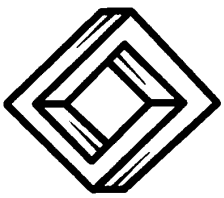
Publicaciones Electrónicas
Sociedad Matemática Mexicana

Lógica, Conjuntos, Relaciones y Funciones.

Álvaro Pérez Raposo

www.sociedadmatematicamexicana.org.mx

Serie: Textos. Vol. 12 (2010)



Lógica, conjuntos, relaciones y funciones

Álvaro Pérez Raposo
Universidad Autónoma de San Luis Potosí
Universidad Politécnica de Madrid

Publicaciones Electrónicas
Sociedad Matemática Mexicana

A la memoria de mi madre,
Cecilia Raposo Llobet.

Prólogo

Este libro es una exposición muy elemental de los tópicos fundamentales de las matemáticas que anuncia el título: lógica, conjuntos, relaciones y funciones. Mi aportación es tener un libro en español, elemental y riguroso. Todos los resultados enunciados tienen su demostración y sigo el esquema habitual de una teoría matemática de axiomas, definiciones y teoremas, todos ellos entrelazados por las reglas de la lógica. La otra característica que he buscado al escribirlo es la brevedad. Se ha conseguido un libro con un contenido importante pero expuesto en pocas páginas. A pesar de ello no carece de explicaciones o ejemplos allí donde se han creído necesarios.

El primer capítulo trata de lógica. Es una exposición de los principios de la lógica que se usan en matemáticas para desarrollar sus teorías. Partiendo de la definición de variable lógica, se llega hasta el concepto de razonamiento lógico, que es el que permite demostrar teoremas. En este capítulo todas las demostraciones de resultados se han hecho mediante tablas. Es un método que se puede evitar en algunos casos, pero es más seguro cuando aún no se ha expuesto en qué consiste un razonamiento lógico. Desde el punto de vista del primer capítulo, podemos pensar en un libro de lógica (capítulo 1) con un ejemplo, la teoría de conjuntos, desarrollado en detalle (capítulos 2, 3 y 4).

El segundo capítulo expone los axiomas y definiciones iniciales de la teoría de conjuntos, además del álgebra de las operaciones habituales de complemento, unión e intersección. He optado por un desarrollo axiomático riguroso de la teoría. Sin embargo no uso el sistema completo de axiomas de Zermelo y Fraenkel, sino una simplificación del mismo reducida a cinco axiomas. La reducción es posible porque no distingo entre clases y conjuntos ni entro en el terreno de los conjuntos ordinales ni de los cardinales, por lo cual la exposición es elemental. A partir de los axiomas y las definiciones introducidas se van demostrando teoremas según las reglas de inferencia lógica expuestas en el capítulo anterior.

El tercer capítulo trata de relaciones, que son la forma de agrupar y ordenar los elementos de un conjunto. En particular se analizan las relaciones de equivalencia y las relaciones de orden parcial y total.

El cuarto capítulo está dedicado a la idea de función que, junto con la de conjunto, es el concepto más fructífero en matemáticas. Este capítulo describe todo el material necesario para llegar a dos teoremas: el que caracteriza las funciones invertibles como las biyectivas y el de descomposición canónica de una función.

Desde el punto de vista de estos tres últimos capítulos, el libro se puede ver como un libro de teoría elemental de conjuntos con un capítulo previo de lógica.

Bajo cualquiera de las dos interpretaciones, se trata de un libro de texto dirigido a alumnos de primer curso de matemáticas, física, ingeniería o, en general, a cualquier estudiante que desee adquirir soltura en el manejo de estos conceptos, que son herramientas comunes en los cursos de cálculo y álgebra. No está pensado como un libro de autoestudio, sino como un libro para seguir con la guía de un profesor. Cada capítulo contiene, al final, una lista de ejercicios propuestos al lector que tienen la misión de analizar ejemplos concretos de la teoría revisada. También hay algunos ejercicios en los que se amplía ésta pues se propone demostrar algún resultado. Los ejercicios considerados de mayor dificultad se han marcado con un asterisco.

No presupongo conocimientos de lógica o conjuntos en el lector. Sin embargo sí uso propiedades de los números naturales, enteros, racionales, reales y complejos, aunque nunca en el desarrollo de la teoría, sino en los ejemplos o en algunos ejercicios. Las demostraciones de los teoremas se concluyen con el símbolo □.

Quiero aprovechar estas líneas para expresar mi agradecimiento a la Sociedad Matemática Mexicana por la publicación de este libro en su sección de publicaciones electrónicas, cuya iniciativa de poner los libros a disposición de los lectores interesados de forma completamente gratuita me parece acertadísima. Asimismo, agradezco a los revisores las sugerencias que hicieron pues han contribuido a mejorar la presentación de este texto. Por último agradezco a los estudiantes de la Facultad de Ciencias de la Universidad Autónoma de San Luis Potosí el buen recibimiento que dieron a una versión previa de este libro pues con ello me animaron a completar esta versión definitiva, muy mejorada con la experiencia de la interacción con ellos.

Índice general

Capítulo 1

Lógica

Este primer capítulo es una breve introducción a la lógica, que es la herramienta que usan las matemáticas para desarrollarse. El objetivo del mismo es describir en qué consiste una teoría matemática. Para lograrlo, primero hay que exponer sucintamente las reglas de la lógica de proposiciones, definir con precisión qué es un razonamiento lógico y, por último, explicar en qué consiste una teoría matemática (brevemente, una serie de axiomas, definiciones y teoremas relacionados entre sí mediante argumentos lógicos).

La lógica es un esquema de reglas que permite deducir verdades a partir de otras verdades. El medio que lleva de las primeras verdades a las otras deducidas se llama razonamiento lógico. La lógica estudia, precisamente, los razonamientos lógicos, estableciendo cuándo un razonamiento es válido, independientemente del contenido de las verdades que se enuncien. Sólo le interesan las manipulaciones que se hacen con los enunciados, no su contenido.

Todos los resultados mostrados en este capítulo se prueban rigurosamente. Sin embargo, no se usa para ello el razonamiento lógico, que se define en la sección 1.5, sino el simple y eficaz camino de las tablas introducidas en la sección 1.1. Por supuesto, algunos resultados sí se podrían demostrar a partir de otros anteriores mediante las leyes del álgebra de proposiciones, que se exponen en la sección 1.3. Pero hemos preferido dejar todo el capítulo en manos de las tablas, pues en el resto del libro son los argumentos lógicos los protagonistas.

Por contra, aunque hasta la sección 1.6 no hablamos de axiomas, definiciones y teoremas en las teorías matemáticas, desde el principio llamamos teoremas a los resultados que vayamos obteniendo.

1.1. Proposiciones y variables lógicas

Puesto que la lógica busca deducir verdades a partir de otras verdades, su materia prima son los enunciados de esas verdades. Eso es lo que llamamos proposiciones: un enunciado que se puede juzgar como verdadero o falso.

1.1 Ejemplo. El enunciado "$\sqrt{2}$ es un número racional" es una proposición,

pues se puede juzgar que es falso. Pero los enunciados "los números enteros son interesantes" o "los números complejos son más complicados que los reales" no son proposiciones, pues no pueden ser juzgados objetivamente.

Deliberadamente no escribimos una definición formal del concepto de proposición en nuestra teoría por dos razones. Primero, en mucho casos es cuestión de opinión si un enunciado se puede juzgar como verdadero o falso, o simplemente, el juicio no será unánime. La segunda razón es que las proposiciones no son parte de la lógica. Son los ladrillos con los que se construyen los razonamientos lógicos. Sin embargo, no son parte de la lógica. La lógica se ocupa de las relaciones entre las proposiciones, no de su contenido.

No nos interesa, pues, estudiar cada proposición en particular. Por ello debemos usar símbolos que representen proposiciones cualesquiera y estudiar las relaciones entre estos símbolos independientemente de su contenido particular. Utilizaremos letras latinas minúsculas, especialmente $p, q, r, s, t \ldots$ para representar proposiciones cualesquiera. La única característica que nos recuerda que representan proposiciones es que estos símbolos pueden tener dos valores: verdadero o falso. Y como representan proposiciones cualesquiera, pueden tomar cualquiera de los dos. Estos símbolos no son proposiciones sino variables, y sí damos una definición formal de ellos; la primera del libro.

1.2 Definición. *Una* variable lógica *o* variable proposicional *es un símbolo que puede tomar dos valores: verdadero (representado por 1) o falso (representado por 0).*

Sin embargo, una vez aclarada la diferencia entre proposiciones y variables lógicas, y puesto que una variable lógica representa una proposición cualquiera, emplearemos los dos términos indistintamente.

En definitiva, nuestro estudio de la lógica va a consistir en analizar variables lógicas y describir las relaciones entre ellas. La relación más sencilla es la de variables dependientes e independientes.

1.3 Definición. *Dos variables lógicas son* dependientes *si el valor que tome una condiciona el valor que puede tomar la otra. Son* independientes *si no son dependientes.*

Representamos las variables lógicas por letras como $p, q, r, \ldots$ Si en una expresión aparecen las variables p y q, ambas pueden tomar los valores 0 y 1, y tenemos un total de cuatro combinaciones posibles de los valores de p y q. Si tenemos tres variables, hay ocho posibilidades (2^3). Una tabla de verdad, o simplemente tabla en este contexto, es una representación en filas y columnas de los valores de algunas variables lógicas. Cada columna representa una variable, y cada fila una posible combinación de los valores de las mismas. En las siguientes tablas se muestran todas las posibles combinaciones de los valores 0 y 1 para dos y tres variables.

p	q
0	0
0	1
1	0
1	1

p	q	r
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

Como ya se ha dicho, una variable lógica puede, en principio, tomar los valores 0 ó 1. Sin embargo, es posible que una variable dependiente de otras, cuyo valor queda condicionado por éstas, tome siempre el valor 1 (verdadero) para cualquier situación de las variables de las que depende. O bien, otra variable que tome siempre el valor 0 (falso). Las variables con este comportamiento reciben un nombre.

1.4 Definición. *Se llama* tautología *a la variable lógica, dependiente de otras, la cual toma el valor 1 independientemente del valor de las variables de las que depende. Análogamente se llama* contradicción *a la variable lógica cuyo valor es 0 en cualquier situación.*

1.2. Conectores de proposiciones

Los conectores permiten construir nuevas proposiciones a partir de unas dadas. La nueva proposición es dependiente de las proposiciones con las que se construye.

Vamos a estudiar un conector monario llamado negación el cual, a partir de una proposición, construye otra. También varios conectores binarios, que a partir de dos proposiciones dan otra: conjunción, disyunción, implicación y doble implicación. En los cinco casos daremos una explicación intuitiva seguida de una definición formal. La definición formal consiste en describir exactamente cómo depende la nueva proposición de las proposiciones con que se construye. Hacemos esta descripción mediante tablas en las que aparecen todas las combinaciones posibles de valores que toman las variables independientes.

