f(a)$ como el único $b$ tal que $\langle a, b\rangle \in f$.

*3*. Si $a \in \operatorname{dom} f$, sabemos que $\langle a, f(a)\rangle \in f$, de modo que $f(a) \in \operatorname{rec} f$. Esto muestra que $\{f(a) : a \in \operatorname{dom} f\} \subseteq \operatorname{rec} f$. Mostramos ahora que $\operatorname{rec} f \subseteq \{f(a) : a \in \operatorname{dom} f\}$. Sea $b \in \operatorname{rec} f$. Entonces hay $x$ tal que $\langle x, b\rangle \in f$. En ese caso $x \in \operatorname{dom} f$ y $f(x) = b$. Por tanto $b \in \{f(a) : a \in \operatorname{dom} f\}$.

*4*. Sea $f : A \to B$ y $a \in A$. Entonces $f(a) \in \operatorname{rec} f$ y $\operatorname{rec} f \subseteq B$, de modo que $f(a) \in B$.

El siguiente resultado es una versión del Axioma de Extensionalidad para funciones.

**Proposición 5.4** 1. *Si* $f, g$ *son funciones con* $\operatorname{dom} f = \operatorname{dom} g$ *y para cada* $a \in \operatorname{dom} f$, $f(a) = g(a)$, *entonces* $f = g$.

2. *Si* $f : A \to B$ *y* $g : A \to C$ *y para cada* $a \in A$, $f(a) = g(a)$, *entonces* $f = g$.

**Prueba**. Sean $f, g$ funciones con el mismo dominio y supongamos que para cada $a \in \operatorname{dom} f$, $f(a) = g(a)$. Vemos que $f \subseteq g$. Sea $\langle a, b\rangle \in f$. Entonces $a \in \operatorname{dom} f$ y $b = f(a)$. Por la hipótesis $a \in \operatorname{dom} g$ y $b = g(a)$. Entonces $\langle a, b\rangle \in g$. Análogamente se muestra que $g \subseteq f$. La segunda parte se sigue inmediatamente de la primera.

Las funciones son relaciones y por tanto pueden darse explicitando qué pares las forman. Pero otra manera usual de presentar las funciones es indicando sus dominios e indicando una regla que permite obtener los valores de los argumentos. Esto debe ser coherente, es decir, para definir una función de $A$ en $B$ de esta manera, la regla debe poder ser aplicada a los elementos de $A$, debe dar un único valor para cada uno de esos argumentos y ese valor debe ser elemento del conjunto $B$. Por ejemplo, se define una función $f$ de $A$ en $\mathcal{P}(A)$ asignando a cada $a \in A$ su conjunto unitario $\{a\}$. En ese caso se escribe

$$f : A \to \mathcal{P}(A)$$

$$f(a) = \{a\}$$

En vez de $f(a) = \{a\}$, se pone a veces simplemente $a \mapsto \{a\}$.

Sea $\Phi$ una colección de conjuntos no vacíos. Una *función de elección para* $\Phi$ es una función $f$ con dominio $\Phi$ y tal que para cada $X \in \Phi$, $f(X) \in X$. El *Axioma de Elección* afirma que para cada colección de conjuntos no vacíos existe una función de elección. En ZF el Axioma de Elección es equivalente al Principio del Buen Orden. Por tanto también es equivalente al Lema de Zorn. La manera habitual de presentar la teoría ZFC es precisamente como el resultado de agregar a ZF el Axioma de Elección (abreviado AC).

**Definición** Sean $X$ e $Y$ conjuntos. El conjunto formado por todas las funciones de $X$ en $Y$ se designa con ${}^XY$. Esto es

$${}^XY = \{f : \ f : X \to Y\}.$$

**Observaciones 5.5** *1.* ${}^{\emptyset}X = \{\emptyset\}$

*2.* *Si* $X \neq \emptyset$, *entonces* ${}^X\emptyset = \emptyset$

**Prueba**. *1*. Hay que mostrar que la única función que existe de $\emptyset$ en $X$ es la función vacía. Claramente $\emptyset : \emptyset \to X$. Por otro lado, si $f : \emptyset \to X$, entonces $\operatorname{dom} f = \emptyset$, de modo que $f = \emptyset$.

*2*. Sea $X \neq \emptyset$. Hay entonces un $a$ tal que $a \in X$. Debemos mostrar que no hay ninguna función de $X$ en $\emptyset$. Supongamos lo contrario y sea $f : X \to X$. Como $a \in X$ resulta entonces que $f(a) \in \emptyset$, lo cual es imposible.

**Definición** Una función $f$ es *inyectiva* si su inversa $\breve{f}$ es también una función, es decir, si

$$\forall xyz(\langle x, z\rangle \in f \wedge \langle y, z\rangle \in f \to x = y).$$

También se dice entonces que $f$ es una función *uno a uno*. Para indicar que $f$ es una función inyectiva de $A$ en $B$ se escribe a veces $f : A \overset{1-1}{\to} B$.

**Observaciones 5.6** *1.* $f$ *es inyectiva si y sólo si* $\forall xy(x \in \operatorname{dom} f \wedge y \in \operatorname{dom} f \wedge f(x) = f(y) \to x = y)$.

*2.* $f$ *es inyectiva si y sólo si* $\forall xy(x \in \operatorname{dom} f \wedge y \in \operatorname{dom} f \wedge x \neq y \to f(x) \neq f(y))$.

*3.* *Si* $f$ *es inyectiva, entonces* $\breve{f}$ *no sólo es una función sino que además es una función inyectiva.*

*4.* $\emptyset$ *es una función inyectiva.*

*5.* $I_A$ *es una función inyectiva.*

**Prueba**. *1*. Sea $f$ inyectiva y supongamos que $x \in \operatorname{dom} f \wedge y \in \operatorname{dom} f \wedge f(x) = f(y)$. Entonces $\langle x, f(x)\rangle \in f \wedge \langle y, f(x)\rangle \in f$ y por ser $f$ inyectiva $x = y$. Mostramos ahora que $f$ es inyectiva suponiendo que se cumple la condición de la derecha. Sea $\langle x, z\rangle \in f \wedge \langle y, z\rangle \in f$ y veamos que $x = y$. Sabemos que $f(x) = z$ y que $f(y) = z$. Por tanto $f(x) = f(y)$ y aplicando la hipótesis obtenemos que $x = y$.

El punto *2* es simplemente una reformulación de *1* dado que la condición $(x \in \operatorname{dom} f \wedge y \in \operatorname{dom} f \wedge f(x) = f(y) \to x = y)$ es equivalente a $(x \in \operatorname{dom} f \wedge y \in \operatorname{dom} f \wedge x \neq y \to f(x) \neq f(y))$.

*3*. Sea $f$ inyectiva. Mostramos que $\breve{f}$ también lo es. Supongamos para ello que $\langle x, z\rangle \in \breve{f} \wedge \langle y, z\rangle \in \breve{f}$ y veamos que $y = z$. Tenemos que $\langle z, x\rangle \in f \wedge \langle z, y\rangle \in f$. Usando simplemente el hecho de que $f$ es una función concluimos que $x = y$.

*4*. Como muchas otras propiedades del conjunto vacío, se establece mostrando que su negación lleva a la contradicción de que el vacío tiene elementos. Finalmente el punto *5* se verifica con mucha facilidad analizando la definición de $I_A$.

**Ejercicio 5.7** *Consideremos las siguientes funciones.*

1. $f_1 : A \to \mathcal{P}(A)$ *la función definida por* $a \mapsto \{a\}$,
2. $f_2 : \mathcal{P}(A) \times \mathcal{P}(A) \to \mathcal{P}(A)$ *la función definida por* $\langle X, Y \rangle \mapsto X \cap Y$,
3. $f_3 : \mathcal{P}(A) \times \mathcal{P}(A) \to \mathcal{P}(A)$ *la función definida por* $\langle X, Y \rangle \mapsto X \cup Y$,
4. $f_4 : \mathcal{P}(A) \times \mathcal{P}(A) \to \mathcal{P}(A)$ *la función definida por* $\langle X, Y \rangle \mapsto X \setminus Y$,
5. $f_5 : \mathcal{P}(A) \to \mathcal{P}(A)$ *la función definida por* $X \mapsto A \setminus X$,
6. $f_6 : \mathbb{Z} \to \mathbb{Z}$ *la función definida por* $n \mapsto -n$,
7. $f_7 : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *la función definida por* $\langle n, m \rangle \mapsto n + m$,
8. $f_8 : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *la función definida por* $\langle n, m \rangle \mapsto n \cdot m$,
9. $f_9 : A \times A \to A$ *la función definida por* $\langle x, y \rangle \mapsto x$,
10. $f_{10} : A \to A \times A$ *la función definida por* $x \mapsto \langle x, x \rangle$,
11. $f_{11} : A \times A \to A \times A$ *la función definida por* $\langle x, y \rangle \mapsto \langle y, x \rangle$.

*Indicar cuáles de estas funciones son inyectivas y cuáles no.*

**Definición** Sea $f$ una función inyectiva. Sabemos que $\breve{f}$ es también una función inyectiva. Es usual usar la notación $f^{-1}$ en vez de $\breve{f}$ en estas circunstancias. Obsérvese que $\breve{f}$ está definida siempre (es una relación) pero $f^{-1}$ sólo está definida cuando $f$ es inyectiva. Claro está, $\operatorname{dom} f^{-1} = \operatorname{rec} f$, $\operatorname{rec} f^{-1} = \operatorname{dom} f$ y para cada $a, b$ $f(a) = b$ si y sólo si $f^{-1}(b) = a$.

**Observaciones 5.8** *Sea $f$ una función inyectiva.*

1. $(f^{-1})^{-1} = f$.
2. *Para cada* $x \in \operatorname{dom} f$, $f^{-1}(f(x)) = x$.
3. *Para cada* $x \in \operatorname{rec} f$, $f(f^{-1}(x)) = x$.

**Prueba**. El punto *1* se sigue de la correspondiente propiedad de la inversión de relaciones: $(\breve{f})\breve{} = f$. Mostramos ahora *2*. Sea $x \in \operatorname{dom} f$. Entonces $\langle x, f(x) \rangle \in f$, con lo cual $\langle f(x), x \rangle \in f^{-1}$, y esto muestra que $f(x) \in \operatorname{dom} f^{-1} \wedge f^{-1}(f(x)) = x$. Finalmente, *3* tiene una prueba similar. Supongamos que $x \in \operatorname{rec} f$. Entonces $x \in \operatorname{dom} f^{-1}$, de manera que $\langle x, f^{-1}(x) \rangle \in f^{-1}$. Entonces $\langle f^{-1}(x), x \rangle \in f$. En ese caso $f^{-1}(x) \in \operatorname{dom} f$ y $f(f^{-1}(x)) = x$.

**Definición** Se dice que $f$ es una función *exhaustiva* o *suprayectiva* de $A$ en $B$, o también que $f$ es una *función de $A$ sobre $B$* si $f : A \to B$ y $\operatorname{rec} f = B$. Se dice que $f$ es una *función biyectiva* de $A$ en $B$ o una *biyección* de $A$ en $B$ si $f$ es una función inyectiva y exhaustiva de $A$ en $B$.

**Ejercicio 5.9** *Decir de cada una de las funciones del ejercicio 5.7 si es exhaustiva y si es biyectiva.*

**Observaciones 5.10**
1. *Si $f$ es una función, $f$ es una función exhaustiva de* $\operatorname{dom} f$ *en* $\operatorname{rec} f$.
2. *Si $f$ es una función inyectiva, $f$ es una función biyectiva de* $\operatorname{dom} f$ *en* $\operatorname{rec} f$.
3. *$\emptyset$ es una biyección de $\emptyset$ en $\emptyset$.*
4. *$I_A$ es una biyección de $A$ en $A$.*
5. *Si $f$ es una biyección de $A$ en $B$, entonces $f^{-1}$ es una biyección de $B$ en $A$.*

**Definición** Sean $f$ y $g$ funciones. Entonces también $f \mid g$ es una función. Es costumbre usar la notación $g \circ f$ para referirse a $f \mid g$ en esta situación. Como en el caso de las relaciones, $f \circ (g \circ h) = (f \circ g) \circ h$ y si $f, g$ son inyectivas $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$. El cambio de orden en la notación se explica por la siguiente proposición.

**Proposición 5.11** *Si $f : A \to B$ y $g : B \to C$, entonces $g \circ f : A \to C$. Además para cada $a \in A$, $g \circ f(a) = g(f(a))$.*

**Prueba**. Por los resultados de 3.11 ya sabemos que $\operatorname{dom} g \circ f = A$ y que $\operatorname{rec} g \circ f \subseteq C$. Sea $a \in A$ y veamos que $g \circ f(a) = g(f(a))$. Como $a \in \operatorname{dom} f$, $\langle a, f(a) \rangle \in f$. Entonces $f(a) \in \operatorname{dom} g$, con lo cual $\langle f(a), g(f(a)) \rangle \in g$. Por definición de composición de relaciones $\langle a, g(f(a)) \rangle \in f \mid g$, esto es $\langle a, g(f(a)) \rangle \in g \circ f$. En ese caso $g(f(a)) = g \circ f(a)$.