Empezamos por la negación de una proposición, que es otra proposición con valor opuesto a la primera. Si la primera es cierta, su negación es falsa y viceversa.

1.5 Ejemplo. La negación de la proposición "-5 es un número entero" es la proposición "-5 no es un número entero".

En términos de variables lógicas, la negación de una variable es otra variable dependiente de la primera porque su valor está determinado por el de ella. A continuación, su definición.

1.6 Definición. *La* negación *de una proposición p, denotada $\neg p$, es la proposición cuyo valor es el opuesto al de p.*

Se puede definir la negación mediante la siguiente tabla. En ella se indica, para cada valor de la proposición p, el valor que toma la proposición $\neg p$.

p	$\neg p$
0	1
1	0

La conjunción es un conector binario que funciona como la conjunción copulativa "y" del español. La conjunción de dos proposiciones, entonces, es una proposición que es cierta si ambas son ciertas, y es falsa si alguna de ellas es falsa.

1.7 Ejemplo. "3 es menor que 5 y 5 es menor que 7" es una proposición cierta, porque las dos proposiciones que la componen son ciertas, pero "3 es menor que 5 y 8 es menor que 4" es falsa porque una de ellas es falsa. También es falsa "5 es menor que 3 y 8 es menor que 4".

1.8 Definición. *La* conjunción *de dos proposiciones p, q, denotada $p \wedge q$, es la proposición que sólo es cierta si ambas son ciertas.*

La definición mediante una tabla consiste ahora en ilustrar, para cada valor que pueden tomar las proposiciones p y q, el valor que resulta en la proposición $p \wedge q$.

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

La disyunción es el conector que opera de forma parecida a la conjunción disyuntiva "o" del español. La disyunción de dos proposiciones es otra proposición que es cierta si alguna de las dos originales es cierta. Es decir, basta que una de ellas sea cierta para que la disyunción lo sea.

1.9 Ejemplo. "3 es menor que 5 ó 9 es menor que 7" es cierta ya que una de las dos afirmaciones es cierta.

En el lenguaje habitual, la conjunción disyuntiva "o" se suele emplear en sentido exclusivo: sólo es cierta si una de las proposiciones es cierta y la otra es falsa. Así ocurre, por ejemplo, cuando decimos "voy al cine o me quedo en casa". Sin embargo en lógica se emplea en sentido inclusivo como se aprecia en la tabla que la define.

1.10 Definición. *La* disyunción *de dos proposiciones p, q, denotada $p \vee q$, es la proposición que sólo es falsa si ambas son falsas.*

En forma de tabla

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

El siguiente conector que introducimos es la implicación, que tiene gran importancia en la lógica pues es la base del razonamiento deductivo. Requiere un poco de atención para entender bien su definición formal que, al principio, no parece responder a la intuición. Cuando decimos que una proposición implica otra queremos expresar el hecho de que si la primera es cierta, entonces la segunda debe ser cierta también.

1.11 Ejemplo. "Si $2 < 3$, entonces $10 < 15$" es una implicación.

En el lenguaje corriente se usa la expresión "Si ... entonces ...". Las dos proposiciones que aparecen en la implicación se llaman antecedente y consecuente. El antecedente es la condición que, si es cierta, asegura que se cumple el consecuente. En el ejemplo anterior, $2 < 3$ es el antecedente, mientras que $10 < 15$ es el consecuente.

Para dar una definición formal debemos, como en las definiciones anteriores, decir qué valor tiene la implicación en cada caso de los posibles valores de antecedente y consecuente. Es claro que quiero decir que una implicación es cierta si el antecedente es cierto y el consecuente también, como ocurre en el ejemplo anterior. Si el antecedente es verdadero y el consecuente falso no se está dando la implicación y, por tanto, digo que es falsa, como en la implicación "si $2 < 3$ entonces $5 < 4$". Quedan los dos casos en que el antecedente es falso, como la implicación "si $3 < 2$ entonces ...". Pero, siendo falso el antecedente, no obliga a nada al consecuente así que ambas opciones (consecuente verdadero o falso) son válidas y debo considerar que la implicación se ha cumplido (ya que no se ha incumplido).

Por todo ello definimos la implicación del siguiente modo.

1.12 Definición. *La* implicación *de dos proposiciones p, q, denotada $p \to q$, es la proposición que sólo es falsa si p es verdadera y q es falsa.*

La tabla correspondiente es

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

Es fácil convencerse de que la proposición $p \to q$ no es la misma que $q \to p$. Basta ver la tabla de la definición anterior o analizar un ejemplo sencillo: Mientras que la implicación "si un número es real entonces su cuadrado es real" la damos por buena, al darle la vuelta obtenemos "si el cuadrado de un número

es real, entonces dicho número es real", la cual no es cierta porque el número complejo i, que no es real, cumple $i^2 = -1$. Esta observación es suficientemente importante como para asignar nombres a cada una de estas implicaciones.

1.13 Definición. *Dada una implicación $p \to q$, otorgamos nombres a las siguientes implicaciones:*

$p \to q$	implicación directa,
$q \to p$	implicación inversa,
$\neg p \to \neg q$	implicación recíproca,
$\neg q \to \neg p$	implicación contrapositiva.

El último conector que introducimos es el de doble implicación o bicondicional. Como su nombre indica, si dos proposiciones están relacionadas con el conector doble implicación, significa que una implica la otra y la otra la una. Entonces, si una de ellas es cierta, la otra debe serlo también, que es lo mismo que decir que si una es falsa la otra también.

Por ello damos la siguiente definición.

1.14 Definición. *La* doble implicación *de dos proposiciones p, q, denotada $p \leftrightarrow q$ es la proposición que sólo es verdadera si ambas coinciden en su valor.*

En forma de tabla resulta

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Una definición que podemos enunciar a partir de la doble implicación es la de variables lógicas equivalentes. La idea es que dos variables son equivalentes si son dependientes de modo que siempre toman el mismo valor. Si una es verdadera, entonces la otra también y viceversa. Es claro que el conector de doble implicación puede ayudar a expresar esta idea. Una forma de hacerlo es decir que la doble implicación entre dos proposiciones equivalentes es siempre cierta, que es la siguiente definición.

1.15 Definición. *Dos variables p y q son* equivalentes*, y se denota $p \Leftrightarrow q$, si $p \leftrightarrow q$ es una tautología.*

Es claro que en cualquier expresión puedo sustituir una proposición por otra equivalente, y la nueva expresión que obtengo es equivalente a la original pues los valores son los mismos. De ahí que el concepto de proposiciones equivalentes sea importante y muy utilizado en lógica.

Ahora podemos enunciar un primer resultado sencillo pero muy útil en la teoría y en la práctica de la lógica. Es la relación entre las implicaciones directa, inversa, recíproca y contrapositiva.

1.16 Teorema. *Las implicaciones directa y contrapositiva son equivalentes, y las implicaciones inversa y recíproca son equivalentes.*

Simbólicamente

$$\begin{aligned} p \to q &\quad \Leftrightarrow \quad \neg q \to \neg p, \\ q \to p &\quad \Leftrightarrow \quad \neg p \to \neg q. \end{aligned}$$

Demostración. Probamos la primera equivalencia, pues la otra es similar. Para ello basta con elaborar una tabla con todos los casos posibles y ver que, efectivamente, en todos ellos las proposiciones directa y contrapositiva toman el mismo valor. Obsérvese que las columnas $\neg p$ y $\neg q$ son auxiliares en esta tabla, pues el objetivo es comparar las columnas etiquetadas como $p \to q$ y $\neg q \to \neg p$.

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg q \to \neg p$
0	0	1	1	1	1
0	1	1	0	1	1
1	0	0	1	0	0
1	1	0	0	1	1

Por tanto, de la tabla anterior construimos la siguiente

p	q	$(p \to q) \leftrightarrow (\neg q \to \neg p)$
0	0	1
0	1	1
1	0	1
1	1	1

donde se ve que la bicondicional es una tautología, pues en cualquiera de los cuatro casos el resultado es la constante 1. □

1.17 Ejemplo. Fijémonos en la implicación "si un número es mayor que 10 entonces es mayor que 5". Es equivalente a decir "si un número no es mayor que 5 entonces no es mayor que 10", que es su contrapositiva.

Sin embargo no es equivalente a su implicación inversa, que es "si un número es mayor que 5 entonces es mayor que 10", pues cualquier número entre 5 y 10 muestra que no es cierta, mientras que la original sí lo es. Tampoco es equivalente a la recíproca, "si un número no es mayor que 10 entonces no es mayor que 5".

Otro teorema relacionado con el concepto de equivalencia es la que dice que el conector doble implicación es equivalente a la implicación directa junto con la implicación inversa. Es la formulación precisa de lo que el símbolo $\leftrightarrow$ expresa abiertamente.

1.18 Teorema. *La doble implicación es equivalente a la conjunción de las implicaciones directa e inversa. Es decir,*

$$((p \to q) \wedge (q \to p)) \Leftrightarrow (p \leftrightarrow q).$$

Demostración. Como antes, basta elaborar las tablas de ambas proposiciones y comprobar que sus resultados son iguales para todos los valores posibles de p

y q. En este caso las dos últimas columnas deben ser iguales, mientras que las columnas $p \to q$ y $q \to p$ son auxiliares.

p	q	$p \to q$	$q \to p$	$(p \to q) \wedge (q \to p)$	$p \leftrightarrow q$
0	0	1	1	1	1
0	1	1	0	0	0
1	0	0	1	0	0
1	1	1	1	1	1

□

Por ser la doble implicación como dos implicaciones, se acostumbra a leer $p \leftrightarrow q$ también con la fórmula "p si, y sólo si, q" (ver ejercicio 1.5).

1.19 Ejemplo. La proposición "el número entero a es mayor que b si, y sólo si, la diferencia $a - b$ es positiva" significa que si a es mayor que b, entonces tenemos la seguridad de que la diferencia $a - b$ es un número positivo y, al revés, que si la diferencia $a - b$ es positiva, entonces sabemos que a es mayor que b.

1.3. Leyes del álgebra proposicional

Los conectores entre proposiciones (negación, conjunción, disyunción, etc.) se pueden ver, desde un punto de vista algebraico, como operaciones definidas en el conjunto de las proposiciones. Se toma una proposición (en el caso de la negación) o dos proposiciones (en los otros casos) y se operan, obteniendo como resultado otra proposición.

Bajo este punto de vista resulta imperativo estudiar algunas propiedades algebraicas de estas operaciones como son la aplicación reiterada, asociatividad, conmutatividad, existencia de elemento neutro, etc.

Como primer paso veamos que los conectores de implicación y doble implicación se pueden escribir en términos de la negación, conjunción y disyunción solamente. Entonces bastará con estudiar las propiedades algebraicas de estas tres operaciones. (En realidad, también el conector de disyunción se puede expresar en función del de conjunción y el de negación, pero estos tres en conjunto tienen más y mejores propiedades algebraicas. Ver ejercicio 1.3).

1.20 Teorema. *La implicación de dos proposiciones es equivalente a la disyunción de la negación de la primera con la segunda.*

$$(p \to q) \Leftrightarrow (\neg p \vee q).$$

Demostración. Construimos las tablas de ambas con la columna auxiliar $\neg p$.

p	q	$\neg p$	$p \to q$	$(\neg p \vee q)$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	0	1	1

La coincidencia de las dos últimas columnas en todos los casos demuestra que ambas proposiciones son equivalentes. □

Por tanto, en cualquier expresión podemos sustituir $p \to q$ por $\neg p \vee q$ y viceversa.

Puesto que ya vimos en el teorema 1.18 que la doble implicación es equivalente a la implicación directa y la inversa, entonces la doble implicación también se puede expresar sólo con negación, conjunción y disyunción.

En definitiva, estudiemos las propiedades de la negación, la conjunción y la disyunción.

1.3.1. Propiedades de la negación

Debido a que la negación es una operación monaria, la única propiedad que en este caso puede analizarse es la aplicación reiterada. El resultado es muy evidente por estar trabajando con proposiciones que sólo pueden tomar dos valores. La negación es cambiar el valor de una proposición, y como sólo hay dos posibilidades, si se cambia dos veces regresamos al valor original.

1.21 Teorema. *La negación de la negación es equivalente a la proposición original. Es decir,*

$$\neg(\neg p) \Leftrightarrow p.$$

Demostración. Construimos una tabla

p	$\neg p$	$\neg(\neg p)$
0	1	0
1	0	1

Puesto que la primera y la última columna son iguales, las variables que representan son equivalentes. □

1.22 Ejemplo. Es interesante constatar que la propiedad de la doble negación no se respeta en muchas expresiones del lenguaje coloquial. Por ejemplo, puesto que "nadie" es la negación de "alguien", la proposición "no hay nadie" es la doble negación de "hay alguien" y, por tanto, deberían ser equivalentes. Sin embargo normalmente se usan como opuestas.

1.3.2. Propiedades de la conjunción

La conjunción es una operación binaria y en ella sí procede estudiar más propiedades. La idempotencia, por ejemplo, da el resultado de operar una proposición consigo misma. La asociatividad nos indica cómo podemos efectuar la conjunción de tres proposiciones. La conmutatividad muestra que el orden de las proposiciones en una conjunción es irrelevante. Existe un elemento neutro (la proposición con valor 1, que denotaremos simplemente como 1) que al operarlo con cualquier proposición da como resultado la misma proposición. Existe también un elemento dominante (la proposición con valor 0, que denotaremos

simplemente como 0) que operado con cualquier proposición arroja el resultado 0.

1.23 Teorema. *La conjunción de proposiciones satisface las propiedades de idempotencia, asociatividad, conmutatividad, existencia de un elemento neutro y de un elemento dominante.*

Simbólicamente, si p, q y r son proposiciones cualesquiera se cumple

1. *Idempotencia:* $p \wedge p \Leftrightarrow p$.
2. *Asociatividad:* $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$.
3. *Conmutatividad:* $p \wedge q \Leftrightarrow q \wedge p$.
4. *Elemento neutro (1):* $p \wedge 1 \Leftrightarrow p$.
5. *Dominación (por 0):* $p \wedge 0 \Leftrightarrow 0$.

Demostración. La idempotencia está demostrada en la misma definición de la operación $\wedge$, (definición 1.8) pues en ella se aprecia que $1 \wedge 1 = 1$ y $0 \wedge 0 = 0$. En la tabla también se prueba la conmutatividad. Asimismo se ve que 1 sirve como neutro y que 0 operado con cualquier otro valor resulta en 0. Entonces sólo resta probar la propiedad asociativa. Construimos una tabla de las proposiciones $(p \wedge q) \wedge r$ y $p \wedge (q \wedge r)$.

p	q	r	$(p \wedge q) \wedge r$	$p \wedge (q \wedge r)$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	0	0
1	0	0	0	0
1	0	1	0	0
1	1	0	0	0
1	1	1	1	1

La igualdad de las dos últimas columnas prueba que ambas proposiciones son equivalentes. □

La presencia de la propiedad asociativa permite definir el símbolo $p \wedge q \wedge r$, sin paréntesis, como $(p \wedge q) \wedge r$ o bien $p \wedge (q \wedge r)$, puesto que son iguales. El resultado en ambos casos es que $p \wedge q \wedge r$ sólo es cierta si las tres proposiciones p, q y r son ciertas. Generalizando esta idea definimos la conjunción de las variables $p_1, p_2, \ldots, p_n$, denotada $p_1 \wedge p_2 \wedge \cdots \wedge p_n$, como la variable que sólo es cierta si todas las variables $p_1, p_2, \ldots, p_n$ son ciertas. Las propiedades asociativa y conmutativa aseguran que la definición es coherente con la anterior.

1.3.3. Propiedades de la disyunción

El estudio de la disyunción sigue los mismos pasos que el de la conjunción pues las propiedades que satisfacen son las mismas. La única diferencia es que los papeles de 1 y 0, como elementos neutro y dominante respectivamente, se invierten ahora.

1.24 Teorema. *La disyunción de proposiciones satisface las propiedades de idempotencia, asociatividad, conmutatividad, existencia de un elemento neutro y de un elemento dominante.*

Es decir, si p, q y r son proposiciones cualesquiera, se cumple

1. *Idempotencia:* $p \vee p \Leftrightarrow p$.
2. *Asociatividad:* $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$.
3. *Conmutatividad:* $p \vee q \Leftrightarrow q \vee p$.
4. *Elemento neutro (0):* $p \vee 0 \Leftrightarrow p$.
5. *Dominación (por 1):* $p \vee 1 \Leftrightarrow 1$.

Demostración. La idempotencia está demostrada en la misma definición de la operación $\vee$, (definición 1.10) pues en ella se aprecia que $1 \vee 1 = 1$ y $0 \vee 0 = 0$. En la tabla también se prueba la conmutatividad. Asimismo se ve que la constante 0 sirve como neutro y que la constante 1 operada con cualquier otro valor resulta en 1. Entonces sólo resta probar la propiedad asociativa. Construimos una tabla de las proposiciones $(p \vee q) \vee r$ y $p \vee (q \vee r)$.

p	q	r	$(p \vee q) \vee r$	$p \vee (q \vee r)$
0	0	0	0	0
0	0	1	1	1
0	1	0	1	1
0	1	1	1	1
1	0	0	1	1
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

□

Como en el caso de la conjunción podemos definir el símbolo $p \vee q \vee r$ como $(p \vee q) \vee r$ o bien $p \vee (q \vee r)$, puesto que son iguales. El resultado es que $p \vee q \vee r$ es cierta si alguna de las tres es cierta, o bien, es falsa sólo si todas son falsas. Generalizando esta idea definimos la disyunción de las variables $p_1, p_2, \ldots, p_n$, denotada $p_1 \vee p_2 \vee \cdots \vee p_n$, como la variable que sólo es falsa si todas las variables $p_1, p_2, \ldots, p_n$ son falsas.

Las propiedades asociativa y conmutativa aseguran que la definición es coherente con la definición de la disyunción de dos variables.

1.3.4. Propiedades de las operaciones combinadas

Ahora estudiamos algunas propiedades que surgen al considerar expresiones con dos o las tres operaciones combinadas.

1.25 Teorema. *Las siguientes relaciones son válidas para cualesquiera proposiciones p, q, r:*

1. *Complementariedad de la negación:*

   $p \wedge \neg p \Leftrightarrow 0$

   $p \vee \neg p \Leftrightarrow 1$

2. *Leyes distributivas:*

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

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

3. *Absorción:*

   $p \wedge (p \vee q) \Leftrightarrow p$

   $p \vee (p \wedge q) \Leftrightarrow p$

4. *Leyes de De Morgan:*

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

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

Demostración. La complementariedad de la negación se prueba en la siguiente tabla.

p	$\neg p$	$p \wedge \neg p$	$p \vee \neg p$
0	1	0	1
1	0	0	1

La prueba de las propiedades distributivas sigue en una tabla de ocho filas. La igualdad de la cuarta y quinta columnas es la prueba de la distribución de $\wedge$ respecto a $\vee$, mientras que la sexta y séptima columnas prueban la otra distribución.

p	q	r	$p \wedge (q \vee r)$	$(p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r)$	$(p \vee q) \wedge (p \vee r)$
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	0	0	0	0
0	1	1	0	0	1	1
1	0	0	0	0	1	1
1	0	1	1	1	1	1
1	1	0	1	1	1	1
1	1	1	1	1	1	1

En una última tabla se prueban las propiedades de absorción (tercera y cuarta columnas que son iguales a la primera) y las leyes de De Morgan (quinta y sexta columnas, primera ley, séptima y octava, segunda ley).

p	q	$p \wedge (p \vee q)$	$p \vee (p \wedge q)$	$\neg(p \wedge q)$	$\neg p \vee \neg q$	$\neg(p \vee q)$	$\neg p \wedge \neg q$
0	0	0	0	1	1	1	1
0	1	0	0	1	1	0	0
1	0	1	1	1	1	0	0
1	1	1	1	0	0	0	0

□

Las leyes demostradas permiten hacer manipulaciones algebraicas con las proposiciones y probar algunos resultados sin necesidad de recurrir a las tablas. Veamos dos ejemplos.

1.26 Ejemplo. Simplificación de una proposición mediante manipulaciones algebraicas. Cada proposición es equivalente a la anterior por la ley algebraica que se indica a su lado.

	$(p \wedge q) \vee \neg(q \vee \neg p)$	proposición a simplificar
$\Leftrightarrow$	$(p \wedge q) \vee (\neg q \wedge \neg\neg p)$	segunda ley de De Morgan
$\Leftrightarrow$	$(p \wedge q) \vee (p \wedge \neg q)$	doble negación y conmutatividad
$\Leftrightarrow$	$p \wedge (q \vee \neg q)$	distributividad
$\Leftrightarrow$	$p \wedge 1$	complementariedad de la negación
$\Leftrightarrow$	p	1 neutro de $\wedge$.

1.27 Ejemplo. Prueba algebraica de la ley de absorción (suponiendo probadas las leyes algebraicas anteriores). Partiendo de la proposición $p \wedge (p \vee q)$, mediante pasos algebraicos llegamos a que es equivalente a la proposición p.