**Proposición 5.12**
1. *Si $f$ y $g$ son funciones inyectivas, $g \circ f$ es una función inyectiva.*
2. *Si $f : A \to B$ es exhaustiva y $g : B \to C$ es exhaustiva, entonces $g \circ f : A \to C$ es exhaustiva.*
3. *Si $f : A \to B$ es biyectiva y $g : B \to C$ es biyectiva, entonces $g \circ f : A \to C$ es biyectiva.*

**Prueba**. Obviamente *3* se sigue de *1* y *2*. Mostramos primero *1*. Sean $f$ y $g$ inyectivas. Para mostrar que $g \circ f$ también lo es supongamos que $x, y$ pertenecen al dominio de $g \circ f$ y que $g \circ f(x) = g \circ f(y)$ y veamos que $x = y$. Por definición de composición $g(f(x)) = g(f(y))$. Observemos que $\operatorname{dom}(g \circ f) \subseteq \operatorname{dom} f$ con lo cual $x, y$ son elementos de $\operatorname{dom} f$ y además $f(x), f(y)$ son elementos de $\operatorname{dom} g$. Como $g$ es inyectiva, $f(x) = f(y)$ y como $f$ es inyectiva, $x = y$.

Finalizamos estableciendo el punto *3*. Sean $f : A \to B$ y $g : B \to C$ exhaustivas. Supongamos que $x \in C$ y veamos que $x \in \operatorname{rec}(g \circ f)$. Como $g$ es exhaustiva existe un $b \in B$ tal que $g(b) = x$. Y como $f$ es exhaustiva hay un $a \in A$ tal que $f(a) = b$. Entonces $x = g(f(a)) = g \circ f(a)$, con lo cual $x \in \operatorname{rec}(g \circ f)$.

**Ejercicio 5.13** *Demostrar que si $f : A \to B$ y $g : B \to C$ y $g \circ f : A \to C$ es biyectiva, entonces $f$ es exhaustiva y $g$ es inyectiva.*

**Ejercicio 5.14** *Con las funciones del ejercicio 5.7, calcular $f_5 \circ f_1$, $f_5 \circ f_2$, $f_1 \circ f_9$, $f_{10} \circ f_9$, $f_6 \circ f_7$, $f_6 \circ f_8$, $f_9 \circ f_{10}$, $f_{11} \circ f_{10}$, $f_9 \circ f_{11}$.*

**Proposición 5.15** *1. Si $f : A \to B$, entonces $I_B \circ f = f = f \circ I_A$.*

*2. Si $f : A \to B$ es biyectiva, entonces $f^{-1} \circ f = I_A$ y $f \circ f^{-1} = I_B$.*

**Prueba**. *1.* Sea $g = I_B \circ f$. Como $I_B : B \to B$, tenemos que $g : A \to B$. Además para cada $a \in A$, $g(a) = I_B \circ f(a) = I_B(f(a)) = f(a)$. Esto muestra que $g = f$, es decir, que $I_B \circ f = f$. La prueba de que $f \circ I_A = f$ es similar.

*2*. Supongamos que $f : A \to B$ es biyectiva. Entonces $f^{-1} : B \to A$ es también biyectiva. La composición $f^{-1} \circ f$ es una función de $A$ en $A$. Si $a \in A$, entonces $f^{-1} \circ f(a) = f^{-1}(f(a)) = a = I_A(a)$. Por tanto $f^{-1} \circ f = I_A$. Similarmente se ve que $f \circ f^{-1} = I_B$.

**Definición** Sea $f$ una función y $X$ un conjunto arbitrario. Definimos la *restricción de $f$ a $X$* como la función

$$f \restriction X = \{\langle x, y\rangle : \langle x, y\rangle \in f \wedge x \in X\}.$$

Obsérvese que si $f : A \to B$ y $X \subseteq A$, entonces $f \restriction X : X \to B$ y para cada $a \in X$, $f \restriction X(a) = f(a)$. Por otro lado, normalmente se puede suponer que $X \subseteq \operatorname{dom} f$, pues si $X' = X \cap \operatorname{dom} f$, resulta que $X' \subseteq \operatorname{dom} f$ y $f \restriction X = f \restriction X'$.

**Observaciones 5.16** *1. $f \restriction \emptyset = \emptyset$.*

*2. $f \restriction \operatorname{dom} f = f$.*

*3. Si $X \subseteq A$, entonces $I_A \restriction X = I_X$.*

**Definición** Sea $f$ una función y $X$ un conjunto arbitrario. Se define la *imagen de $X$ en $f$* como el conjunto $f[X] = \operatorname{rec}(f \restriction X)$, es decir, $f[X] = \{y : \exists x(x \in X \wedge \langle x, y\rangle \in f)\}$. Si $X \subseteq \operatorname{dom} f$ resulta que $f[X] = \{f(a) : a \in X\}$. Normalmente se puede suponer que $X \subseteq \operatorname{dom} f$, pues si $X' = X \cap \operatorname{dom} f$, resulta que $f[X] = f[X']$ y $X' \subseteq \operatorname{dom} f$.

**Observaciones 5.17** *1. $f[\emptyset] = \emptyset$.*

*2. $f[\operatorname{dom} f] = \operatorname{rec} f$.*

*3. Si $X \subseteq A$, entonces $I_A[X] = X$.*

*4. Si $X \subseteq Y$, entonces $f[X] \subseteq f[Y]$.*

*5. Si $a \in \operatorname{dom} f$, entonces $\{f(a)\} = f[\{a\}]$.*

**Ejercicio 5.18** *Decidir si los siguientes enunciados son verdaderos. En caso afirmativo dar una demostración y en caso negativo un contraejemplo. Considerar después las mismas preguntas en el caso de que $f$ sea una función inyectiva.*

1. $f[X \cup Y] = f[X] \cup f[Y]$
2. $f[X \cap Y] = f[X] \cap f[Y]$
3. $f[X \setminus Y] = f[X] \setminus f[Y]$

**Definición** Sea $f$ una función y $X$ un conjunto arbitrario. Se define la *imagen inversa de $X$ en $f$* como el conjunto $f^{-1}[X] = \{a : a \in \operatorname{dom} f \wedge f(a) \in X\}$. La función $f$ puede no ser inyectiva. Cuando $f$ es inyectiva, la notación $f^{-1}[X]$ puede entenderse en dos sentidos: como la imagen inversa de $X$ en $f$ y como la imagen de $X$ en $f^{-1}$. Es fácil ver que sin embargo el conjunto así definido es el mismo.

**Observaciones 5.19** *1.* $f^{-1}[\emptyset] = \emptyset$.

2. $f^{-1}[\operatorname{rec} f] = \operatorname{dom} f$.
3. *Si $Y \subseteq A$, entonces $I_A^{-1}[Y] = Y$.*
4. *Si $X \subseteq Y$, entonces $f^{-1}[X] \subseteq f^{-1}[Y]$.*
5. $f^{-1}[X \cup Y] = f^{-1}[X] \cup f^{-1}[Y]$.
6. $f^{-1}[X \cap Y] = f^{-1}[X] \cap f^{-1}[Y]$.
7. $f^{-1}[X \setminus Y] = f^{-1}[X] \setminus f^{-1}[Y]$.
8. *Si $X \subseteq \operatorname{dom} f$, entonces $X \subseteq f^{-1}[f[X]]$.*
9. *Si $Y \subseteq \operatorname{rec} f$, entonces $f[f^{-1}[Y]] = Y$.*

**Prueba**. *1*. $f^{-1}[\emptyset] = \{a : a \in \operatorname{dom} f \wedge f(a) \in \emptyset\} = \emptyset$ ya que la condición $f(a) \in \emptyset$ no puede cumplirla ningún objeto.

*2*. Por definición ya es claro que $f^{-1}[\operatorname{rec} f] \subseteq \operatorname{dom} f$. Para mostrar la otra inclusión observemos que si $a \in \operatorname{dom} f$ entonces $f(a) \in \operatorname{rec} f$ por lo cual $a \in f^{-1}[\operatorname{rec} f]$.

*3*. Sea $Y \subseteq A$. Entonces $I_A^{-1}[Y] = \{a : a \in A \wedge I_A(a) \in Y\} = \{a : a \in A \wedge a \in Y\} = A \cap Y = Y$.

*4*. Sea $X \subseteq Y$, supongamos que $a \in f^{-1}[X]$ y veamos que $a \in f^{-1}[Y]$. Sabemos que $a \in \operatorname{dom} f \wedge f(a) \in X$. Como $X \subseteq Y$, $f(a) \in Y$ y por tanto $a$ cumple las condiciones necesarias para pertenecer a $f^{-1}[Y]$.

*5*. Se obtiene de las siguientes equivalencias

$$\begin{array}{rcl} a \in f^{-1}[X \cup Y] & \leftrightarrow & a \in \operatorname{dom} f \wedge f(a) \in X \cup Y \\ & \leftrightarrow & a \in \operatorname{dom} f \wedge (f(a) \in X \vee f(a) \in Y) \\ & \leftrightarrow & (a \in \operatorname{dom} f \wedge f(a) \in X) \vee (a \in \operatorname{dom} f \wedge f(a) \in Y) \\ & \leftrightarrow & a \in f^{-1}[X] \vee a \in f^{-1}[Y] \\ & \leftrightarrow & a \in f^{-1}[X] \cup f^{-1}[Y] \end{array}$$

*6*. Se obtiene de las siguientes equivalencias

$$
\begin{aligned}
a \in f^{-1}[X \cap Y] &\leftrightarrow a \in \operatorname{dom} f \wedge f(a) \in X \cap Y \\
&\leftrightarrow a \in \operatorname{dom} f \wedge f(a) \in X \wedge f(a) \in Y \\
&\leftrightarrow (a \in \operatorname{dom} f \wedge f(a) \in X) \wedge (a \in \operatorname{dom} f \wedge f(a) \in Y) \\
&\leftrightarrow a \in f^{-1}[X] \wedge a \in f^{-1}[Y] \\
&\leftrightarrow a \in f^{-1}[X] \cap f^{-1}[Y]
\end{aligned}
$$

*7*. Se obtiene de las siguientes equivalencias

$$
\begin{aligned}
a \in f^{-1}[X \setminus Y] &\leftrightarrow a \in \operatorname{dom} f \wedge f(a) \in X \setminus Y \\
&\leftrightarrow a \in \operatorname{dom} f \wedge f(a) \in X \wedge f(a) \notin Y \\
&\leftrightarrow a \in f^{-1}[X] \wedge a \notin f^{-1}[Y] \\
&\leftrightarrow a \in f^{-1}[X] \setminus f^{-1}[Y]
\end{aligned}
$$

*8*. Sea $X \subseteq \operatorname{dom} f$, sea $a \in X$ y veamos que $a \in f^{-1}[f[X]]$. Como $a \in X$ y $X \subseteq \operatorname{dom} f$, $f(a) \in f[X]$. Entonces $a \in \operatorname{dom} f \wedge f(a) \in f[X]$, de manera que $a \in f^{-1}[f[X]]$.

*9*. Sea $Y \subseteq \operatorname{rec} f$. Vemos primero que $f[f^{-1}[Y]] \subseteq Y$. Sea $a \in f[f^{-1}[Y]]$. Entonces hay $x$ tal que $x \in \operatorname{dom} f \wedge x \in f^{-1}[Y] \wedge f(x) = a$. Como $x \in f^{-1}[Y]$, debe ser $f(x) \in Y$, esto es $a \in Y$. Ahora mostramos que $Y \subseteq f[f^{-1}[Y]]$. Sea $a \in Y$. Como $Y \subseteq \operatorname{rec} f$, hay un $x \in \operatorname{dom} f$ tal que $f(x) = a$. Como $f(x) \in Y$, $x \in f^{-1}[Y]$. Entonces $a = f(x) \wedge x \in \operatorname{dom} f \wedge x \in f^{-1}[Y]$. Esto significa que $a \in f[f^{-1}[Y]]$.

La relación en la que están dos conjuntos cuando existe una biyección entre ellos es la precisión formal de la relación de tener el mismo tamaño. El estudio de esta noción conduce a la teoría de los *números cardinales*, que es parte esencial de la Teoría de Conjuntos pero que en esta introducción no podemos desarrollar. Nos limitamos a exponer una serie de hechos básicos sobre biyectabilidad.

**Definición** Sean $X$ e $Y$ conjuntos. Decimos que $X$ *es biyectable con* $Y$ y escribimos $X \sim Y$ si existe una biyección de $X$ en $Y$. También se dice que $X$ e $Y$ tienen el *mismo tamaño* o la *misma cardinalidad*.

**Observaciones 5.20** *1.* $A \sim A$.

*2.* *Si* $A \sim B$, *entonces* $B \sim A$.

*3.* *Si* $A \sim B$ *y* $B \sim C$, *entonces* $A \sim C$.

**Prueba**. Para *1* basta ver que $I_A$ es una biyección de $A$ en $A$. Para *2*, si $f$ es una biyección de $A$ en $B$, entonces $f^{-1}$ es una biyección de $B$ en $A$. Para *3*, si $f$ es una biyección de $A$ en $B$ y $g$ es una biyección de $B$ en $C$, entonces $g \circ f$ es una biyección de $A$ en $C$.

**Ejercicio 5.21** *Demostrar los siguientes enunciados.*

*1.* *Si* $A \sim A'$, $B \sim B'$, *y* $A \cap B = A' \cap B' = \emptyset$, *entonces* $A \cup B \sim A' \cup B'$.

*2.* $A \times B \sim B \times A$.

*3.* $A \times (B \times C) \sim (A \times B) \times C$.

*4.* *Si* $A \sim A'$ *y* $B \sim B'$, *entonces* $A \times B \sim A' \times B'$.