	$p \wedge (p \vee q)$	
$\Leftrightarrow$	$(p \wedge (p \vee q)) \vee 0$	0 neutro de $\vee$
$\Leftrightarrow$	$(p \wedge (p \vee q)) \vee (q \wedge \neg q)$	comp. de negación
$\Leftrightarrow$	$(p \vee (q \wedge \neg q)) \wedge ((p \vee q) \vee (q \wedge \neg q))$	distributividad
$\Leftrightarrow$	$(p \vee q) \wedge (p \vee \neg q) \wedge (p \vee q \vee q) \wedge (p \vee q \vee \neg q)$	distributividad
$\Leftrightarrow$	$(p \vee q) \wedge (p \vee \neg q) \wedge (p \vee q) \wedge (p \vee 1)$	idemp. y complemento
$\Leftrightarrow$	$p \vee (q \wedge \neg q) \wedge 1$	distrib., idemp. y dominación
$\Leftrightarrow$	$p \vee 0$	complemento y 1 neutro de $\wedge$
$\Leftrightarrow$	p	0 neutro de $\vee$.

1.4. Cuantificadores

En esta sección introducimos los enunciados abiertos y, tras ellos, los cuantificadores. Son elementos muy habituales en la formulación de definiciones y resultados en matemáticas en expresiones de la forma “para todo número entero . . . ” o “existe una función tal que . . . ”.

1.28 Definición. *Llamamos* abierto *a un enunciado que contiene variables que toman valores en un conjunto dado, llamado* universo*, de forma que para cada valor que tomen las variables, el enunciado se convierte en una proposición.*

1.29 Ejemplo. Si la variable x toma valores en el universo de los dígitos (los números $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$), el enunciado "el número x es mayor que 5" es abierto.

Un enunciado abierto no es una proposición por sí mismo, sino que se convierte en una cuando las variables toman un valor. En el ejemplo anterior, el enunciado puede ser verdadero o falso según los valores que tome la variable.

Puesto que las proposiciones las representamos por letras $p, q, r, \ldots$, los enunciados abiertos los representamos por símbolos como $p(x)$, $q(x, y)$, $r(x, y, z)$, ... donde x, y, z son las variables que contiene el enunciado.

Los cuantificadores son unos prefijos que, antepuestos a enunciados abiertos, los convierten en proposiciones. Utilizaremos dos: el cuantificador universal y el cuantificador existencial. El primero se simboliza por $\forall$, y se suele leer "para todo". Indica que el enunciado que le sigue debe ser cierto para todos los posibles valores de la variable. El segundo se simboliza por $\exists$, y se lee "existe algún". Indica que el enunciado que sigue es cierto para, al menos, uno de los valores que puede tomar la variable.

Tomamos su propiedad de convertir enunciados abiertos en proposiciones como base para dar una definición.

1.30 Definición. *Si $p(x)$ es un enunciado abierto que depende de la variable x, la cual toma valores en un conjunto universo dado, definimos el símbolo $\forall x, p(x)$ como la proposición que es cierta sólo si el enunciado abierto es verdadero para todos los valores que la variable puede tomar en su universo.*

Asimismo definimos el símbolo $\exists x, p(x)$ como la proposición que es cierta si el enunciado abierto es verdadero para algún valor de los que la variable toma en su universo.

La proposición $\forall x, p(x)$ no es en realidad otra cosa que una conjunción, mientras que $\exists x, p(x)$ se trata de una disyunción como se aprecia en el siguiente ejemplo.

1.31 Ejemplo. Continuando el ejemplo anterior, donde la variable x toma valores en los dígitos, es decir, puede valer 0, 1, 2, ..., 9, llamamos $p(x)$ a la proposición "x es mayor que 5". Entonces, la proposición $\forall x, p(x)$ equivale a $p(0) \wedge p(1) \wedge \cdots \wedge p(9)$ y, claro está, es falsa. Por otro lado, la proposición $\exists x, p(x)$ equivale a $p(0) \vee p(1) \vee \cdots \vee p(9)$ y sí es cierta.

La necesidad de introducir los cuantificadores aparece cuando los posibles valores de la variable x no se pueden enlistar como en el ejemplo anterior: si ahora x toma valores en los números reales, no se puede escribir $\forall x, p(x)$ de otro modo.

Para usar cuantificadores basta recordar que un cuantificador junto a un enunciado abierto es una proposición y, a partir de ahí, se maneja como cualquier otra proposición. Sin embargo hay algunas reglas que simplifican el uso

de proposiciones que contienen cuantificadores. En concreto analizaremos dos de ellas: la negación de proposiciones con cuantificadores y la combinación de cuantificadores.

Una proposición que comienza con el cuantificador universal necesita que el enunciado abierto sea cierto para todos los valores de la variable, por tanto basta con que en un valor sea falso para que toda la proposición sea falsa. Por ello, la negación con un cuantificador universal nos lleva a un cuantificador existencial y viceversa. Si recordamos que $\forall x, p(x)$ es una conjunción y $\exists x, p(x)$ es una disyunción, esto no es otra cosa que las leyes de De Morgan vistas en el teorema 1.25. El resultado preciso se recoge en el siguiente teorema.

1.32 Teorema. *Si $p(x)$ es un enunciado abierto, con x una variable, entonces se cumplen las equivalencias*

$$\neg(\forall x, p(x)) \Leftrightarrow \exists x, \neg p(x)$$
$$\neg(\exists x, p(x)) \Leftrightarrow \forall x, \neg p(x)$$

Demostración. Como se ha dicho, se trata de las leyes de De Morgan. Razonemos una de ellas como muestra. La negación de la proposición $\forall x, p(x)$ es cierta si el enunciado $p(x)$ no se cumple en algún valor de la variable. Pero eso es precisamente lo que dice la proposición $\exists x, \neg p(x)$. □

Si un enunciado abierto contiene varias variables, se necesita un cuantificador para cada una. Así, si $p(x, y)$ es un enunciado abierto con las variables x e y, entonces $\forall x, p(x, y)$, $\exists x, p(x, y)$ son enunciados abiertos con una variable: y. Pero $\forall x, \forall y, p(x, y)$, $\forall x, \exists y, p(x, y)$ son proposiciones. La combinación de varios cuantificadores tiene algunas reglas que permiten simplificar su escritura, pero requiere atención pues no todos los casos son simplificables.

Las primera y segunda reglas nos dicen que combinar cuantificadores universales y combinar cuantificadores existenciales es conmutativo.

1.33 Teorema. *Si $p(x, y)$ es un enunciado abierto que depende de dos variables, x, y, se cumplen las siguientes equivalencias entre proposiciones.*

$$\forall x, \forall y, p(x, y) \Leftrightarrow \forall y, \forall x, p(x, y)$$
$$\exists x, \exists y, p(x, y) \Leftrightarrow \exists y, \exists x, p(x, y)$$

Demostración. La proposición $\forall x, \forall y, p(x, y)$ sólo es verdadera si dado cualquier x, puedo elegir cualquier y y obtengo que $p(x, y)$ es verdadero. Pero en tal caso el valor de y elegido es independiente de x, y puedo escogerlo primero. Entonces, dado cualquier y, puedo elegir cualquier x y tendré $p(x, y)$ verdadero, lo cual es la proposición $\forall y, \forall x, p(x, y)$. Con esto se ha probado que cuando la primera es cierta, la segunda también. El mismo razonamiento pero a la inversa muestra que cuando la segunda es cierta la primera también. En total ambas tienen siempre el mismo valor y, por tanto, son equivalentes.

Análogamente la proposición $\exists x$, $\exists y$, $p(x, y)$ afirma que existe algún x de modo que puedo encontrar una y tal que $p(x, y)$ es verdadero. Puedo tomar los valores en orden inverso: escoger primero el valor de y encontrado antes, luego

el de x y tendré $p(x, y)$ verdadero. Hemos probado, pues, que si $\exists x, \exists y, p(x, y)$ es cierta, entonces $\exists y, \exists x, p(x, y)$ también lo es. El mismo razonamiento se aplica a la inversa y llegamos a que ambas son equivalentes. □

Gracias a este resultado podemos escribir sin ambigüedad $\forall x, y$ ó $\forall y, x$ en lugar de $\forall x, \forall y$, así como $\exists x, y$ ó $\exists y, x$ en lugar de $\exists x, \exists y$, y el orden de las variables x e y es irrelevante.

Sin embargo hay que tener cuidado pues el orden sí es importante cuando se combinan cuantificadores de ambos tipos, como muestra el siguiente ejemplo.

1.34 Ejemplo. Consideremos el enunciado abierto "$x \neq y$", donde x, y toman valores en el conjunto de los números enteros. Entonces la proposición $\forall x, \exists y, x \neq y$ afirma que dado un número entero cualquiera, x, existe al menos un número, y, que es distinto que él, lo cual es cierto. Sin embargo, la proposición $\exists x, \forall y, x \neq y$ afirma que existe un número entero, x, tal que cualquier número entero, y, es distinto que él, lo cual es falso.

Para terminar esta sección definimos el cuantificador de existencia y unicidad, simbolizado $\exists!$. Como su nombre indica este símbolo contiene dos afirmaciones: primero, la existencia de un elemento que cumple el enunciado; segundo, que dicho elemento es el único que lo cumple. La forma de enunciar la unicidad es diciendo que si hay dos elementos que cumplen la propiedad, entonces son iguales. Todo esto se reúne en la siguiente definición.

1.35 Definición. *Si $p(x)$ es un enunciado abierto, el símbolo $\exists! x, p(x)$ es la proposición definida por*

$$(\exists x, p(x)) \wedge \forall a, b, (p(a) \wedge p(b) \rightarrow a = b).$$

1.36 Ejemplo. La proposición $\exists! x, x^2 = x$, donde x toma valores en los enteros, significa que existe un entero, y sólo uno, que verifica que elevado al cuadrado se queda igual. Se trata de una proposición falsa puesto que, aunque cumple la existencia ($x = 1$ lo verifica), no cumple la unicidad (porque $x = 0$ también lo verifica).

1.37 Ejemplo. La proposición $\exists! x, \forall y, x + y = y$, donde tanto x como y toman valores enteros, enuncia que hay un número entero, y sólo uno, que sumado a cualquier otro lo deja igual; es decir, un elemento neutro de la suma. Esta proposición sí es cierta, lo cual se demuestra en dos pasos. Primero, la existencia: el 0 cumple lo dicho. Segundo, la unicidad: hay que probar que si hay dos elementos neutros, llamémoslos x_1 y x_2, entonces son iguales. Ahora bien, puesto que x_1 es neutro, sumado con x_2 resulta $x_1 + x_2 = x_2$. Por la misma razón, pues x_2 también es neutro, tenemos $x_2 + x_1 = x_1$. Por último, por la propiedad conmutativa de la suma sabemos que $x_1 + x_2 = x_2 + x_1$, de donde concluimos que $x_1 = x_2$.

1.5. El razonamiento lógico

Abordamos finalmente el objetivo de la lógica: obtener proposiciones verdaderas a partir de otras proposiciones verdaderas ya conocidas. Esta deducción se efectúa mediante lo que se llama un razonamiento lógico. Por ello, en esta sección vamos a definir qué es un razonamiento lógico y veremos cómo construirlo. Como se señaló en la introducción, la finalidad de este capítulo y, en particular de esta sección, no es desarrollar la capacidad de crear nuevos razonamientos lógicos, sino poder analizar razonamientos ya hechos y determinar si son correctos.

Lo que se pretende con un razonamiento lógico es deducir una proposición verdadera nueva a partir de otras proposiciones verdaderas ya conocidas. Analicemos esta idea, empezando por nombrar sus elementos. Las proposiciones que son conocidas se llaman hipótesis o premisas. La proposición que se deduce es la tesis, resultado o consecuencia. El hecho de que las premisas nos lleven a deducir la consecuencia se puede expresar por medio de una implicación: si las premisas son ciertas, entonces la consecuencia debe ser cierta. Si $p_1, p_2, \cdots, p_n$ son las premisas y q es la consecuencia, quiero expresar la idea de que si todas las premisas son ciertas, entonces la consecuencia es cierta. Es decir $p_1 \wedge p_2 \wedge \cdots \wedge p_n \to q$.

Ahora, la idea clave. Nos interesa el razonamiento lógico independientemente del contenido de las proposiciones. Si es cierto que de las premisas $p_1, p_2, \cdots, p_n$ se sigue necesariamente la consecuencia q, entonces la expresión $p_1 \wedge p_2 \wedge \cdots \wedge p_n \to q$ debe ser siempre verdadera. Esta idea se recoge elegantemente en la siguiente definición.

1.38 Definición. *Una proposición de la forma* $p_1 \wedge p_2 \wedge \cdots \wedge p_n \to q$ *es un* razonamiento lógico *si es una tautología. Entonces el razonamiento se denota*

$$p_1 \wedge p_2 \wedge \cdots \wedge p_n \Rightarrow q,$$

las proposiciones $p_1, p_2, \cdots, p_n$ *se llaman* premisas *y la proposición* q consecuencia.

1.39 Ejemplo. Consideremos las proposiciones "si un número entero no es cero, entonces su valor absoluto es positivo" y "-4 no es cero". Puedo deducir que el valor absoluto de -4 es un número positivo. Pero la deducción no depende de que estemos hablando acerca del valor absoluto de números enteros, sino de su estructura lógica. Las premisas son $p \to q$ ("si un número entero no es cero, entonces su valor absoluto es positivo") y p ("un número entero, -4, no es cero"), es decir, $(p \to q) \wedge p$, y la consecuencia es q ("su valor absoluto, $|-4|$, es positivo"). El razonamiento ha sido $(p \to q) \wedge p \Rightarrow q$ y es válido sean quienes sean p y q. Por ello tiene nombre propio: *modus ponendo ponens* (del latín, que se puede traducir como el razonamiento que afirmando p (*ponendo*) afirma q (*ponens*)).

Veamos otros dos ejemplos de razonamiento lógico.

1.40 Ejemplo. Con la misma implicación de antes "si un número entero no es cero, entonces su valor absoluto es positivo" y además con la proposición "el

valor absoluto del número a no es positivo", puedo deducir que "el número a es cero".

El razonamiento en este caso ha sido $(p \to q) \wedge \neg q \Rightarrow \neg p$, y se llama *modus tollendo tollens* (el razonamiento que negando q (*tollendo*) niega p (*tollens*).

1.41 Ejemplo. Un último ejemplo con estas proposiciones. Si tengo las dos implicaciones "si un número entero no es cero, entonces su valor absoluto es positivo" y "si un número entero a es positivo, entonces a es mayor que su opuesto, $-a$", puedo deducir que "si un número entero a no es cero, entonces $|a| > -|a|$".

Este razonamiento, cuya estructura es $(p \to q) \wedge (q \to r) \Rightarrow (p \to r)$, se llama silogismo.

La pregunta ahora es, dado una expresión de la forma $p_1 \wedge p_2 \wedge \cdots \wedge p_n \to q$, ¿cómo saber si es un razonamiento lógico o no? Las dos formas de probar que es un razonamiento lógico son: Primera, demostrar directamente que dicha proposición es una tautología, por ejemplo mediante una tabla. Es útil para razonamientos sencillos, cuyas tablas no sean grandes. Segunda, descomponer el razonamiento en razonamientos más simples ya conocidos. Es decir, partiendo de las premisas y aplicando razonamientos simples conocidos ir deduciendo nuevas proposiciones ciertas hasta llegar a la que se enunciaba como consecuencia. Este segundo es el método habitual de probar la validez de razonamientos lógicos complejos.

Para poder utilizar cadenas de razonamientos simples en la prueba de un razonamiento complicado necesitamos tener algunos razonamientos ya demostrados de forma directa. En el siguiente teorema se exponen algunos de estos razonamientos que son muy habituales y, prácticamente, podríamos decir que responden en gran medida al sentido común: se llaman reglas de inferencia y tienen nombres propios.

1.42 Teorema. *Para proposiciones cualesquiera p, q, r, s los siguientes son razonamientos lógicos:*

1. *Modus ponendo ponens:* $((p \to q) \wedge p) \Rightarrow q$.
2. *Modus tollendo tollens:* $((p \to q) \wedge \neg q) \Rightarrow \neg p$.
3. *Silogismo:* $((p \to q) \wedge (q \to r)) \Rightarrow (p \to r)$.
4. *Demostración por contradicción:* $(\neg p \to 0) \Rightarrow p$.
5. *Demostración por casos:* $((p \to r) \wedge (q \to r)) \Rightarrow ((p \vee q) \to r)$
6. *Silogismo disyuntivo:* $((p \vee q) \wedge (\neg p)) \Rightarrow q$.
7. *Conjunción:* $(p) \wedge (q) \Rightarrow (p \wedge q)$.
8. *Simplificación conjuntiva:* $(p \wedge q) \Rightarrow p$.
9. *Amplificación disyuntiva:* $p \Rightarrow (p \vee q)$.
10. *Especificación universal:* $\forall x, p(x) \Rightarrow p(a)$, *con a un elemento cualquiera del universo de x.*
11. *Generalización universal:* $(p(a) \wedge (a \text{ es arbitrario})) \Rightarrow \forall x, p(x)$.
12. *Especificación existencial:* $\exists x, p(x) \Rightarrow p(a)$, *con a el elemento al que se refiere la existencia.*

Demostración. Todas estas reglas de inferencia se pueden probar elaborando la tabla correspondiente, pero también mediante manipulaciones algebraicas. En cualquier caso son todas muy similares, por lo cual expondremos la prueba de tres de ellas con todo detalle, a modo de muestra, dejando el resto como ejercicio.

Prueba del *modus ponendo ponens* mediante una tabla. Para probar $((p \to q) \wedge p) \Rightarrow q$ debemos probar que $((p \to q) \wedge p) \to q$ es una tautología. Construimos la tabla con todos los ingredientes de esta última expresión.

p	q	$p \to q$	$(p \to q) \wedge p$	$((p \to q) \wedge p) \to q$
0	0	1	0	1
0	1	1	0	1
1	0	0	0	1
1	1	1	1	1

La última columna muestra que, efectivamente, la implicación es una tautología y por tanto el razonamiento es válido.

Prueba del razonamiento por contradicción mediante manipulaciones algebraicas. Para probar que la implicación $(\neg p \to 0) \to p$ es un razonamiento, debo probar que es equivalente a la proposición 1 (tautología) mediante una cadena de proposiciones equivalentes entre sí. En cada paso se da la razón que lo justifica.

$$
\begin{array}{ll}
(\neg p \to 0) \to p & \\
\Leftrightarrow \neg(\neg\neg p \vee 0) \vee p & \text{(por la equivalencia } a \to b \Leftrightarrow \neg a \vee b\text{, teorema 1.20)} \\
\Leftrightarrow \neg(p \vee 0) \vee p & \text{(doble negación)} \\
\Leftrightarrow \neg p \vee p & \text{(0 neutro de } \vee\text{)} \\
\Leftrightarrow 1 & \text{(complementariedad de la negación).}
\end{array}
$$

Por último, la prueba de uno de los razonamientos que involucran cuantificadores y enunciados abiertos. Probamos el razonamiento de especificación universal usando uno de los razonamientos lógicos de este mismo teorema, supuesto ya demostrado. La proposición $\forall x, p(x)$ es equivalente a la conjunción de la proposición $p(x)$ cuando x toma todos los valores posibles. Entonces, por la regla de simplificación conjuntiva, de la premisa deducimos que cualquiera de las proposiciones es cierta, en particular, si a es un valor posible de x, $p(a)$ es cierta. □

1.6. Axiomas, definiciones y teoremas en matemáticas

La matemática deduce resultados nuevos a partir de otros ya conocidos usando la herramienta de la lógica. Una teoría matemática se compone de axiomas, definiciones y teoremas, así que veamos qué es cada uno de ellos.

Axiomas: Son las proposiciones de partida de una teoría y, por tanto, no pueden ser probadas dentro de ella. La idea es que los axiomas van a ser las primeras premisas que permitan deducir consecuencias de ellas, es decir,

obtener los primeros resultados. Es claro que toda teoría que se construya mediante razonamientos lógicos debe tener axiomas, ya que los razonamientos parten de premisas ciertas para deducir una consecuencia cierta. Es decir, en todo caso necesitamos partir de algunas premisas.

1.43 Ejemplo. La proposición "el conjunto $\mathbb{N}$ de los números naturales contiene al menos un elemento" se utiliza como axioma en la construcción de los números debida a Peano.

Definición: Es la asignación de un nombre a una proposición y por ello tiene forma de equivalencia. Obsérvese que el papel de las definiciones en una teoría matemática no es determinante, pues sólo sirven para simplificar la escritura (aunque ciertamente sería impensable escribir una teoría sin la ayuda de las definiciones). Es interesante hacer notar que, por ser una equivalencia, una definición debería leerse "... si y sólo si ...", sin embargo es costumbre escribir únicamente "... si ..." como si se tratara de una implicación, aún sabiendo que es algo más.

1.44 Ejemplo. La proposición "un número natural es primo si (y sólo si) es mayor que 1 y sus únicos divisores son 1 y él mismo" es una definición. Simbólicamente

$$p \text{ primo } \Leftrightarrow p > 1 \wedge \forall n, (n|p \rightarrow (n = 1 \vee n = p)).$$

Sirve para sustituir en cualquier punto de la teoría la proposición $p > 1 \wedge \forall n, (n|p \rightarrow n = 1 \vee n = p)$ por la otra más breve "p es primo".

Teoremas: Son los resultados de la teoría y, por tanto, el objetivo de las matemáticas. Son proposiciones que pueden tener diversas formas. Un tipo habitual de teorema es un razonamiento lógico, de la forma descrita anteriormente $((p_1 \wedge p_2 \wedge \ldots \wedge p_n) \Rightarrow q)$, en el cual las premisas son los axiomas de la teoría o bien otros teoremas ya probados en la teoría. La consecuencia es otra proposición relativa a la teoría.