*5.* *Si* $A \sim A'$, *entonces* $\mathcal{P}(A) \sim \mathcal{P}(A')$.

*6. Si $A \sim A'$ y $B \sim B'$, entonces ${}^{A}B \sim {}^{A'}B'$.*

**Teorema 5.22 (Cantor)** $A \not\sim \mathcal{P}(A)$

**Prueba**. Supongamos lo contrario, es decir, que existe una biyección $f$ de $A$ en $\mathcal{P}(A)$. Si $a$ es un argumento de $f$, entonces $a$ es un elemento de $A$ y su valor $f(a)$ es un subconjunto de $A$, de manera que puede ocurrir que $a \in f(a)$ o que $a \notin f(a)$. Sea $X$ el conjunto de los argumentos de $f$ que no pertenecen a su valor, esto es $X = \{a : a \in A \wedge a \notin f(a)\}$. Como $X \in \mathcal{P}(A)$ y $f : A \to \mathcal{P}(A)$ es exhaustiva, hay un $x \in A$ tal que $f(x) = X$. Nos hacemos entonces la pregunta de si $x$ pertenece a su valor o no. Si fuera $x \in f(x)$, tendríamos $x \in X = \{a : a \in A \wedge a \notin f(a)\}$, de modo que $x \notin f(x)$. Y si $x \notin f(x)$, entonces $x \in \{a : a \in A \wedge a \notin f(a)\} = X = f(x)$, de modo que $x \in f(x)$. Esta contradicción fuerza a admitir que tal biyección $f$ no puede existir.

**Proposición 5.23** *1. Si $A \cap B = \emptyset$, entonces ${}^{A\cup B}C \sim {}^{A}B \times {}^{B}C$.*

*2. ${}^{A\times B}C \sim {}^{A}({}^{B}C)$.*

*3. ${}^{\{a\}}B \sim B$.*

**Prueba**. *1*. Sea $F : {}^{A}C \times {}^{B}C \to {}^{A\cup B}C$ la función definida por $F(\langle f, g\rangle) = f \cup g$. Mostraremos que es biyectiva. Obsérvese primero que está bien definida, es decir, que siempre que $f \in {}^{A}C$ y $g \in {}^{B}C$, entonces $(f \cup g) : A \cup B \to C$ y por tanto $f \cup g \in {}^{A\cup B}C$. Esto ocurre porque $A \cap B = \emptyset$, pues en otro caso $f \cup g$ quizás ni sería una función. Mostramos que $F$ es exhaustiva. Sea $f \in {}^{A\cup B}C$. Sea $g = f \restriction A$ y $h = f \restriction B$. Entonces $g : A \to C$, $h : B \to C$ y por tanto $\langle g, h\rangle \in {}^{A}C \times {}^{B}C$. Además es claro que $F(\langle g, h\rangle) = g \cup h = f$. Para mostrar, finalmente, que $F$ es inyectiva, supongamos que $f, f'$ pertenecen a ${}^{A}C$, que $g, g'$ pertenecen a ${}^{B}C$ y que $F(\langle f, g\rangle) = F(\langle f', g'\rangle)$. Debemos mostrar que $\langle f, g\rangle = \langle f', g'\rangle$, es decir, que $f = f'$ y $g = g'$. Sabemos, pues, que $f \cup g = f' \cup g'$. Entonces $f = (f \cup g) \restriction A = (f' \cup g') \restriction A = f'$. Similarmente, $g = (f \cup g) \restriction B = (f' \cup g') \restriction B = g'$.

*2*. Vamos a definir una biyección $F : {}^{A}({}^{B}C) \to {}^{A\times B}C$. Vamos a asignar a cada $f : A \to {}^{B}C$ la función $F(f) : A \times B \to C$ definida por la regla $F(f)(\langle a, b\rangle) = f(a)(b)$. Para ver que esta función está bien definida sólo hay que observar que siempre que $f : A \to {}^{B}C$ y $a \in A$, entonces $f(a) : B \to C$ y por tanto para cada $b \in B$, $b \in \operatorname{dom} f(a)$ y $f(a)(b) \in C$. Vamos ahora a ver que $F$ es exhaustiva. Sea $g : A \times B \to C$ y veamos que hay $f : A \to {}^{B}C$ tal que $F(f) = g$. Definimos explícitamente

$$f = \{\langle a, h\rangle : a \in A \wedge h \in {}^{B}C \wedge \forall x(x \in B \to h(x) = g(\langle a, x\rangle))\}.$$

Por definición $f$ es una relación con dominio incluido en $A$ y recorrido incluido en ${}^{B}C$. Si $a \in A$ y $h = \{\langle b, g(\langle a, b\rangle) : b \in B\}$ entonces $h : B \to C$ y $\langle a, h\rangle \in f$. Esto muestra que $\operatorname{dom} f = A$. Sólo falta mostrar que $f$ es una función, pero ello es claro dado que si $\langle a, h\rangle \in f$ y $\langle a, h'\rangle \in f$, entonces $h$ y $h'$ son dos funciones de $B$ en $C$ con los mismos valores y por tanto $h = h'$. De todo ello se sigue que $f \in {}^{A}({}^{B}C)$. Sólo falta verificar ahora que $F(f) = g$. Por definición $F(f) : A \times B \to C$ y los valores se obtienen de acuerdo con la regla $F(f)(\langle a, b\rangle) = f(a)(b)$. Pero $f(a)(b) = g(\langle a, b\rangle)$. Por tanto $F(f) = g$. La última cuestión es establecer que $F$ es inyectiva. Supongamos para ello que $f$ y $f'$ son funciones de $A$ en ${}^{B}C$ y que $F(f) = F(f')$ y veamos que $f = f'$. Tanto $F(f)$ como $F(f')$ son funciones de $A \times B$ en $C$. Sea $a \in A$. Entonces $f(a)$ y $f'(a)$ son funciones de $B$ en $C$. Para cada $b \in B$,

$f(a)(b) = F(f)(\langle a, b\rangle) = F(f')(\langle a, b\rangle) = f'(a)(b)$. Por tanto $f(a) = f'(a)$ y, en definitiva, $f = f'$.

*3*. Queremos definir una biyección $F$ entre $B$ y ${}^{\{a\}}B$. Para ello asignamos a cada $b \in B$ la función $F(b) : \{a\} \to B$ dada por $F(b)(a) = b$. Obviamente $F$ es una función de $B$ en ${}^{\{a\}}B$. Hay que ver que es biyectiva. Si $g : \{a\} \to B$ y $b = g(a)$, entonces $F(b) = g$, de manera que $F$ es exhaustiva. Y si $b, b'$ son elementos de $B$ y $F(b) = F(b')$, entonces $b = F(b)(a) = F(b')(a) = b'$. Esto muestra que $F$ es inyectiva.

**Proposición 5.24** *Si $B$ tiene dos elementos, entonces $\mathcal{P}(A) \sim {}^{A}B$.*

**Prueba**. Sea $B = \{a, b\}$ con $a \neq b$. Definimos una función $F : \mathcal{P}(A) \to {}^{A}B$ de modo que para cada $X \in \mathcal{P}(A)$, $F(X)$ sea la función de $A$ en $B$ definida por $F(X)(x) = a$ si $x \in X$ y $F(X)(x) = b$ si $x \notin X$. Explícitamente

$$F(X) = (X \times \{a\}) \cup ((A \smallsetminus X) \times \{b\}).$$

Vemos primero que $F$ es exhaustiva. Sea $f : A \to B$ y veamos que hay $X \in \mathcal{P}(A)$ tal que $F(X) = f$. Basta especificar $X = \{x : x \in A \wedge f(x) = a\}$. Es claro que $F(X) = f$. Para mostrar que $F$ es inyectiva supongamos que $X, Y$ son subconjuntos de $A$ y que $F(X) = F(Y)$ y veamos que $X = Y$. Sea $x \in X$. Entonces $F(X)(x) = a$ y por tanto $F(Y)(x) = a$ y con ello $x \in Y$. Esto muestra que $X \subseteq Y$. Similarmente se muestra que $Y \subseteq X$ y así que $X = Y$.

# Capítulo 6

# Números Naturales

**Definición** Un *sistema de Peano* es un conjunto $A$ con una función inyectiva $f : A \to A$ y un elemento $a \in A \smallsetminus \operatorname{rec} f$ que verifican el *principio de inducción*

$$\forall X(X \subseteq A \wedge a \in X \wedge \forall x(x \in X \to f(x) \in X) \to X = A).$$

Nos referiremos al sistema de Peano con la notación $(A, f, a)$.

**Lema 6.1** *Si $(A, f, a)$ es un sistema de Peano, entonces* $\operatorname{rec} f = A \smallsetminus \{a\}$.

**Prueba**. Sea $X = \operatorname{rec} f \cup \{a\}$. Ya sabemos que $X \subseteq A$ y que $a \notin \operatorname{rec} f$. Sólo falta mostrar que $X = A$ y ello puede hacerse usando el principio de inducción. Es claro que $a \in X$, de modo que para establecer que $X = A$ queda únicamente verificar que $\forall x(x \in X \to f(x) \in X)$. Pero esto último es también claro, pues para cada $x \in A$, $f(x) \in \operatorname{rec} f \subseteq X$.

Una de las características de los sistemas de Peano es que en ellos se pueden definir funciones por *recursión*. La próxima proposición establece este hecho.

**Proposición 6.2** *Sea $(A, f, a)$ un sistema de Peano, sea $B$ un conjunto, $g : B \to B$ y $b \in B$. Existe entonces una única función $h : A \to B$ que verifica las siguientes condiciones*

- $h(a) = b$
- $\forall x(x \in A \to h(f(x)) = g(h(x)))$

**Prueba**. Consideremos el conjunto $H$ formado por todas las funciones $s$ que verifican las siguientes condiciones

1. $\operatorname{dom} s \subseteq A$
2. $\operatorname{rec} s \subseteq B$
3. $\forall x(x \in A \wedge f(x) \in \operatorname{dom} s \to x \in \operatorname{dom} s)$
4. $(a \in \operatorname{dom} s \to s(a) = b)$

5. $\forall x(x \in \operatorname{dom} s \wedge f(x) \in \operatorname{dom} s \rightarrow s(f(x)) = g(s(x)))$

Se trata del conjunto de todas las funciones con dominio contenido en $A$ y con valores en $B$ y que verifican las cláusulas que pedimos a $h$ en la medida en que los elementos pertinentes de $A$ estén en su dominio. Pedimos además que los dominios de estas funciones tengan la propiedad adicional de que siempre que $f(x)$ está, también $x$ está. Vamos a establecer diversas propiedades de $H$.

(1) Si $h_1, h_2 \in H$, entonces $h_1(x) = h_2(x)$ para cada $x \in \operatorname{dom} h_1 \cap \operatorname{dom} h_2$. Para ello basta ver que si $X = \{x : x \in A \wedge (x \in \operatorname{dom} h_1 \cap \operatorname{dom} h_2 \rightarrow h_1(x) = h_2(x))\}$ entonces $X = A$. Esto puede establecerse usando el principio de inducción. Es claro que $a \in X$, de modo que basta ver que $\forall x(x \in X \rightarrow f(x) \in X)$. Sea entonces $x \in X$ y veamos que $f(x) \in X$. Para ello supongamos que $f(x) \in \operatorname{dom} h_1 \cap \operatorname{dom} h_2$. Como $h_1, h_2 \in H$, resulta entonces que $x \in \operatorname{dom} h_1 \cap \operatorname{dom} h_2$. Como hemos supuesto que $x \in X$, tenemos que $h_1(x) = h_2(x)$. Entonces, como $h_1, h_2 \in H$, $h_1(f(x))) = f(h_1(x)) = f(h_2(x)) = h_2(f(x))$. Así $f(x) \in X$.

Del punto (1) ya se sigue que sólo puede haber una función $h$ con las propiedades que exigimos, pues si $h_1$ y $h_2$ son funciones de $A$ en $B$ tales que $h_1(a) = h_2(a) = b$, $\forall x(x \in A \rightarrow h_1(f(x)) = g(h_1(x)))$ y $\forall x(x \in A \rightarrow h_2(f(x)) = g(h_2(x)))$ entonces $h_1, h_2 \in H$ y $A = \operatorname{dom} h_1 \cap \operatorname{dom} h_2$. Así pues sólo queda mostrar que hay al menos una tal función $h$. Para ello necesitamos demostrar primero más propiedades de $H$. El punto siguiente se establece sin dificultades.

(2) Si $h_1 \in H$, $x \in \operatorname{dom} h_1$ y $h_2 = h_1 \cup \{\langle f(x), g(h_1(x))\rangle\}$, entonces $h_2 \in H$.

(3) Para cada $x \in A$ existe una $h_1 \in H$ tal que $x \in \operatorname{dom} h_1$. Sea $X = \{x : x \in A \wedge \exists h_1(h_1 \in H \wedge x \in \operatorname{dom} h_1)\}$. Vemos que $X = A$ usando el principio de inducción. Primero hay que ver que $a \in X$. Pero ello es claro pues si $h_1 = \{\langle a, b\rangle\}$ entonces $a \in \operatorname{dom} h_1$ y $h_1 \in H$. Ahora supongamos que $x \in X$ y veamos que también $f(x) \in X$. Como $x \in X$, hay $h_1 \in H$ tal que $x \in \operatorname{dom} h_1$. De (2) inferimos entonces que hay también $h_2 \in H$ tal que $f(x) \in \operatorname{dom} h_2$. Por tanto $f(x) \in X$.

Sea ahora $h = \bigcup H$. Es claro que $h$ es una relación con $\operatorname{dom} h \subseteq A$ y $\operatorname{rec} h \subseteq B$. De (1) se sigue que si $\langle x, y\rangle \in h$ y $\langle x, z\rangle \in h$, entonces $y = z$ y por tanto que $h$ es una función. De (3) se sigue que $\operatorname{dom} h = A$. Así pues $h : A \rightarrow B$.

(4) Si $h_1 \in H$ y $x \in \operatorname{dom} h_1$, entonces $h_1(x) = h(x)$. En efecto, supongamos que $x \in \operatorname{dom} h_1$. Como $\langle x, h(x)\rangle \in h = \bigcup H$, existe $h_2 \in H$ tal que $\langle x, h(x)\rangle \in h_2$. Entonces $x \in \operatorname{dom} h_2$ y $h(x) = h_2(x)$. Por (1) sabemos que $h_1(x) = h_2(x)$. Por tanto $h(x) = h_1(x)$.

Del punto (4) se siguen las restantes propiedades que necesitamos de $h$. Por un lado que $h(a) = b$ y por otro lado que $\forall x(x \in A \rightarrow h(f(x)) = g(f(x)))$.

**Definición** Sean $(A, f, a)$ y $(B, g, b)$ sistemas de Peano. Un *isomorfismo* entre $(A, f, a)$ y $(B, f, b)$ es una biyección $h$ de $A$ en $B$ tal que $h(a) = b$ y para cada $x \in A$, $h(f(x)) = g(h(x))$. Decimos que los sistemas de Peano son *isomorfos* si existe un isomorfismo entre ellos. Es fácil ver que la relación de isomorfía es una relación de equivalencia entre sistemas de Peano.

**Proposición 6.3** *Cualesquiera dos sistemas de Peano son isomorfos.*

**Prueba**. Sean $(A, f, a)$ y $(B, g, b)$ sistemas de Peano. Usando la Proposición 6.2 sabemos que existe una función $h : A \rightarrow B$ tal que $h(a) = b$ y $\forall x(x \in A \rightarrow h(f(x)) = g(h(x)))$. Falta mostrar que $h$ es biyectiva. Para mostrar que es exhaustiva consideramos el conjunto $X = \operatorname{rec} h$

y usamos el principio de inducción en $(B, g, b)$. Queremos ver que $X = B$ y para ello basta establecer que $b \in X$ y que $\forall y(y \in X \to g(y) \in X)$. Lo primero es claro pues $b = h(a)$. Para justificar lo segundo supongamos que $y \in \operatorname{rec} h$. Hay entonces $x \in A$ tal que $h(x) = y$. Las cláusulas que caracterizan a $h$ nos dan que $h(f(x)) = g(f(x))$. Así $g(y) = h(f(x))$, de modo que $g(y) \in X$. Para finalizar debemos mostrar que $h$ es inyectiva. Aplicamos el principio de inducción en $(A, f, a)$ al conjunto $X' = \{x : x \in A \wedge \forall y(y \in A \wedge h(x) = h(y) \to x = y)\}$. Mostraremos que $X' = A$ y con ello concluirá la prueba. El primer paso es ver que $a \in X'$. Supongamos para ello que $h(a) = h(y)$ y veamos que $a = y$. Sabemos que $h(a) = b$. Si fuera $y \neq a$ entonces, por el lema 6.1 habría un $z \in A$ tal que $y = f(z)$. En ese caso $b = h(y) = f(h(z))$, pero sin embargo $b \notin \operatorname{rec} g$. Esta contradicción fuerza a aceptar que $y = a$ y por tanto que $a \in X'$. Supongamos ahora que $x \in X'$ y veamos que también $f(x) \in X'$. Sea $h(f(x)) = h(y)$. Debemos mostrar que $f(x) = y$. Sabemos que $h(f(x)) = g(h(x))$. No puede ser entonces $y = a$, pues $h(a) = b \notin \operatorname{rec} g$. Por el lema 6.1 sabemos entonces que hay $z \in A$ tal que $f(z) = y$. En ese caso $h(y) = h(f(z)) = g(h(z))$ y por tanto $g(h(x)) = g(h(z))$. Como $g$ es inyectiva $h(x) = h(z)$ y como además $x \in X'$, se obtiene que $x = z$. Entonces $f(x) = f(z) = y$.

Los números naturales se construyen en Teoría de Conjuntos como un particular sistema de Peano. Hay diversas maneras de hacerlo aunque como ya se ha indicado todos son isomorfos entre sí, hecho que permite transferir ciertas propiedades de uno a otro. Estas propiedades transferibles son las que no dependen de la peculiar construcción que se ha escogido. Aquí presentamos la construcción más usual, debida a von Neumann. Para cualquiera de ellas necesitamos añadir un nuevo axioma a la teoría, el *Axioma del Infinito.*

**Axioma 6.4 (Axioma del Infinito)** *Hay un conjunto $x$ tal que $\emptyset \in x$ y $\forall y(y \in x \to y \cup \{y\} \in x)$.*

**Definición** Un conjunto $x$ es *inductivo* si $\emptyset \in x$ y $\forall y(y \in x \to y \cup \{y\} \in x)$. Obsérvese que el axioma del infinito afirma precisamente que hay conjuntos inductivos. Veremos a continuación que hay un menor conjunto inductivo, es decir, un conjunto inductivo que está incluido en todos los otros conjuntos inductivos.

**Observación 6.5** *Si $\Phi$ es una colección no vacía de conjuntos inductivos, entonces $\bigcap \Phi$ es un conjunto inductivo. En particular, si $x, y$ son conjuntos inductivos, entonces $x \cap y$ es inductivo.*

**Proposición 6.6** *Hay un único conjunto inductivo $x$ tal que para cada conjunto inductivo $y$, $x \subseteq y$.*

**Prueba**. Es claro que no puede haber dos conjuntos inductivos distintos con la propiedad indicada. Mostramos que hay al menos uno. Por el Axioma del Infinito sabemos que hay un conjunto inductivo $a$. Sea $\Phi = \{y : y \text{ es inductivo y } y \subseteq a\}$. Entonces $\Phi$ es una colección no vacía de conjuntos inductivos. Sea $x = \bigcap \Phi$. Por la observación anterior sabemos que $x$ es un conjunto inductivo. Sea $y$ otro conjunto inductivo arbitrario y veamos que $x \subseteq y$. Por la observación previa $a \cap y$ es inductivo. Entonces $a \cap y \in \Phi$, con lo cual $x \subseteq a \cap y$. En especial $x \subseteq y$.

**Definición** Nos referimos con $\omega$ al conjunto caracterizado en la proposición anterior como el menor conjunto inductivo. Así $\omega$ es un conjunto inductivo y para cada conjunto inductivo $x$, $\omega \subseteq x$. Llamamos *números naturales* a los elementos de $\omega$. Es habitual usar las letras $n, m, i, j, k, \ldots$ como variables de números naturales. En este contexto se define el número cero como $0 = \emptyset$. Como $\omega$ es inductivo, siempre que $n \in \omega$ también $n \cup \{n\} \in \omega$. Por tanto se puede definir una función $S : \omega \to \omega$ poniendo $S(n) = n \cup \{n\}$. La función $S$ se llama función *sucesor*. Los números uno, dos, tres, etc. pueden definirse mediante $1 = S(0) = \{0\}$, $2 = S(1) = 1 \cup \{1\} = \{0, 1\}$, $3 = S(2) = 2 \cup \{2\} = \{0, 1, 2\}$ etc.

**Definición** Decimos que $x$ es un conjunto *transitivo* si los elementos de los elementos de $x$ son elementos de $x$, es decir, si $\forall yz(z \in y \land y \in x \to z \in x)$. Obsérvese que esto equivale a decir que $\bigcup x \subseteq x$ y también a que $x \subseteq \mathcal{P}(x)$.

**Lema 6.7** *Todo número natural es transitivo.*

**Prueba**. En general, una estrategia para mostrar que todos los números naturales tienen una cierta propiedad consiste en formar el conjunto de los números naturales que tienen la propiedad en cuestión y mostrar a continuación que se trata de un conjunto inductivo. En este caso consideramos el conjunto $x = \{n : n \in \omega \land n \text{ es transitivo } \}$ y veamos que es inductivo. Es inmediato que $\emptyset$ es transitivo y por tanto que $0 \in x$. Supongamos ahora que $n \in x$ y veamos que también $S(n) \in x$. Sabemos entonces que $n$ es transitivo y queremos ver que $n \cup \{n\}$ también lo es. Para ello supongamos que $z \in y \land y \in n \cup \{n\}$. Debemos mostrar que $z \in n \cup \{n\}$. Se plantean dos casos, según $y \in n$ o bien $y = n$. En el primer caso, como hemos supuesto que $n$ es transitivo, $z \in n$ y así $z \in n \cup \{n\}$. Y en el caso $y = n$ tenemos $z \in n$ y por tanto $z \in n \cup \{n\}$.

**Lema 6.8** *Si $n$ es un número natural, $n \notin n$.*

**Prueba**. Consideremos el conjunto $x = \{n : n \in \omega \land n \notin n\}$. Como $0 = \emptyset$, $0 \in x$. Supongamos que $n \in x$ y veamos que también $S(n) \in x$. En caso contrario, $S(n) \in S(n) = n \cup \{n\}$, de manera que $S(n) \in n$ o bien $S(n) = n$. En el caso $S(n) \in n$, como $n \in S(n)$ y el lema anterior nos garantiza que $n$ es transitivo, tenemos que $n \in n$. En el caso $S(n) = n$ se llega a la misma conclusión de modo inmediato. Sin embargo hemos supuesto que $n \in x$, de manera que $n \notin n$.

**Proposición 6.9** $(\omega, S, 0)$ *es un sistema de Peano.*

**Prueba**. Si $X \subseteq \omega$ tiene las propiedades de que $0 \in X$ y $\forall x(x \in X \to S(x) \in X)$, entonces $X$ es inductivo y por tanto $X = \omega$. Por otro lado es claro que $0 \notin \operatorname{rec} S$. Así pues sólo nos queda ver que $S$ es una función inyectiva. Supongamos para ello que $n, m \in \omega$ y que $S(n) = S(m)$. Mostraremos que $n = m$. Tenemos que $n \cup \{n\} = m \cup \{m\}$. Si suponemos que $n \neq m$ concluimos que $n \in m \land m \in n$. Como $n$ es transitivo se tiene entonces que $n \in n$, en contra de lema previo.

Como los números naturales constituyen un sistema de Peano podemos usar la Proposición 6.2 para definir funciones por recursión. Dado un conjunto $A$ un elemento $a \in A$ y una aplicación $g : A \to A$ existe una única función $f : \omega \to A$ que verifica las condiciones

- $f(0) = a$
- $\forall n(n \in \omega \to f(S(n)) = g(f(n)))$.

Usaremos este procedimiento a continuación para introducir la suma el producto y la exponenciación de números naturales.

**Proposición 6.10** *Hay una única función $f : \omega \times \omega \to \omega$ tal que*

1. *Para cada $n \in \omega$, $f(\langle n, 0\rangle) = n$*
2. *Para cada $n, m \in \omega$, $f(\langle n, S(m)\rangle) = S(f(\langle n, m\rangle))$.*

**Prueba**. Sea $n$ un número natural. Consideremos el conjunto $A = \omega$, el elemento $a = n$ de $A$ y la función $g = S$. Podemos definir una función por recursión. Se trata de la única función $f_n : \omega \to \omega$ que verifica

1. $f_n(0) = n$
2. Para cada $m \in \omega$, $f_n(S(m)) = S(f_n(m))$.

La existencia de la función $f$ se garantiza poniendo $f(\langle n, m\rangle) = f_n(m)$. Para demostrar la unicidad de $f$ supongamos que $f' : \omega \times \omega \to \omega$ es otra función que cumple

1. Para cada $n \in \omega$, $f'(\langle n, 0\rangle) = n$
2. Para cada $n, m \in \omega$, $f'(\langle n, S(m)\rangle) = S(f'(\langle n, m\rangle))$.

Sea $n \in \omega$ arbitrario. Queremos ver que para cada $m \in \omega$, $f'(\langle n, m\rangle) = f(\langle n, m\rangle)$. Consideramos el conjunto $X = \{m : m \in \omega \wedge f'(\langle n, m\rangle) = f(\langle n, m\rangle)\}$ y mostramos por inducción que $X = \omega$. Como $f'(\langle n, 0\rangle) = n = f(\langle n, 0\rangle)$, es claro que $0 \in X$. Supongamos ahora que $m \in X$ y veamos que $S(m) \in X$. Como $m \in X$, $f'(\langle n, m\rangle) = f(\langle n, m\rangle)$. Entonces

$$f'(\langle n, S(m)\rangle) = S(f'(\langle n, m\rangle)) = S(f(\langle n, m\rangle) = f(\langle n, S(m)\rangle)$$

de modo que también $S(m) \in X$.

**Definición** La *suma* de números naturales es la aplicación $+ : \omega \times \omega \to \omega$ garantizada por la proposición previa. Usamos la notación habitual $n + m = +(\langle n, m\rangle)$. Queda definida por las cláusulas

1. Para cada $n \in \omega$, $n + 0 = n$.
2. Para cada $n, m \in \omega$, $n + S(m) = S(n + m)$.

**Proposición 6.11** *Hay una única función $f : \omega \times \omega \to \omega$ tal que*

1. *Para cada $n \in \omega$, $f(\langle n, 0\rangle) = 0$*
2. *Para cada $n, m \in \omega$, $f(\langle n, S(m)\rangle) = f(\langle n, m\rangle) + n$.*

**Prueba**. Como en la proposición anterior vemos que para cada número natural $n$ hay una única función $f_n : \omega \to \omega$ que verifica

1. $f_n(0) = 0$.
2. Para cada $m \in \omega$, $f_n(S(m)) = f_n(m) + n$.