1.45 Ejemplo. El resultado "si m y n son primos distintos, entonces su máximo común divisor es 1" es un teorema, que podemos escribir también como

$$m \text{ primo } \wedge n \text{ primo } \wedge m \neq n \Rightarrow \text{mcd}(m, n) = 1.$$

Otros teoremas tienen forma de equivalencia ($\Leftrightarrow$) en lugar de implicación ($\Rightarrow$). Pero, como se ha visto en el teorema 1.18, un teorema de doble implicación equivale a dos teoremas de una implicación. Esto es, un teorema de la forma $p \Leftrightarrow q$ es equivalente a $p \Rightarrow q \wedge q \Rightarrow p$.

Todo teorema de una teoría debe ser probado rigurosamente.

Por tanto, la exposición de una teoría matemática debe observar dos reglas imprescindibles: un estricto orden de presentación, para que cada teorema use

como premisas sólo resultados anteriores, ya probados, y que cada teorema vaya seguido inmediatamente de su demostración, que consiste en verificar el razonamiento lógico.

Como ejemplo de esta estructura básica de una teoría matemática citamos el libro de Mosterín [1] y los libros de Landau [8, 9], en cuya presentación la austeridad está llevada al máximo.

Es conveniente señalar que, en ocasiones, se dan otros nombres a resultados de la teoría. Algunos nombres muy utilizados son los de proposición, lema y corolario. Todos ellos son sinónimos de teorema en cuanto a que son resultados de la teoría. Los distintos nombres se utilizan para agrupar los resultados por categorías. Una proposición es un resultado de no mucha importancia. Se suele llamar lema a un resultado cuya única aplicación es en la prueba de algún otro resultado posterior. La palabra teorema se reserva para los resultados más importantes de la teoría. Por último, corolario es un resultado cuya prueba es inmediata a partir de un teorema anterior. Como se puede apreciar, llamar a los resultados de una teoría teoremas, lemas, proposiciones o corolarios es una cuestión subjetiva que queda a gusto del autor en cada caso.

1.6.1. Un ejemplo

A continuación construimos un ejemplo de un desarrollo matemático. Introducimos algunos elementos de la teoría de la divisibilidad de números naturales con el formato explicado: axiomas, definiciones, teoremas y su demostración. En concreto ilustramos un axioma de los naturales, el de inducción, y cuatro teoremas demostrando cada uno con un estilo de prueba diferente: una prueba de la implicación directa, una prueba usando la implicación contrapositiva, una prueba por inducción y una prueba por contradicción.

Para estos ejemplos asumimos conocidas las propiedades algebraicas de la suma y el producto de los naturales como son la asociatividad, conmutatividad o propiedad distributiva o que $n+1$ es el sucesor del número n.

1.46 Axioma (Axioma de inducción de los naturales)**.** *Si el natural 1 verifica una propiedad y para cada natural n que cumple dicha propiedad también el sucesor de n la cumple, entonces la propiedad se verifica para todos los naturales. Simbólicamente, si $p(x)$ es un enunciado abierto y la variable x toma valores en los naturales,*

$$p(1) \wedge \forall n, (p(n) \to p(n+1)) \Rightarrow \forall x, p(x).$$

1.47 Definición. *Un natural a divide a otro b, y lo denotamos $a|b$, si existe un número c tal que se verifica $b = ac$. Es decir,*

$$a|b \Leftrightarrow \exists c,\ b = ac.$$

En tal caso decimos que a es divisor de b y que b es múltiplo de a.

1.48 Ejemplo. $3|12$ pues $12 = 3 \cdot 4$, pero $5 \not| 12$ (que es la negación de $5|12$).

Es obvio que 1 divide a cualquier número b ya que $b = 1b$ y, por la misma razón, todo número es divisor de sí mismo. Algunos números únicamente tienen estos divisores y por ello merecen especial atención.

1.49 Definición. *Un natural p mayor que 1 es primo si 1 y p son sus únicos divisores. Simbólicamente*

$$p \text{ primo } \Leftrightarrow p > 1 \wedge \forall a, (a|p \rightarrow a = 1 \vee a = p).$$

Un natural mayor que 1 que no es primo se llama compuesto.

1.50 Ejemplo. Los números primos menores que 100 son

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 73, 79, 83, 89, 97.$$

1.51 Teorema (Propiedad transitiva de los divisores)**.** *Si a divide a b y éste, a su vez, divide a c, entonces a divide a c, que lo podemos escribir como*

$$a|b \wedge b|c \Rightarrow a|c.$$

Demostración. Se trata de un teorema con forma de implicación y mostramos una prueba directa, es decir, que partiendo de las premisas y resultados anteriores (propiedades de los números naturales), llegamos a la conclusión mediante las reglas de inferencia enumeradas en el teorema 1.42.

1. Por hipótesis $a|b$.
2. Por la definición 1.47, y por la regla de especificación existencial, existe un número, y lo llamamos k_1, que cumple $b = k_1 a$.
3. Por hipótesis $b|c$.
4. Por la definición 1.47, y por la regla de especificación existencial, existe un número, y lo llamamos k_2, que cumple $c = k_2 b$.
5. Sustituyendo la igualdad del punto 2 en la del punto 4 tenemos $c = k_2(k_1 a)$.
6. Por la propiedad asociativa del producto de números naturales la igualdad anterior se puede escribir como $c = (k_2 k_1)a$.
7. El número $k_2 k_1$ hace que se verifique la definición de divisibilidad para a y c, luego concluimos que a divide a c.

□

1.52 Teorema. *El natural a divide a b sólo si a es menor o igual que b. Simbólicamente*

$$a|b \Rightarrow a \leq b.$$

Demostración. Este teorema tiene de nuevo la forma de una implicación, pero ahora vamos a probar la implicación contrapositiva, que es equivalente a la enunciada:

$$a > b \Rightarrow a \not| b.$$

Ahora los pasos para demostrar ésta.

1. Por hipótesis $a > b$.
2. Consideremos un natural arbitrario c.
3. Por las propiedades del orden de los naturales $c \geq 1$.
4. Por las propiedades del orden de los naturales $ac \geq a$.
5. Por los puntos 4 y 1 y las propiedades del orden tenemos $ac > b$, y por tanto, $ac \neq b$.
6. Por generalización universal, teniendo en cuenta el punto 2, tenemos $\forall x,\ ax \neq b$.
7. La proposición anterior es equivalente a $\neg\exists x,\ ax = b$.
8. Por la definición 1.47 llegamos a $a \not| b$ y la implicación contrapositiva queda probada.

□

1.53 Teorema. *Todo número natural cumple que, o bien es 1, o bien es divisible por un primo, y lo expresamos como sigue*

$$\forall n,\ n = 1 \vee \exists p,\ (p \text{ primo } \wedge p|n).$$

Demostración. Aquí presentamos una típica prueba por inducción, que hace uso del axioma del mismo nombre. Para probar que la propiedad enunciada en el teorema es válida para todos los naturales hay que probar que se cumple para el 1 y que para todo número n que la verifica, la propiedad es válida para el sucesor. Al asumir que se cumple para un número n se puede asumir también que se cumple para todos los menores a él.

1. Llamamos $P(n)$ al enunciado $n = 1 \vee \exists p,\ (p \text{ primo } \wedge p|n)$.
2. La proposición $P(1)$ es cierta, ya que se cumple $1 = 1$.
3. Para probar $P(n) \rightarrow P(n+1)$ consideramos un número n arbitrario y la hipótesis $P(n)$. Entonces el número n, si no es 1, es divisible por un primo y lo mismo cumplen todos los números menores que n.

   Puesto que el número $n+1$ no puede ser 1, hay que probar que es divisible por un primo. Separamos esta parte en dos casos.
4. Si $n+1$ es primo entonces, puesto que $n+1|n+1$, es divisible por un primo y la proposición $P(n+1)$ es cierta.

5. Si $n+1$ no es primo entonces, por la definición 1.49, tiene un divisor diferente de 1 y de sí mismo. Por la regla de especificación existencial llamamos a a este divisor.
6. Por el teorema 1.52, $a < n+1$.
7. Por conjunción de los puntos 5 y 6 tenemos $a \neq 1 \wedge a < n+1$.
8. Por la hipótesis de inducción (punto 3) aplicada al número a, y por la regla de especificación existencial, existe un número primo, y lo llamamos p, que cumple $p|a$.
9. Por conjunción de los puntos 5 y 8 tenemos $p|a \wedge a|n+1$.
10. Usando el teorema 1.51 concluimos $p|n+1$, es decir $P(n+1)$ es cierta también en este caso.
11. Por la regla de inferencia de demostración por casos aplicada a los puntos 4 y 10 concluimos que $\forall n, P(n) \rightarrow P(n+1)$ es cierta.
12. Por conjunción de los puntos 2 y 11 y el axioma 1.46 llegamos a que el enunciado $P(n)$ es cierto para todos los naturales, luego el teorema queda probado.

□

Por último enunciamos un famoso teorema y su, no menos famosa, prueba debida a Euclides: la infinitud de los números primos y su demostración por contradicción.

1.54 Teorema (Euclides)**.** *La cantidad de números primos es infinita.*

Demostración. Aquí presentamos la prueba debida a Euclides, que procede por contradicción o, como también se llama, reducción al absurdo.

1. Negamos el teorema: La cantidad de números primos es finita.
2. Por ser finita, podemos denotar los números primos como $p_1, p_2, \ldots, p_n$.
3. Consideremos el número $q = p_1 p_2 \cdots p_n + 1$.
4. Por su construcción y las propiedades del orden de los naturales $q > 1$, por lo cual $q \neq 1$.
5. En este punto demostramos que p_1 no divide a q utilizando también un razonamiento por contradicción: negamos la afirmación, asumiendo entonces que p_1 sí divide a q. Entonces $q = p_1 k$ para algún número k y, operando en la definición de q, podemos escribir $1 = p_1(k - p_2 p_3 \cdots p_n)$. Esta igualdad indica que p_1 divide a 1. Por el teorema 1.52 tenemos que $p_1 \leq 1$. Sin embargo, por hipótesis p_1 es primo y, por la definición 1.49, esto supone $p_1 > 1$. Tenemos la contradicción $p_1 \leq 1 \wedge p_1 > 1$. Por tanto concluimos que la negación es falsa y queda probado que $p_1 \nmid q$. Análogamente tenemos $p_2 \nmid q$, $\ldots$, $p_n \nmid q$.

6. Por conjunción de los dos puntos anteriores tenemos que el número q no es 1 y no es divisible por ningún primo, lo cual es una contradicción con el teorema 1.53.

7. Por la regla de contradicción concluimos que el enunciado original es cierto.

□

Las demostraciones que aquí se han puesto como ejemplo han sido ilustradas con mucho detalle, pero habitualmente la redacción de pruebas de teoremas se hace mucho más breve. Las cuatro pruebas anteriores, en un lenguaje habitual, se reducirían a unas pocas líneas cada una, especialmente porque no se mencionan las reglas de inferencia que se usan en cada paso ya que son ampliamente conocidas.

Ejercicios

1.1. Determinar el valor (verdadero o falso) de las siguientes proposiciones:

a) 11 es entero y $\sqrt{3}$ es irracional.

b) π es complejo y -2 es natural.

c) $\sqrt{5}$ es racional o π es complejo.

d) $\frac{2}{3}$ es complejo y $\frac{2}{3}$ es racional.

e) $1+i$ es real o $1+i$ es entero.

f) $\frac{2}{5}$ es complejo o $\frac{7}{3}$ es real.

g) Si i es real entonces $\sqrt{2}$ es natural.

h) Si todo complejo es real entonces $\sqrt{5}$ es entero.

i) Si $\sqrt{2}$ es complejo entonces no es real.

j) i es real si, y sólo si, π es entero.

k) Todo real es complejo si, y sólo si, todo complejo es real.

1.2. Para cada una de las siguientes implicaciones, construir su inversa, recíproca y contrapositiva y dar el valor de cada una de ellas.

a) Si $-2 < -1$ entonces $-\sqrt{5} < 1$.

b) Si $\frac{4}{5}$ es complejo entonces π es entero.

c) Si i es entero entonces 4 es complejo.

d) Si -1 es natural entonces $\frac{3}{2}$ es es entero.

1.3. Los conectores binarios $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, entre proposiciones son sólo algunos de todos los posibles. Muéstrese que hay dieciséis conectores binarios diferentes y elabórese una tabla que los defina.

A continuación, pruébese que todos ellos se pueden expresar sólo con los conectores $\neg$, $\wedge$ y las constantes 0 y 1.

1.4. La implicación $p \rightarrow q$ se puede traducir al lenguaje ordinario de muchas formas. Una de ellas es "si p, entonces q". Otras dos expresiones muy habituales y relacionadas con la implicación son las que se enuncian a continuación. Tradúzcanse a símbolos lógicos las proposiciones siguientes.

a) "p es condición necesaria para q".

b) "p es condición suficiente para q".

c) "p es condición necesaria y suficiente para q".

1.5. Escribir la negación de una implicación.

Escribir la negación de un teorema que consiste en varias premisas que implican una consecuencia. Esto es lo que se emplea cuando se quiere demostrar un teorema por la regla de contradicción: hay que comenzar por negar el teorema y luego llegar a contradicción.

1.6. Indicar el valor de las siguientes proposiciones construidas con cuantificadores. El conjunto universo para la variable x es el de los enteros $\mathbb{Z}$.

a) $\forall x, x < 1000.$

b) $\exists x, x < 1000.$

c) $\forall x, x^3 > 0.$

d) $\exists x, x^3 < 0.$

e) $\forall x, x^2 \leq x.$

f) $\exists x, x^2 \leq x.$

g) $\exists! x, x^2 = 1.$

h) $\exists! x, x^2 = 0.$

1.7. Indicar el valor de las siguientes proposiciones construidas con dos cuantificadores. El conjunto universo para las variables x e y es el de los enteros $\mathbb{Z}$.

a) $\forall x, y; x > y.$

b) $\forall x, y; x + 1 = y.$

c) $\forall x, y; (x > y \wedge y > x).$

d) $\forall x, y; (x > y \vee x < y).$

e) $\exists x, y; xy < x.$

f) $\exists x, y; (x > y \wedge y > x).$

g) $\exists x, y; x + y < xy.$

h) $\forall x, \exists y; x < y.$

i) $\exists y, \forall x; x < y.$

j) $\forall x, \exists y; x = y + 1.$

k) $\exists x, \forall y; x + y = y$.

l) $\forall x, \exists y; x + y = y$.

m) $\forall x, \exists y; xy = x$.

n) $\forall x, \exists y; xy = y$.

1.8. Escribir la negación de cada una de las proposiciones de los ejercicios 1.6 y 1.7.

1.9. Demostrar que la proposición p es una tautología, donde a y b son proposiciones cualesquiera:

$$p : [\neg(a \wedge b)] \leftrightarrow [\neg a \vee \neg b].$$

1.10. Demostrar que la proposición q es una contradicción , donde a y b son proposiciones cualesquiera:

$$q : (\neg a \vee a) \rightarrow (b \wedge \neg b).$$

1.11. Probar las reglas de inferencia lógica enunciadas en el teorema 1.42 que no han sido probadas en el texto.

1.12. Consideremos las siguientes proposiciones como premisas: "Todos los días, si no llueve, Paco va al parque a correr y, si llueve, no va", "Paco compra el periódico sólo si sale a correr" y "los domingos, Paco no compra el periódico".

a) Llamando $p(x)$, $q(x)$, $r(x)$ a los enunciados "el día x llueve", "el día x Paco sale a correr" y "el día x compra el periódico", respectivamente, donde x toma valores en los días de la semana, escribir las premisas con estos enunciados, cuantificadores y conectores lógicos.

b) Probar que la proposición "Si el sábado Paco compra el periódico, entonces es que no ha llovido" es una consecuencia lógica de las premisas. Analizar las reglas de inferencia que permiten deducir el resultado.

c) Consideramos la proposición "Si el sábado no llueve, Paco compra el periódico" y su justificación en los siguientes pasos:

1. Puesto que el sábado no llueve, Paco va a correr.
2. Ya que sale a correr y no es domingo, entonces compra el periódico

La conclusión no es válida, por tanto esta justificación es incorrecta. Encontrar el error.

1.13. Dar una prueba directa (no por la contrapositiva como se ha hecho en la página 22) del teorema 1.52.

1.14. Probar el siguiente teorema de la teoría de la divisibilidad de números naturales.

Si c es un divisor común de a y b, entonces c divide a cualquier número de la forma $ma + nb$ con m y n naturales arbitrarios. Simbólicamente

$$c|a \wedge c|b \Rightarrow \forall m, n; c|(ma + nb).$$

El teorema tiene forma de implicación y es posible una prueba directa partiendo de las premisas y avanzando, mediante las reglas de inferencia y las definiciones o teoremas ya enunciados en páginas anteriores, hasta llegar a la conclusión.

1.15. En este ejercicio enunciamos un supuesto teorema (y su supuesta demostración) de la teoría de la divisibilidad. Se trata de una versión del recíproco del teorema del ejercicio anterior.

Si un entero divide a una suma de enteros, entonces divide a cada sumando. Simbólicamente,

$$k|(m+n) \Rightarrow k|m \wedge k|n.$$

Demostración. Puesto que k divide a $(m+n)$, existe un entero p tal que $m+n = p\,k$. Ahora bien, si uno de los enteros,m, es divisible entre k, entonces existe otro entero q tal que $m = k\,q$. Por tanto, operando, $n = k(p-q)$, y como $(p-q)$ es un entero, entonces k también divide a n. □

Se pide:

a) Describir los pasos lógicos que se siguen en la demostración y señalar exactamente cuál es el incorrecto.

b) Demostrar que el teorema es falso. Para ello, escribir la negación del teorema y demostrar que es cierta. En este caso, esto se denomina dar un contraejemplo.

* 1.16. Definimos el concepto de *máximo común divisor* de dos naturales a y b, denotado $\mathrm{mcd}(a,b)$, como el mayor de los divisores comunes de a y b. Es decir, $d = \mathrm{mcd}(a,b)$ si

$$d|a \wedge d|b \wedge \forall c, ((c|a \wedge c|b) \rightarrow c \leq d).$$

El máximo común divisor tiene muchas propiedades notables. La principal es la llamada identidad de Bezout, que afirma que existen dos enteros m y n (obsérvese que necesariamente uno de los dos debe ser negativo, por eso son enteros) tales que $ma + nb = \mathrm{mcd}(a,b)$ y, además, es el menor natural que se puede obtener mediante estas combinaciones de a y b.

Asumiendo este teorema, probar esta otra propiedad que es mucho más sencilla.

Los divisores comunes de dos naturales son exactamente los divisores de su máximo común divisor. Simbólicamente,

$$c|a \wedge c|b \Leftrightarrow c|\mathrm{mcd}(a,b).$$

* 1.17. Definimos el concepto de *mínimo común múltiplo* de dos naturales a y b, denotado $\mathrm{mcm}(a,b)$, como el menor de los múltiplos comunes de a y b. Esto es, $m = \mathrm{mcm}(a,b)$ si

$$a|m \wedge b|m \wedge \forall c, ((a|c \wedge b|c) \rightarrow m \leq c).$$

Las dos propiedades más notables del mínimo común múltiplo son las siguientes, que se pide demostrar.

Los múltiplos comunes de dos naturales son exactamente los múltiplos del mínimo común múltiplo. Simbólicamente,

$$a|c \wedge b|c \Leftrightarrow \mathrm{mcm}(a,b)|c.$$

El máximo común divisor y el mínimo común múltiplo verifican la siguiente igualdad:

$$ab = \mathrm{mcd}(a,b)\mathrm{mcm}(a,b).$$

* 1.18. Pruébese que, si n es un natural,

$$2|n^2 \Rightarrow 2|n.$$

Análogamente se tiene para cualquier primo p en el lugar de 2, es decir, si un primo divide al cuadrado de un número, entonces divide al número.

* 1.19. Pruébese que no hay ningún número racional cuyo cuadrado sea 2 (en otras palabras, que el número $\sqrt{2}$ no es racional). Para ello se puede proceder por contradicción suponiendo que sí existe tal número, y que lo representamos por la fracción $\frac{p}{q}$, en la cual p y q no tienen divisores comunes. Esta fracción cumple, según la hipótesis,

$$\frac{p^2}{q^2} = 2.$$

Utilizando el ejercicio 1.18, lléguese a la contradicción de que p y q tienen un divisor común, el 2.

Análogamente se prueba que si n es un entero no cuadrado, no existe un racional cuyo cuadrado sea n (es decir, que $\sqrt{3}, \sqrt{5}, \sqrt{7}, \ldots$ no son racionales).

Capítulo 2

Conjuntos

En este capítulo abordamos los elementos básicos de la teoría de conjuntos. Los conjuntos se han convertido en los objetos matemáticos más fundamentales, sobre los que se construye el resto de las matemáticas. Y la teoría de conjuntos, a su vez, se edifica sólidamente sobre axiomas mediante las leyes de la lógica de las que se ha hecho un esbozo en el capítulo precedente.

Por ello la primera sección de este capítulo se dedica a declarar los axiomas que usaremos, para continuar después mediante definiciones y teoremas con sus demostraciones. La colección de axiomas de la teoría de conjuntos es un tema complicado y nunca cerrado a la discusión. Actualmente se considera como esquema básico el de los nueve axiomas de Zermelo y Fraenkel. Sin embargo, para nuestro propósito, mucho más modesto, de introducir las operaciones entre conjuntos, basta con cinco axiomas y a ellos nos limitaremos. Los otros axiomas son necesarios para desarrollar la teoría de los ordinales y los cardinales, y se pueden encontrar, por ejemplo, en libros como [1], [2],[4] o [5].