La función que buscamos se obtiene poniendo $f(\langle n, m\rangle) = f_n(m)$. La unicidad se demuestra por inducción como en la proposición anterior.

**Definición** El *producto* de números naturales es la aplicación $\cdot : \omega \times \omega \to \omega$ garantizada por la proposición previa. Usamos la notación habitual $n \cdot m = \cdot(\langle n, m\rangle)$. El producto queda entonces definido por las cláusulas

1. Para cada $n \in \omega$, $n \cdot 0 = 0$.
2. Para cada $n, m \in \omega$, $n \cdot S(m) = n \cdot m + n$.

**Proposición 6.12** *Hay una única función $f : \omega \times \omega \to \omega$ tal que*

1. *Para cada $n \in \omega$, $f(\langle n, 0\rangle) = 1$*
2. *Para cada $n, m \in \omega$, $f(\langle n, S(m)\rangle) = f(\langle n, m\rangle) \cdot n$.*

**Prueba**. Análoga a la de las dos proposiciones anteriores.

**Definición** La *exponenciación* de números naturales es la aplicación $\exp : \omega \times \omega \to \omega$ garantizada por la proposición previa. Usamos la notación habitual $n^m = \exp(\langle n, m\rangle)$. La exponenciación queda, por consiguiente, definida mediante las cláusulas

1. Para cada $n \in \omega$, $n^0 = 1$.
2. Para cada $n, m \in \omega$, $n^{S(m)} = n^m \cdot n$.

A partir de aquí puede desarrollarse la aritmética elemental. Podemos demostrar que $2 + 2 = 4$. Por definición $2 = S(S(0))$ y $4 = S(S(2))$. Entonces

$$2 + 2 = 2 + S(S(0)) = S(2 + S(0)) = S(S(2 + 0)) = S(S(2)) = 4.$$

Mostramos a continuación las propiedades básicas de la suma y el producto. Las demostraciones proceden usualmente por inducción. Para mostrar que todos los números naturales tienen una propiedad $P$ se muestra primero que el número 0 tiene $P$ y se muestra a continuación que siempre que un número $n$ tiene $P$, entonces su sucesor $n + 1$ también tiene $P$. En ese contexto se dice que la hipótesis de que $n$ tenga $P$ es la *hipótesis inductiva* y el objetivo de demostrar que $n + 1$ tiene $P$ se llama el *caso inductivo* o el caso $n + 1$ de la inducción, siendo el caso del cero el *caso inicial*. Por tanto, en una inducción se establece primero el caso inicial y se establece a continuación el caso inductivo con ayuda de la hipótesis inductiva.

En ocasiones el enunciado que se quiere establecer tiene cuantificación múltiple, como $\forall m \forall n(m \in \omega \land n \in \omega \to m + n = n + m)$. La prueba se puede hacer de dos maneras. La primera posibilidad es escoger la variable $m$, considerar la propiedad $P$ que tiene un número natural $m$ cuando $\forall n(n \in \omega \to m + n = n + m)$ y mostrar que todos los números naturales tienen esa propiedad $P$. La segunda posibilidad consiste en escoger la variable $n$, considerar la propiedad $Q$ que tiene un número natural $n$ cuando $\forall m(m \in \omega \to m + n = n + m)$ y mostrar que todos los números naturales tienen la propiedad $Q$. En el primer caso se dice que se hace inducción en $m$ y en el segundo caso que se hace inducción en $n$. La prueba puede ser muy sencilla o muy complicada dependiendo de si se ha elegido acertadamente la variable en la que hacer la inducción. También se dice que se hace inducción en $n$ si se fija un $m$ arbitrario y se muestra por inducción que todos los números naturales $n$ tienen la propiedad $P'$ que consiste en verificar la ecuación $m + n = n + m$.

**Proposición 6.13** *Para cualesquiera $n, m, k \in \omega$, $(n + m) + k = n + (m + k)$.*

**Prueba**. Sean $n, m \in \omega$ arbitrarios. Vemos por inducción en $k$ que $\forall k(k \in \omega \to (n+m)+k = n + (m + k))$. En el caso inicial, tenemos que $(n + m) + 0 = n + m = n + (m + 0)$. Por la hipótesis inductiva, $(n + m) + k = n + (m + k)$. En ese caso

$$(n + m) + S(k) = S((n + m) + k) = S(n + (m + k)) = n + S(m + k) = n + (m + S(k)).$$

**Lema 6.14** *1. Para cada $n \in \omega$, $0 + n = n$.*

*2. Para cada $n, m \in \omega$, $S(m) + n = S(m + n)$.*

**Prueba**. Establecemos el primer punto por inducción en $n$. Como $0 + 0 = 0$, ya tenemos el caso inicial. Supongamos que $0+n = n$. Entonces $S(n)+0 = S(n+0) = S(n) = S(0+n) = 0 + S(n)$. Esto finaliza la inducción. Consideramos a continuación el segundo punto. Sea $m \in \omega$ arbitrario. Vemos por inducción en $n$ que $\forall n(n \in \omega \to S(m) + n = S(m + n))$. Tenemos que $S(m) + 0 = S(m) = S(m + 0)$. Supongamos ahora que $S(m) + n = S(m + n)$. Entonces $S(m + S(n)) = S(S(m + n)) = S(S(m) + n) = S(S(m) + S(n))$.

**Proposición 6.15** *Para cada $n, m \in \omega$, $n + m = m + n$.*

**Prueba**. Sea $n \in \omega$ arbitrario, y veamos por inducción en $m$ que $\forall m(m \in \omega \to n + m = m + n)$. Por el lema 6.14 tenemos que $n + 0 = n = 0 + n$ de modo que el caso $m = 0$ está establecido. Consideremos ahora el caso inductivo. Por la hipótesis inductiva, $n + m = m + n$. De nuevo por el lema 6.14, $S(m) + n = S(m + n) = S(n + m) = n + S(m)$.

**Proposición 6.16** *Para cada $n, m, k \in \omega$, $n \cdot (m + k) = n \cdot m + n \cdot k$.*

**Prueba**. Sean $n, m \in \omega$. Mostramos por inducción en $k$ que $\forall k(k \in \omega \to n \cdot (m + k) = (n \cdot m) + (n \cdot k))$. Por definición de producto y de suma tenemos que $n \cdot (m + 0) = n \cdot m$ y $n \cdot m + n \cdot 0 = n \cdot m + 0 = n \cdot m$. Por tanto tenemos el caso inicial. Supongamos que $n \cdot (m + k) = n \cdot m + n \cdot k$. Usando la definición de suma y producto y la asociatividad de la suma obtenemos que

$$n\cdot(m+S(k)) = n\cdot S(m+k) = n\cdot(m+k)+n = (n\cdot m+n\cdot k)+n = n\cdot m+(n\cdot k+n) = n\cdot m+n\cdot S(k).$$

**Proposición 6.17** *Para cada $n, m, k \in \omega$, $(n \cdot m) \cdot k = n \cdot (m \cdot k)$.*

**Prueba**. Sean $n, m \in \omega$. Por inducción en $k$ establecemos que $\forall k(k \in \omega \rightarrow (n \cdot m) \cdot k = n \cdot (m \cdot k))$. Por definición de producto tenemos que $(n \cdot m) \cdot 0 = 0$ y $n \cdot (m \cdot 0) = n \cdot 0 = 0$. Supongamos ahora que $(n \cdot m) \cdot k = n \cdot (m \cdot k)$. Usando la definición de producto y la Proposición 6.16 concluimos que

$$(n \cdot m) \cdot S(k) = (n \cdot m) \cdot k + n \cdot m = n \cdot (m \cdot k) + n \cdot m = n \cdot (m \cdot k + m) = n \cdot (m \cdot S(k)).$$

**Lema 6.18** *1. Para cada $n \in \omega$, $0 \cdot n = 0$.*

*2. Para cada $n, m \in \omega$, $S(m) \cdot n = n + (m \cdot n)$.*

**Prueba**. Mostramos el primer punto por inducción en $n$. El caso $n = 0$ es claro, pues por definición de producto tenemos $0 \cdot 0 = 0$. Supuesto ahora que $0 \cdot n = 0$, usando la definición del producto y las propiedades ya establecidas de la suma, vemos que $0 \cdot S(n) = (0 \cdot n) + 0 = 0 + 0 = 0$. Establecemos ahora el segundo punto considerando un $m$ arbitrario y mostrando por inducción en $n$ que $\forall n(n \in \omega \rightarrow S(m) \cdot n = n + (m \cdot n))$. En el caso $n = 0$ tenemos por definición de producto que $S(m) \cdot 0 = 0 = 0 + (m \cdot 0)$. Consideremos ahora el caso inductivo. Usando la hipótesis inductiva así como la conmutatividad y asociatividad de la suma vemos que

$$S(m) \cdot S(n) = S(m) \cdot n + S(m) = ((m \cdot n) + n) + S(m) = (m \cdot n) + (n + S(m)) =$$

$$= (m \cdot n) + (S(n) + m) = S(n) + ((m \cdot n)) + m = S(n) + m \cdot S(n).$$

**Proposición 6.19** *Para cada $n, m \in \omega$, $n \cdot m = m \cdot n$.*

**Prueba**. Sea $n \in \omega$. Vemos por inducción en $m$ que $\forall m(m \in \omega \rightarrow n \cdot m = m \cdot n)$. En el caso $m = 0$ usamos el punto *1* de 6.18 y vemos que $n \cdot 0 = 0 = 0 \cdot n$. En el caso inductivo usamos la hipótesis inductiva y el punto *2* de 6.18 y concluimos que

$$n \cdot S(m) = n \cdot m + n = n + n \cdot m = S(m) \cdot n.$$

**Ejercicio 6.20** *Demostrar las siguientes propiedades de la exponenciación.*

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

Otra de las aspectos fundamentales de los números naturales es su ordenación. Puede introducirse de distintos modos equivalentes.

**Definición** La relación $\leq$ es la relación en $\omega$ definida por

$$n \leq m \leftrightarrow \exists k(k \in \omega \wedge n + k = m).$$

**Ejercicio 6.21** *Mostrar las siguientes propiedades de la suma de números naturales.*

1. *Si $n + k = n$, entonces $k = 0$.*

2. *Si $n+m=0$, entonces $n=m=0$.*

**Proposición 6.22** *La relación $\leq$ es un orden total reflexivo en $\omega$. El orden estricto asociado se define por*

$$n < m \leftrightarrow \exists k(k \in \omega \wedge k \neq 0 \wedge n+k=m).$$

**Prueba**. Sea $n \in \omega$. Como $n+0=n$, tenemos que $n \leq n$. Por tanto se trata de una relación reflexiva. Es fácil mostrar que es transitiva, pues si, $n+k=m$ y $m+k'=l$, resulta que $n+(k+k')=l$. Mostramos ahora que es antisimétrica. Supongamos para ello que $n \leq m$ y que $m \leq n$. Queremos mostrar que $n=m$. Por definición de $\leq$, hay $k$ tal que $n+k=m$ y hay $k'$ tal que $m+k'=n$. Entonces $n+(k+k')=n$. Utilizando las propiedades expuestas en el ejercicio previo se concluye primero que $k+k'=0$ y a continuación que $k=k'=0$. Por tanto $m=n+k=n+0=n$.

El orden estricto asociado a $\leq$ se define al modo usual: $n < m \leftrightarrow n \leq m \wedge n \neq m$. Si $n < m$, entonces $n \leq m$ y por tanto hay un $k \in \omega$ tal que $n+k=m$. Si fuera $k=0$ tendríamos $m=n+k=n+0=n$, lo cual es imposible dado que $n<m$. Así pues, debe ser $k \neq 0$. A la inversa, supongamos que hay un $k \in \omega$ tal que $n+k=m \wedge k \neq 0$ y veamos que $n<m$. Es claro que $n \leq m$. Si fuera $n=m$ tendríamos $n+k=n$ y, por el ejercicio previo, $k=0$. Debe ser por tanto $n \neq m$ y con ello $n<m$.

Falta establecer que el orden es total. Mostramos por inducción en $m$ que para cualesquiera $n, m \in \omega$, $n \leq m \vee m \leq n$. Comenzamos con el caso $m=0$. Como $0+n=n$ tenemos $0 \leq n$ y por tanto $n \leq 0 \vee 0 \leq n$. Consideramos a continuación el caso inductivo. Sea $n \in \omega$ arbitrario. Por hipótesis inductiva tenemos que $n \leq m \vee m \leq n$. En el caso $n \leq m$ sabemos que hay un $k$ tal que $n+k=m$ y en ese caso $n+S(k)=S(m)$ y así $n \leq S(m)$. Analizamos ahora el caso $m \leq n$. Hay un $k$ tal que $m+k=n$. En el caso $k=0$ resulta $n=m$ y por tanto $n \leq S(m)$ puesto que $n+1=m+1=S(m)$. Falta analizar el caso $k \neq 0$. En ese caso hay un $i \in \omega$ tal que $S(i)=k$. Entonces $S(m)+i=m+S(i)=m+k=n$ con lo cual $n \leq S(m)$. Esto finaliza la inducción y la prueba.

**Proposición 6.23** *El orden de los números naturales es un orden discreto sin mayor elemento. Tiene menor elemento, que es* 0*. Además, para cada $n \in \omega$, $S(n)$ es el sucesor inmediato de $n$ en el orden.*

**Prueba**. Como $n+0=n$, 0 es el menor elemento de $\omega$. Como $n+1=S(n) \wedge 1 \neq 0$, tenemos que $n<S(n)$. Falta ver que no hay ningún $m \in \omega$ tal que $n<m<S(n)$. Supongamos lo contrario, de manera que hay $k, k' \in \omega$ distintos de 0 y tales que $m=n+k$ y $S(n)=m+k'$. Entonces $S(n)=n+(k+k')$. Como $k \neq 0$, hay un $i \in \omega$ tal que $k=S(i)$. Entonces $S(n)=n+S(i+k')=S(n+(i+k'))$, de manera que $n=n+(i+k')$. Pero entonces $i+k'=0$, con lo cual $i=k'=0$. Pero habíamos supuesto que $k' \neq 0$.

**Proposición 6.24** *El orden de los números naturales es un buen orden.*

**Prueba**. Hay que demostrar que todo conjunto no vacío de números naturales tiene un menor elemento. Lo mostraremos efectuando un argumento por inducción. Lo que mostraremos por inducción en $n$ es que si $X \subseteq \omega$ y hay $m \leq n$ tal que $m \in X$, entonces $X$ tiene un menor elemento. De ello se sigue que cualquier subconjunto no vacío de $\omega$ tiene un menor elemento. El caso $n=0$ es particularmente sencillo porque 0 mismo es el menor elemento de $X$. Consideremos el caso inductivo. Supongamos que hay un $m \leq S(n)$ tal que $m \in X$. Si también hay algún elemento en $X$ menor o igual que $n$ podemos aplicar la hipótesis inductiva para garantizar que $X$ tiene menor elemento. Supongamos entonces que eso no ocurre, es decir, que todos los elementos de $X$ son mayores que $n$. En particular $m > n$ y por tanto $m = S(n)$. Entonces $S(n)$ es el menor elemento de $X$.

Para finalizar vamos a ver ahora que el orden de $\omega$ también puede caracterizarse en términos de las relaciones de pertenencia y de inclusión. Ésta no es una propiedad intrínseca de los números naturales sino una peculiar propiedad de la construcción de los números naturales de von Neumann. No tiene por qué ocurrir en otros sistemas de Peano.

**Proposición 6.25** *El orden estricto de $\omega$ coincide con la pertenencia y el orden reflexivo coincide con la inclusión. Por tanto, para cada $n, m \in \omega$,*

1. $n < m \leftrightarrow n \in m$
2. $n \leq m \leftrightarrow n \subseteq m$

*En particular, para cada $n \in \omega$, $n = \{m : m \in \omega \wedge m < n\}$.*

**Prueba**. Comenzamos demostrando por inducción en $n$ que para cada $n \in \omega$, $n = \{m : m \in \omega \wedge m < n\}$. El caso $n = 0$ es claro dado que $0 = \emptyset = \{m : m \in \omega \wedge m < 0\}$. Consideramos ahora el caso inductivo. Queremos mostrar que $S(n) = \{m : m \in \omega \wedge m < S(n)\}$. Por hipótesis inductiva $n = \{m : m \in \omega \wedge m < n\}$ y por definición $S(n) = n \cup \{n\}$. Como $S(n)$ es el sucesor inmediato de $n$ en el orden, usando estos datos vemos que $\{m : m \in \omega \wedge m < S(n)\} = \{m : m \in \omega \wedge m \leq n\} = \{m : m \in \omega \wedge m < n\} \cup \{n\} = n \cup \{n\} = S(n)$.

Establecido este punto podemos demostrar muy fácilmente *1*, pues si $m, n \in \omega$,

$$m \in n \leftrightarrow m \in \{m : m \in \omega \wedge m < n\} \leftrightarrow m < n.$$

Respecto a *2*, supongamos primero que $n \leq m$ y veamos que $n \subseteq m$. Tenemos que $n < m \vee n = m$. En el caso $n < m$ sabemos por *1* que $m \in n$. Como los números naturales son transitivos, resulta entonces que $m \subseteq n$. Pero $S(n) = n \cup \{n\}$ y por ello también $m \subseteq S(n)$. El caso $m = n$ es obvio dado que $S(n) = n \cup \{n\}$. Ahora falta establecer que si $m, n \in \omega$ y $m \subseteq n$, entonces $m \leq n$. Lo hacemos por inducción en $m$. El caso $m = 0$ no ofrece dificultades dado que $0 = \emptyset \subseteq n$. Supongamos ahora que $S(m) \leq n$ y veamos que $S(m) \subseteq n$. Por un lado $m \leq n$ y entonces la hipótesis inductiva nos garantiza que $m \subseteq n$. Por otro lado $m < n$ y por *1* tenemos que $m \in n$, con lo cual $\{m\} \subseteq n$. Como $S(m) = m \cup \{m\}$, uniendo estos dos resultados se concluye que $S(m) \subseteq n$.

También se puede introducir el orden directamente a partir de la operación de sucesión, sin necesidad de esperar a tener la suma. La definición adecuada es en ese caso como sigue:

$$m \leq n \leftrightarrow \forall X(X \subseteq \omega \wedge \forall k(k \in \omega \wedge S(k) \in X \rightarrow k \in X) \wedge n \in X \rightarrow m \in X).$$

# Capítulo 7

# Conjuntos Finitos y Conjuntos Infinitos

**Definición** Un conjunto $X$ es *finito* si hay un número natural $n$ tal que

$$X \sim \{m : m \in \omega \wedge m < n\}.$$

Si no hay tal número natural, se dice que el conjunto $X$ es *infinito*. Obsérvese que el conjunto $\{m : m \in \omega \wedge m < n\}$ tiene $n$ elementos. Además en la construcción efectuada de los números naturales resulta que $\{m : m \in \omega \wedge m < n\} = n$. Por tanto exactamente igual podríamos haber dicho que $X \sim n$.

**Observaciones 7.1** *1.* $\emptyset$ *es finito.*

*2.* *Si* $X$ *es finito, también lo es* $X \cup \{a\}$*.*

*3.* *Si* $X$ *es finito, también lo es* $X \setminus \{a\}$*.*

*4.* *Los subconjuntos de un conjunto finito también son finitos.*

**Prueba**. Los números naturales son conjuntos finitos, de manera que $\emptyset = 0$ lo es. Para mostrar ahora *2*, supongamos que $X$ es finito. Si $a \in X$ entonces $X \cup \{a\} = X$ y por ello es finito. Consideremos la otra posibilidad: $a \notin X$. Por ser $X$ finito hay un número natural $n$ tal que $X \sim n$. Sea $f$ una biyección de $X$ en $n$. Como $n \notin n$, $f \cup \{\langle a, n\rangle\}$ es una biyección entre $X \cup \{a\}$ y $n \cup \{n\}$. Pero $n \cup \{n\}$ es el número natural $n+1$. Por tanto $X \cup \{a\}$ es finito.

*3*. Sea $X$ finito. Mostramos por inducción natural que para cada $n \in \omega$, si $X \sim n$ entonces $X \setminus \{a\}$ es finito. En el caso $n = 0$ debe ser $X = \emptyset$ y por tanto $X \setminus \{a\} = X$ es finito. Supongamos que $X \sim n+1$ y recordemos que $n + 1 = n \cup \{n\}$. Sea $f$ una biyección entre $X$ y $n \cup \{n\}$. Podemos suponer que $a \in X$, pues en otro caso $X \setminus \{a\} = X$. Definimos

$$g = (f \setminus \{\langle a, f(a)\rangle, \langle f^{-1}(n), n\rangle\}) \cup \{\langle a, n\rangle, \langle f^{-1}(n), f(a)\rangle\}.$$

Es fácil comprobar que también $g$ es una biyección entre $X$ y $n \cup \{n\}$. Como $g(a) = n$, resulta que $g \restriction (X \setminus \{a\})$ es una biyección entre $X \setminus \{a\}$ y $n$, de manera que $X \setminus \{a\}$ es finito.

*4*. Supongamos que $X$ es finito. Mostramos de nuevo por inducción natural que para cada $n \in \omega$, si $X \sim n$ entonces todos los subconjuntos de $X$ son finitos. En el caso $n = 0$ la cosa es clara pues $X$ es vacío y el único subconjunto de $\emptyset$ es $\emptyset$. Consideremos ahora el caso inductivo $X \sim n + 1$. Como $X \neq \emptyset$, podemos escoger $a \in X$. Por *3* sabemos que también $X \smallsetminus \{a\}$ es finito. De hecho la prueba de *3* nos indica que $X \smallsetminus \{a\} \sim n$, de manera que podemos aplicar la hipótesis inductiva y garantizar que todos los subconjuntos de $X \smallsetminus \{a\}$ son finitos. Sea $Y$ un subconjunto de $X$. Entonces $Y \smallsetminus \{a\}$ es un subconjunto de $X \smallsetminus \{a\}$ y por tanto es finito. En el caso de que $a \notin Y$ resulta que $Y$ es finito porque $Y = Y \smallsetminus \{a\}$. Y en el caso de que $a \in Y$ tenemos que $Y = (Y \smallsetminus \{a\}) \cup \{a\}$ y por *2* podemos concluir que $Y$ es finito.

**Lema 7.2** *1. Un número natural no es nunca biyectable con un subconjunto propio suyo.*

*2. Si $X$ es un conjunto finito, hay un único número natural $n$ tal que $X \sim n$.*

**Prueba**. *1*. Mostramos por inducción natural que para cada $n \in \omega$, $n$ no es biyectable con ningún subconjunto propio suyo. Ello es claro para el caso inicial $n = 0$ dado que $0 = \emptyset$ no tiene subconjuntos propios. Consideremos el caso inductivo $n + 1$. Supongamos, buscando una contradicción, que existe una biyección $f$ entre $n+1 = n \cup \{n\}$ y un subconjunto propio suyo $X \subsetneq n \cup \{n\}$. Si $X \subseteq n$, entonces $f \restriction n$ es una biyección entre $n$ y $X \smallsetminus \{f(n)\}$, que es un subconjunto propio de $n$. Pero esto contradice a la hipótesis inductiva. Por tanto $X$ no es un subconjunto de $n$, lo cual implica que $n \in X$. Definimos

$$g = (f \smallsetminus \{\langle n, f(n)\rangle, \langle f^{-1}(n), n\rangle\}) \cup \{\langle n, n\rangle, \langle f^{-1}(n), f(n)\rangle\}.$$

Es otra biyección entre $n \cup \{n\}$ y $X$ y tiene la propiedad adicional de que $g(n) = n$. Pero entonces $g \restriction n$ es una biyección entre $n$ y $X \smallsetminus \{n\}$, que es un subconjunto propio de $n$. Esto, de nuevo, contradice a la hipótesis inductiva.

*2*. Supongamos que el conjunto finito $X$ es biyectable con los números naturales $n$ y $m$. Entonces $n \sim m$. Si son números distintos, uno de ellos es menor que el otro y por tanto un subconjunto propio del otro. Pero esto contradice al punto *1*.

**Definición** Si $X$ es un conjunto finito, mediante $|X|$ nos referimos al único número natural con el que $X$ es biyectable. Llamamos a $|X|$ la *cardinalidad* de $X$. Obsérvese que, de acuerdo con esto, para cada número natural $n$, $|n| = n$.

**Observaciones 7.3** *Sea $X$ un conjunto finito.*

1. $|X| \in \omega$.
2. $X \sim |X|$.
3. *Si $n \in \omega$ y $X \sim n$, entonces $|X| = n$.*
4. *Si $Y$ es finito, entonces $X \sim Y$ si y sólo si $|X| = |Y|$.*

**Observaciones 7.4** *1.* $|\emptyset| = 0$.

*2. Si $X$ es finito y $a \notin X$, entonces $|X \cup \{a\}| = |X| + 1$.*

3. *Si $X$ es finito y $a \in X$, entonces $|X| = |X \smallsetminus \{a\}| + 1$.*

4. *Si $X$ es finito e $Y \subseteq X$, entonces $|Y| \leq |X|$.*

**Prueba**. Esencialmente es una repetición de las pruebas de 7.1.

Muy a menudo se establece que todos los conjuntos finitos $X$ tienen una cierta propiedad efectuando una *inducción en* $|X|$. Esto significa que se muestra por inducción en $n$, que para cada número natural $n$, si $|X| = n$, entonces $X$ tiene la propiedad en cuestión. Los casos a analizar son entonces, el caso inicial $|X| = 0$, y el caso inductivo, donde se muestra que los conjuntos $X$ con $|X| = S(n)$ tienen la propiedad usando la hipótesis inductiva según la cual los conjuntos $Y$ con $|Y| = n$ tienen la propiedad.

**Proposición 7.5** *Si $X, Y$ son conjuntos finitos entonces los conjuntos $X \cup Y$ y $X \cap Y$ también son finitos y*

$$|X \cup Y| + |X \cap Y| = |X| + |Y|.$$

*En particular, si $X, Y$ son conjuntos finitos disjuntos, entonces $|X \cup Y| = |X| + |Y|$.*

**Prueba**. Mostramos por inducción en $|Y|$ que si $X, Y$ son finitos y disjuntos, entonces $|X \cup Y| = |X| + |Y|$. De ello se sigue que en general, si $X, Y$ son finitos, entonces $|X \cup Y| + |X \cap Y| = |X| + |Y|$. La razón de que se siga es que $|X \cup Y| + |X \cap Y| = |(X \smallsetminus Y) \cup Y| + |X \cap Y| = (|X \smallsetminus Y| + |Y|) + |X \cap Y| = (|X \smallsetminus Y| + |X \cap Y|) + |Y| = |(X \smallsetminus Y) \cup (X \cap Y))| + |Y| = |X| + |Y|$. Comenzando ya la inducción, vemos que el caso $|Y| = 0$ significa $Y = \emptyset$ y entonces $|X \cap Y| = |X| = |X| + 0 = |X| + |Y|$. Consideramos ahora el caso inductivo. Sea $S(n) = |Y|$ y $X \cap Y = \emptyset$. Entonces $Y \neq \emptyset$, de manera que podemos escoger $a \in Y$. Sea $Y' = Y \smallsetminus \{a\}$. Utilizando ahora las Observaciones 7.4 vemos que $|Y'| = n$. Como también $X \cap Y' = \emptyset$, por la hipótesis inductiva tenemos que $|X \cup Y'| = |X| + |Y'| = |X| + n$. Usando de nuevo las Observaciones 7.4 y además el hecho de que $a \notin X \cup Y$ , concluimos que

$$|X \cup Y| = |(X \cup Y') \cup \{a\}| = |X \cup Y'| + 1 = (|X| + n) + 1 = |X| + S(n) = |X| + |Y|.$$

**Proposición 7.6** *Si $X, Y$ son conjuntos finitos, entonces también $X \times Y$ es finito y*

$$|X \times Y| = |X| \cdot |Y|.$$

**Prueba**. Efectuamos una inducción en $|Y|$. Si $|Y| = 0$, entonces $Y = \emptyset$, con lo cual $X \times Y = \emptyset$ y $|X \times Y| = 0 = |X| \cdot 0 = |X| \cdot |Y|$. Consideremos ahora el caso inductivo $|Y| = S(n)$. Entonces hay $a \in Y$, y si $Y' = Y \smallsetminus \{a\}$, resulta que $|Y'| = n$, de modo que, por hipótesis inductiva, $|X \times Y'| = |X| \cdot n$. Observemos ahora que $X \times Y = (X \times Y') \cup X \times \{a\}$ y que los conjuntos $X \times Y'$ y $X \times \{a\}$ son disjuntos. Aplicando entonces la Proposición 7.5, vemos que

$$|X \times Y| = |X \times Y'| + |X \times \{a\}| = |X| \cdot n + |X \times \{a\}|.$$

Pero es fácil ver que $X \sim X \times \{a\}$, de manera que $|X \times \{a\}| = |X|$. Reuniendo estos datos y usando la definición del producto se concluye que

$$|X \times Y| = |X| \cdot n + |X| = |X| \cdot S(n) = |X| \cdot |Y|.$$

**Proposición 7.7** *Si $X, Y$ son conjuntos finitos, entonces también ${}^{X}Y$ es finito y*

$$|\,{}^{X}Y| = |Y|^{|X|}.$$

**Prueba**. Hacemos inducción en $|X|$. En el caso $|X| = 0|$ tenemos $X = \emptyset$, con lo cual ${}^{X}Y = \{\emptyset\}$ y así $|{}^{X}Y| = |\{\emptyset\}| = 1 = |Y|^0 = |Y|^{|X|}$. Consideramos ahora el caso inductivo $|X| = S(n)$. Escogemos $a \in X$ y ponemos $X' = X \setminus \{a\}$. Por hipótesis inductiva, $|{}^{X'}Y| = |Y|^n$. Observemos que $X'$ y $\{a\}$ son conjuntos disjuntos y $X = X' \cup \{a\}$, de modo que podemos usar la Proposición 5.23 y la Proposición 7.6 para obtener que

$$|{}^{X}Y| = |{}^{X' \cup \{a\}}Y| = |{}^{X'}Y| \cdot |{}^{\{a\}}Y| = |Y|^n \cdot |{}^{\{a\}}Y|.$$

Se comprueba que ${}^{\{a\}}Y \sim Y$ y entonces se puede concluir usando la definición de exponenciación que

$$|{}^{X}Y| = |Y|^n \cdot |Y| = |Y|^{S(n)} = |Y|^{|X|}.$$

**Corolario 7.8** *Si $X$ es finito, entonces también $\mathcal{P}(X)$ es finito y*

$$|\mathcal{P}(X)| = 2^{|X|}.$$

**Prueba**. Se sigue de la Proposición 7.7 usando también la Proposición 5.24.

**Ejercicio 7.9** *Mostrar que la unión de una colección finita de conjuntos finitos es finita.*

**Proposición 7.10** *$\omega$ es infinito.*

**Prueba**. La función sucesor $S : \omega \to \omega$ es inyectiva y su recorrido es $\omega \setminus \{0\}$. Por tanto, es una biyección entre $\omega$ y $\omega \setminus \{0\}$, que es un subconjunto propio de $\omega$. Pero del Lema 7.2 se sigue fácilmente que ningún conjunto finito puede ser biyectable con un subconjunto propio suyo.

**Definición** Sean $X$ e $Y$ conjuntos arbitrarios. Ponemos $X \preceq Y$ y decimos que $X$ *tiene tamaño menor o igual que* $X$ si hay una función inyectiva de $X$ en $Y$. Escribimos $X \prec Y$ y decimos que $X$ *tiene menor tamaño que* $Y$ si $X \preceq Y$ pero no hay ninguna biyección entre $X$ e $Y$, es decir, $X \not\sim Y$.

**Teorema 7.11 (Schröder-Bernstein)** *Si $X \preceq Y$ y $Y \preceq X$, entonces $X \sim Y$.*

**Prueba**. Sean $f : X \to Y$ y $g : Y \to X$ funciones inyectivas. Queremos obtener una biyección entre $X$ e $Y$. Definimos por recursión una función auxiliar $j : \omega \to \mathcal{P}(X)$ mediante las cláusulas

- $j(0) = X \setminus g[Y]$
- $j(S(n)) = g[f[j(n)]]$.

y definimos la función $h : X \to Y$ mediante las cláusulas

- $h(x) = f(x)$ si hay un $n \in \omega$ tal que $x \in j(n)$.
- $h(x) = g^{-1}(x)$ si para cada $n \in \omega$, $x \notin j(n)$.

Observemos antes que nada que la función está bien definida, pues si $x \in X$ pero $x \notin j(n)$ para cada $n \in \omega$, entonces $x \in X \setminus j(0) \subseteq \operatorname{rec} g$, de manera que tiene sentido aplicar $g^{-1}$ a $x$. Verificaremos a continuación que $h$ es inyectiva y exhaustiva, con lo cual quedará establecido que es una biyección entre $X$ e $Y$. Para establecer que es inyectiva, supongamos que $x, y \in X$ son distintos pero que $h(x) = h(y)$ y veremos cómo de ello se obtienen contradicciones. Como tanto $f$ como $g^{-1}$ son inyectivas, la única posibilidad es que uno de ellos, digamos que $x$, pertenezca a algún $j(n)$ mientras que el otro no esté en ningún $j(n)$. Entonces $f(x) = h(x) = h(y) = g^{-1}(y)$. Como $x \in j(n)$, resulta que $g(f(x)) \in g[f[j(n)]] = j(S(n))$. Sin embargo $g(f(x)) = g(g^{-1}(y) = y$, de modo lo que estamos afirmando es que $y \in j(S(n))$, en contra de la hipótesis de que $y$ no pertenecía a ningún valor de $j$.

Finalizamos mostrando que $h$ es exhaustiva. Sea $y \in Y$ y veamos que $y \in \operatorname{rec} h$. Si hay un $n \in \omega$ tal que $y \in f[j(n)]$, entonces $y \in \operatorname{rec} h$, pues $y = h(f^{-1}(y))$. Y si para cada $n \in \omega$ resulta que $y \notin f[j(n)]$, entonces podemos mostrar que para cada $n < \omega$, $g(y) \notin j(n)$. En efecto, si $n = 0$, resulta que $g(y) \notin j(0)$ porque $j(0) \cap \operatorname{rec} g = \emptyset$. Y si $n \neq 0$, entonces hay un $m \in \omega$ tal que $n = S(m)$ y no puede ser que $g(y) \in j(S(m))$ pues $j(S(m)) = g[f[j(m)]]$ y $y \notin f[j(m)]$. Establecido que $g(y)$ no está en ningún valor de $j$, vemos que su valor mediante $h$ debe ser $h(g(y)) = g^{-1}(g(y)) = y$, lo cual establece que $y \in \operatorname{rec} h$ también en este segundo caso.

**Observaciones 7.12** *1.* $X \preceq Y \wedge Y \preceq Z \to X \preceq Z$

*2.* $X \preceq Y \wedge Y \prec Z \to X \prec Z$

*3.* $X \prec Y \wedge Y \preceq Z \to X \prec Z$

**Prueba**. El punto *1* es claro, pues si $f : X \to Y$ es inyectiva y $g : Y \to Z$ es inyectiva, entonces $g \circ f : X \to Z$ es inyectiva. Mostramos *2* y omitimos la prueba de *3*, pues es similar. Supongamos que $X \preceq Y$ y que $Y \prec Z$. Por *1* ya sabemos que $X \preceq Z$. Falta mostrar que $X \not\sim Z$. Supongamos lo contrario, $X \sim Z$. Entonces $Z \preceq Y$, pues $Z \preceq X \wedge X \preceq Y$. Por otro lado $Y \preceq Z$. Aplicando el Teorema 7.11 concluimos que $Y \sim Z$, lo cual contradice a la hipótesis de que $Y \prec Z$.

**Proposición 7.13** *Sean $X, Y$ finitos.*

*1.* $X \preceq Y \leftrightarrow |X| \leq |Y|$

*2.* $X \prec Y \leftrightarrow |X| < |Y|$

**Prueba**. *1*. Supongamos primero que $|X| \leq |Y|$. Por la Proposición 6.25 sabemos que el orden $\leq$ coincide con la inclusión, de manera que $|X| \subseteq |Y|$. Entonces la identidad en $|X|$ es una función inyectiva de $|X|$ en $|Y|$ y así $|X| \preceq |Y|$. Como $X \sim |X|$ y $Y \sim |Y|$, también $X \preceq Y$. Para demostrar la otra dirección, supongamos ahora que $X \preceq Y$. Si no ocurre que $|X| \leq |Y|$, entonces $|Y| < |X|$. En particular $|Y| \leq |X|$ y por lo ya demostrado $Y \preceq X$. Por el Teorema 7.11 $X \sim Y$, con lo cual $|X| = |Y|$. Pero esto contradice a $|Y| < |X|$. El punto *2* se sigue de *1* teniendo en cuenta que $|X| = |Y| \leftrightarrow X \sim Y$.

La siguiente caracterización de la relación $\prec$ de tener menor tamaño se aplica únicamente a conjuntos finitos. Es incorrecta para conjuntos infinitos. Por ejemplo la función sucesor $S : \omega \to \omega$ es inyectiva pero no exhaustiva. Pero eso no significa que $\omega \prec \omega$.

**Proposición 7.14** *Si $X, Y$ son finitos, entonces $X \prec Y$ si y sólo si hay una función inyectiva de $X$ en $Y$ que no es exhaustiva.*

**Prueba**. Con independencia de la finitud, es claro que si $X \prec Y$ existe una función inyectiva de $X$ en $Y$ que no es exhaustiva, pues no hay ninguna biyección entre $X$ e $Y$. Para la otra dirección la finitud de $X$ e $Y$ es esencial. Supongamos que hay una función inyectiva $f : X \to Y$ que no es exhaustiva. Sea $Z = \operatorname{rec} f$. Entonces $Z$ y $Y \setminus Z$ son dos conjuntos finitos disjuntos cuya unión es $Y$. Por tanto $|Y| = |Z| + |Y \setminus Z|$. Como $|Y \setminus Z|$ es un número natural distinto de cero, de la Proposición 6.22 se sigue que $|Z| < |Y|$. Pero $f$ es una biyección entre $X$ y $Z$, de modo que $X \sim Z$ y así $|X| = |Z|$. En definitiva, $|X| < |Y|$. Por la Proposición 7.13 se concluye que $X \prec Y$.

**Lema 7.15** *Supongamos que $\alpha = \omega$ o $\alpha \in \omega$. Sea $<_X$ un orden total del conjunto $X$ y sea $f : \alpha \to X$. Si para cada $n \in \omega$ tal que $S(n) \in \alpha$ se tiene $f(n) <_X f(S(n))$, entonces para cada $n, m \in \alpha$, si $n < m$ entonces $f(n) <_X f(m)$. Además $f$ es inyectiva.*

**Prueba**. Mostramos por inducción en $m$ que si $n, m \in \alpha$ y $n < m$ entonces $f(n) <_X f(m)$. El caso $m = 0$ no ofrece dificultades dado que el antecedente es falso. Consideremos el caso $S(m)$. Sea $n < S(m)$. Entonces $n \leq m$. Si $n = m$ tenemos $f(n) = f(m) <_X f(S(m))$ por la hipótesis del lema. Y si $n < m$ obtenemos por hipótesis inductiva que $f(n) <_X f(m)$. Como $f(m) <_X f(S(m))$, concluimos también en este caso que $f(n) <_X f(S(m))$. La inyectividad de $f$ se obtiene de modo inmediato a partir de lo ya establecido, pues si $m, n \in \alpha$ y $m \neq n$, entonces $m < n$ o $n < m$, con lo cual $f(n) <_X f(m)$ o $f(m) <_X f(n)$. En cualquier caso $f(n) \neq f(m)$.

**Proposición 7.16** *El Principio del Buen Orden implica que para cada conjunto infinito $X$, $\omega \preceq X$.*

**Prueba**. Sea $X$ un conjunto infinito arbitrario. Por el Principio del Buen Orden existe un buen orden $<_X$ de $X$.Sea $a$ el menor elemento de $X$. Sea $f : \mathcal{P}(X) \to X$ la función que asigna a cada subconjunto no vacío $Y$ de $X$ el menor elemento $f(Y)$ de $Y$ en el buen orden $<_X$ y que asigna a $\emptyset$ el menor elemento $a$ de $X$. Usando la Proposición 6.2 definimos ahora la función $g : \omega \to X$ mediante las cláusulas

1. $g(0) = a$
2. Para cada $n \in \omega$, $g(S(n)) = f(\{x : x \in X \wedge x >_X g(n)\})$

Mostraremos ahora que $g$ es inyectiva, lo cual dará el resultado de que $\omega \preceq X$. Supongamos primero que para cada $n \in \omega$ el conjunto $\{x : x \in X \wedge x >_X g(n)\}$ es no vacío. En ese caso $g(S(n)) >_X g(n)$ para cada $n \in \omega$ pues $g(S(n)) \in \{x : x \in X \wedge x >_X g(n)\}$. Por el Lema 7.15, de ello se sigue que $g$ es inyectiva. Por tanto $\omega \preceq X$. Supongamos ahora que hay un $n \in \omega$ para el que $\{x : x \in X \wedge x >_X g(n)\} = \emptyset$. Escojamos $n$ mínimo con tal propiedad. Entonces para cada $m \in \omega$ tal que $S(m) \leq n$ se tiene como antes que $g(m) <_X g(S(m))$. Usando de nuevo el Lema 7.15 tenemos que para $m, k \leq n$, si $m < k$, entonces $g(m) <_X g(k)$. En particular $g \restriction S(n)$ es inyectiva. Veremos que de hecho es una biyección entre $S(n)$ y $X$, con lo cual $X$ no puede ser infinito. Sea $x \in X$. Debe ser $x \leq_X g(n)$ ya que no puede ser $x >_X g(n)$. Hay entonces un menor $m \in \omega$ tal que $m < S(n)$ y $x \leq_X g(m)$. Si $m = 0$, entonces $x = a$ y por tanto $x \in g[S(n)]$. Y si $m \neq 0$, entonces hay $k$ tal que $S(k) = m$. En ese caso $g(k) <_X x \leq g(m)$. Pero entonces $x = g(m)$ pues $g(m) = g(S(k))$ se ha definido precisamente como el menor elemento de $X$ que es mayor que $g(k)$ en $<_X$. En definitiva, para cada $x \in X$ hay siempre un $m < S(n)$ tal que $g(m) = x$. Esto significa que $g \restriction S(n)$ es una función exhaustiva de $S(n)$ en $X$ y por ello una biyección entre $S(n)$ y $X$. Pero esto entra en contradicción con la infinitud de $X$.

Usando el Principio del Buen Orden podemos caracterizar ahora a los conjuntos finitos como los conjuntos que no son biyectables con ningún subconjunto propio. Esta caracterización tiene la ventaja de que no presupone los números naturales en su formulación.

**Corolario 7.17** *El Principio del Buen Orden implica que para cada conjunto $X$, $X$ es finito si y sólo si $X$ no es biyectable con un subconjunto propio suyo.*

**Prueba**. El hecho de que si $X$ es finito entonces no es biyectable con ningún subconjunto propio se sigue del Lema 7.2. Para la otra dirección, supongamos que $X$ es infinito y veamos que $X$ es biyectable con un subconjunto propio. Por la Proposición 7.16 sabemos que $\omega \preceq X$, de manera que hay una función inyectiva $f : \omega \to X$. Sea $Y = \operatorname{rec} f$ y sea $a = f(0)$. Del mismo modo que la función sucesor $S$ es una biyección entre $\omega$ y $\omega \smallsetminus \{0\}$, la composición $g = f \circ S \circ f^{-1}$ es una biyección entre $Y$ y $Y \smallsetminus \{a\}$. Entonces la función $h = g \cup I_{X \smallsetminus Y}$ es una biyección entre $X$ y $X \smallsetminus \{a\}$, que es un subconjunto propio de $X$.

Para finalizar, enunciamos una proposición que asegura que entre los conjuntos de tamaño infinito no es posible encontrar uno mayor que todos los demás. Hay, por tanto, infinitos tamaños posibles para los conjuntos infinitos.

**Proposición 7.18** *Para cada conjunto $X$ existe un conjunto $Y$ tal que $X \prec Y$.*

**Prueba**. Sea $X$ un conjunto arbitrario. La función $f : X \to \mathcal{P}(X)$ definida por $f(x) = \{x\}$ es inyectiva. Por tanto $X \preceq \mathcal{P}(X)$. Pero por el Teorema 5.22 sabemos que $X \not\sim \mathcal{P}(X)$. Uniendo estos resultados se concluye que $X \prec \mathcal{P}(X)$.

Con un poco más de trabajo se puede demostrar que para cada conjunto $X$ existe un conjunto $Y$ cuyo tamaño es estrictamente mayor que el de $X$, es decir, no hay tamaños intermedios entre el de $X$ y el de $Y$. Usando el Principio del Buen Orden se puede establecer a continuación que los tamaños infinitos comienzan con el tamaño del conjunto $\omega$ de los números naturales, tamaño que se designa mediante $\aleph_0$, y que a este tamaño le siguen inmediatamente los tamaños $\aleph_1, \aleph_2, \ldots$. Los conjuntos de los números enteros y de los números racionales tienen el tamaño $\aleph_0$, pero el conjunto de los números reales tiene tamaño $2^{\aleph_0}$, que es mayor o igual que $\aleph_1$. La *Hipótesis del Continuo* sostiene que $2^{\aleph_0} = \aleph_1$.

La cuestión de si hay conjuntos que tengan tamaño superior a todos los $\aleph_n$ obtenidos con los distintos números naturales $n \in \omega$ no puede resolverse con los axiomas que hemos introducido hasta el momento, ni siquiera usando el Principio del Buen Orden. Este problema se resuelve en sentido positivo si se añade el *Esquema Axiomático del Reemplazo*. La teoría presentada hasta el momento es la teoría Z de Zermelo. Este esquema de axiomas añadido a la teoría Z de Zermelo nos da la teoría ZF de Zermelo-Fraenkel. Formulamos el Esquema de Reemplazo usando la noción de relación en un sentido intuitivo, sin presuponer que se trate de un conjunto, del mismo modo que usábamos la noción de propiedad para formular el Esquema de Separación. El Esquema del Reemplazo establece entonces que para cada relación $R(x, y)$ expresable mediante una fórmula de la lógica de primer orden en el lenguaje de nuestra teoría se verifica lo siguiente:

$$\forall xyz(R(x, y) \wedge R(x, z) \rightarrow y = z) \rightarrow \forall u \exists v \forall y(y \in v \leftrightarrow \exists x(x \in u \wedge R(x, y))).$$

Para completar la lista de axiomas de la teoría ZF conviene decir un par de palabras sobre el *Axioma de Regularidad*. Muy a menudo se añade a los axiomas ya enunciados. Es el enunciado siguiente:

$$\forall x(x \neq \emptyset \rightarrow \exists y(y \in x \wedge y \cap x = \emptyset)).$$

Este axioma contribuye a simplificar ciertas demostraciones, incluso en el desarrollo de las propiedades de los números naturales. Por otro lado al añadirlo a nuestro sistema axiomático podemos explicar con cierto rigor cuáles son los conjuntos que existen pues son los que se obtienen efectuando ciertas operaciones que proporcionan la llamada *jerarquía acumulativa* o *jerarquía de von Neumann*. Pero estas cuestiones exceden los límites de estas notas.

**Ejercicio 7.19** *Demostrar usando el Axioma de Regularidad que no hay ningún conjunto* $x$ *tal que* $x \in x$ *y también que no hay conjuntos* $x, y$ *tales que* $(x \in y \wedge y \in x)$.

# Bibliografía


[1] H. B. Enderton. *Elements of Set Theory.* Academic Press, New York, 1977.

[2] P. Halmos. *Naive Set Theory.* Springer–Verlag, Berlin, 1974.

[3] R. L. Vaught. *Set Theory. An Introduction.* Birkhäuser, Boston, second edition, 1995.

# Índice alfabético


$A/E$, 26
$A \,\Delta\, B$, 13
$A \cap B$, 11
$A \cup B$, 11
$A \smallsetminus B$, 11
$A \subseteq B$, 5
$A \times B$, 19
$I_A$, 21
$R \mid S$, 21
$S$, 49
$X \prec Y$, 59
$X \preceq Y$, 59
$X \sim Y$, 43
$[a]_E$, 26
${}^XY$, 38
$\aleph_n$, 62
$\bigcap \Phi$, 15
$\bigcup \Phi$, 15
$\breve{R}$, 21
campo $R$, 20
dom $R$, 20
$\emptyset$, 8
$\exp(n, m)$, 51
$\langle x, y\rangle$, 18
$\omega$, 49
$\overline{A}$, 14
rec $R$, 20
$\{x, y\}$, 9
$\{x : P(x)\}$, 6
$\{x\}$, 9
$\{x_1, \ldots, x_n\}$, 9
$f(a)$, 36
$f : A \to B$, 36
$f[X]$, 41
$f \circ g$, 40
$f \restriction X$, 41
$f^{-1}$, 39
$f^{-1}[X]$, 42
$n + m$, 50
$n \cdot m$, 51
$n^m$, 51
$x < y$, 30
$xRy$, 20
$x \in y$, 4
$x \leq y$, 30
$\mathcal{P}(A)$, 14
$|X|$, 57

abstractor, 6, 16
alephs, 3, 62
aplicación de $A$ en $B$, 36
argumento, 36
Axioma
  de Elección, 37
  de Existencia de Conjuntos, 8
  de Existencia de Conjuntos Finitos, 9
  de Extensionalidad, 5, 20, 37
  de Regularidad, 63
  de Uniones, 11, 15
  del Conjunto Potencia, 14
  del Infinito, 48
axioma, 5

biyección, 39
biyectable, 43
buen orden, 31

cadena, 33
campo, 20
cardinalidad, 3, 43, 57
caso inductivo, 51
clase de equivalencia, 26
complemento, 14
componente, 18
composición
  de funciones, 40
  de relaciones , 21
conjunto, 4
  cociente, 26
  denso, 34
  inductivo, 48

potencia, 14
transitivo, 49
unitario, 9
universal, 8
vacío, 8
coordenada, 18
corolario, 5
cota
inferior, 32
inferior estricta, 32
superior, 32
superior estricta, 32
cuantificación acotada, 16

definición, 5
diferencia, 11
diferencia simétrica, 13
dominio, 20

elemento, 4
maximal, 32
minimal, 32
Esquema Axiomático
de Separación, 7
del Reemplazo, 62
exponenciación, 51

finito, 56, 62
función, 36
biyectiva, 39
exhaustiva, 39
inyectiva, 38
uno a uno, 38
función de $A$ en $B$, 36

gran
intersección, 15
unión, 15

Hipótesis del Continuo, 3, 62
hipótesis inductiva, 51

identidad, 21
igual tamaño, 43
igualdad, 5
imagen, 41
inversa, 42
inclusión, 5, 13
inducción, 51
en $n$, 51
en $|X|$, 58
ínfimo, 33
infinito, 56, 62
intersección, 11
intervalo, 35
isomorfía, 34, 47
isomorfismo, 47

jerarquía acumulativa, 63

lema, 5
Lema de Zorn, 33, 37

máximo, 31
mínimo, 31
mayor elemento, 31
menor elemento, 31
menor tamaño, 59, 60
multiplicación, 51

números cardinales, 3
números naturales, 49

objeto, 4
objeto primitivo, 4
orden, 28
de $\omega$, 53
denso, 34
discreto, 34
estricto, 28
estricto asociado, 30
parcial, 28
reflexivo, 28
reflexivo asociado, 30
total, 30

par, 9
ordenado, 18
Paradoja
de Richard, 7
de Russell, 6
partición, 27
pertenencia, 4, 6
predecesor, 34
inmediato, 34
Principio del Buen Orden, 31, 33, 37
producto, 51
cartesiano, 19
proposición, 5

recorrido, 20
recursión, 46, 49
relación, 20
antisimétrica, 23

asimétrica, 23
de buen orden, 31
de equivalencia, 26
de orden
estricto, 28
parcial, 28
reflexivo, 28
total, 30
en $A$, 20
inversa, 21
irreflexiva, 23
reflexiva, 23
reflexiva en $A$, 23
simétrica, 23
transitiva, 24
restricción, 41

segmento inicial, 35
sistema de Peano, 46
subconjunto, 5
sucesor, 34
inmediato, 34
suma, 50
supremo, 33

teoría, 4
de Zermelo, 62
de Zermelo-Fraenkel, 62
Teorema
de Cantor, 44
de Schröder-Bernstein, 59
teorema, 5

unión, 11

valor, 36

ZF, 32, 37, 62
ZFC, 37