En la segunda parte del capítulo se introducen las operaciones del complemento, unión e intersección. Las definiciones son una traducción, paso por paso, de los conectores entre proposiciones lógicas: negación, disyunción y conjunción respectivamente. Por ello no debe extrañar que el álgebra de conjuntos sea idéntica al álgebra de proposiciones (es la estructura algebraica conocida como álgebra de Boole). Finalmente se define una operación más entre conjuntos, el producto cartesiano, que no tiene un análogo en el capítulo anterior.

2.1. Axiomas y primeras definiciones

Cualquier intento de definir el concepto de conjunto está condenado a enumerar sinónimos como son colección, familia, agregado, agrupación, etc. Lo importante de la idea que asociamos al término conjunto es que contiene elementos y debemos poder expresar si un elemento pertenece o no a un conjunto: la pertenencia es el concepto sobre el que se construye la teoría de conjuntos, es el concepto primitivo (es decir, que no se define). El símbolo que indica que x

pertenece al conjunto A es $x \in A$, y decimos que x es elemento de A, mientras que $x \notin A$ es su negación.

La teoría de conjuntos tiene esencialmente dos actividades: comparar conjuntos y construir nuevos conjuntos a partir de unos dados (para, después, comparar los nuevos con los originales). En cualquiera de los dos casos, la teoría usa conjuntos ya existentes, no puede crear un conjunto de la nada. Por ello el primer axioma que enunciamos es el que dice que, al menos, existe un conjunto de modo que toda la teoría no se quede vacía.

2.1 Axioma (De existencia)**.** *Existe un conjunto.*

La primera tarea es, por tanto, comparar conjuntos. La comparación más básica es saber si dos conjuntos son iguales o no, que es lo que resuelve el segundo axioma.

2.2 Axioma (De igualdad)**.** *Dos conjuntos son iguales si, y sólo si, contienen los mismos elementos. De manera simbólica lo escribimos*

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

Lo que dice este axioma es que un conjunto queda completamente caracterizado por los elementos que contiene, y no importa si los elementos los guardamos en una caja o en una bolsa, si los ordenamos o están desordenados; sólo importa cuáles son los elementos. También se llama axioma de extensión porque permite definir un conjunto describiendo todos y cada uno de sus elementos, es decir, describiendo su extensión. Para definir un conjunto por extensión se escriben sus elementos entre llaves, por ejemplo $A = \{1, 2, 3, 4, 5\}$.

2.3 Ejemplo. En vista del axioma de igualdad, es claro que $\{1, 2, 3\} = \{2, 3, 1\}$ ya que los dos conjuntos tienen exactamente los mismos elementos. Más aún, también se cumple $\{a, a\} = \{a\}$ por la misma razón.

Ahora podemos definir otra forma de comparar conjuntos más poderosa que la mera igualdad: la inclusión, en la que definimos cuándo un conjunto está contenido en otro y lo llamamos subconjunto.

2.4 Definición. *Un conjunto B es* subconjunto *de otro conjunto A, y se denota $B \subset A$, si todo elemento de B es elemento de A. Es decir,*

$$B \subset A \Leftrightarrow \forall x(x \in B \to x \in A).$$

Para ver que la inclusión es una comparación más poderosa que la igualdad, en el siguiente resultado se indica cómo verificar la igualdad de conjuntos usando la inclusión: la igualdad es una doble inclusión.

2.5 Teorema. *Dos conjuntos son iguales si, y sólo si, cada uno es subconjunto del otro, o bien,*

$$A = B \Leftrightarrow (A \subset B) \wedge (B \subset A).$$

Demostración. Primero, la implicación directa. Si $A = B$ entonces, por el axioma 2.2 todo elemento de A es elemento de B y viceversa. Pero, según la definición anterior, esto que es lo mismo que decir $A \subset B \wedge B \subset A$.

Segundo, la implicación inversa. Si $A \subset B \wedge B \subset A$, entonces todo elemento de A está en B y todo elemento de B está en A, lo cual se puede escribir $\forall x(x \in A \leftrightarrow x \in B)$. Pero esta proposición es precisamente el antecedente del axioma 2.2, por lo cual $A = B$. □

En particular, todo conjunto es subconjunto de sí mismo: $A \subset A$.

Los siguientes tres axiomas son para construir nuevos conjuntos a partir de conjuntos ya conocidos. El primero de ellos, el axioma de especificación utiliza un enunciado abierto $p(x)$ y construye el conjunto formado por los elementos que hacen cierto el enunciado.

2.6 Axioma (De especificación)**.** *Dado un conjunto A y un enunciado abierto $p(x)$ existe el conjunto de los elementos de A que hacen cierto el enunciado.*

Es decir, existe el conjunto B que cumple

$$\forall x(x \in B \leftrightarrow x \in A \wedge p(x)).$$

El conjunto recién definido se representa mediante el símbolo

$$B = \{x \in A \,|\, p(x)\}.$$

Es claro que el nuevo conjunto B es subconjunto de A. En el ejercicio 2.20 se explica la necesidad de exigir que los elementos del nuevo conjunto B se escojan únicamente entre los elementos de algún conjunto A ya conocido.

Vamos a utilizar este axioma inmediatamente para definir un conjunto con nombre propio, el conjunto vacío, que es un conjunto sin elementos. Una definición por especificación es elegante y útil, más que una por extensión.

2.7 Definición. *Sea A un conjunto cualquiera. Definimos el* conjunto vacío *como*

$$\varnothing = \{x \in A \,|\, x \neq x\}.$$

Obsérvese que para definir el vacío así hace falta la existencia de, al menos, un conjunto. Pero el axioma de existencia asegura que sí lo tenemos. Por su definición resulta inmediato que el vacío es subconjunto de cualquier otro.

2.8 Teorema. *El conjunto vacío es subconjunto de cualquier conjunto.*

Esto es, si B es un conjunto arbitrario,

$$\varnothing \subset B.$$

Demostración. Queremos probar la proposición $\forall x(x \in \varnothing \to x \in B)$. Pero el antecedente es siempre falso pues, por definición del conjunto vacío, $\forall x, x \notin \varnothing$. Entonces la implicación es siempre cierta, independientemente del consecuente, y el teorema queda probado. (Ver ejercicio 2.10 para otra prueba). □

En el axioma de especificación se construye, a partir de uno dado, un conjunto más pequeño. En los siguientes axiomas la construcción es al revés: se construyen conjuntos más grandes. En ambos aparecen conjuntos cuyos elementos también son conjuntos.

2.9 Axioma (De la unión)**.** *Dada una familia de conjuntos F, existe un conjunto que contiene los elementos de los elementos de F.*

Si llamamos E a dicho conjunto, entonces podemos definir el conjunto llamado unión de F utilizando el axioma de especificación como sigue.

2.10 Definición. *Dada una familia de conjuntos F, la unión de la familia F es el conjunto formado exactamente por los elementos de los conjuntos que están en F:*

$$\bigcup F = \{x \in E \mid \exists A \in F, x \in A\}.$$

2.11 Ejemplo. Sean los conjuntos $X = \{1, 2, 3\}$ e $Y = \{3, 4, 5\}$ y con ellos la familia $F = \{X, Y\}$. Entonces la unión de F es el conjunto $\bigcup F = \{1, 2, 3, 4, 5\}$.

Por último, si consideramos familias de conjuntos, hay una muy natural y útil: la familia formada por todos los subconjuntos de un conjunto. Pero de nuevo es necesario un axioma que asegure que tal cosa es un conjunto: éste es el quinto y último axioma que utilizamos.

2.12 Axioma (Del conjunto potencia)**.** *Dado un conjunto A, existe el conjunto cuyos elementos son los subconjuntos de A, llamado conjunto potencia y denotado $\mathcal{P}(A)$.*

2.13 Ejemplo. El conjunto potencia de $A = \{1, 2, 3\}$ es

$$\mathcal{P}(A) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{3, 1\}, \{1, 2, 3\}\}.$$

Finalizamos esta sección reuniendo en una lista los cinco axiomas enunciados que son los que usaremos en la teoría desarrollada en este libro:

1. Axioma de existencia
2. Axioma de igualdad
3. Axioma de especificación
4. Axioma de la unión
5. Axioma del conjunto potencia

2.2. Complemento, unión e intersección

En esta sección definimos las operaciones de complemento, unión e intersección y estudiamos sus principales propiedades, que constituyen el álgebra de conjuntos. También mencionamos las operaciones de diferencia y diferencia simétrica que enseguida escribimos en función de las otras.

La operación de unión de conjuntos no es más que el axioma de la unión ya enunciado y la definición que le sigue. Sin embargo lo volveremos a enunciar en el caso particular de dos conjuntos, que es la forma más habitual de manejarla. De hecho, el axioma de la unión es el que permite establecer los resultados algebraicos que aparecen en esta sección. Si tenemos dos conjuntos A y B, dicho axioma nos permite hablar de un conjunto E que contiene todos los elementos de A y todos los elementos de B. Utilizaremos el conjunto E para escribir la definición de las operaciones y deducir sus propiedades. Al definir las tres operaciones en el marco de un conjunto E ocurre que son una traducción directa de las operaciones entre proposiciones lógicas: el complemento corresponde a la negación, la unión a la disyunción y la intersección a la conjunción.

Hay una representación gráfica de los conjuntos que es particularmente apropiada para visualizar las operaciones entre conjuntos: los diagramas de Venn. Un diagrama de Venn representa al conjunto E por un rectángulo, y cualquier subconjunto del mismo por una curva cerrada dentro del rectángulo. Si es posible, los elementos del conjunto E se marcan como puntos dentro del rectángulo y la curva que representa a un subconjunto encierra sus elementos.

2.14 Ejemplo. Los conjuntos $E = \{a, b, c, d\}$ y $A = \{a, b\} \subset E$ se representan en la figura 2.1.

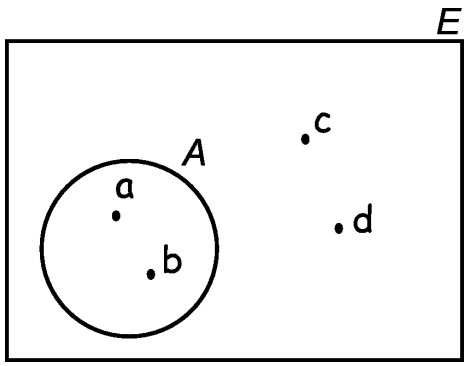


Figura 2.1: Ejemplo de representación gráfica con diagramas de Venn

Debe quedar claro que los diagramas de Venn no sirven como demostraciones de teoremas. Sólo son ilustraciones de los mismos.

Las primera operación que abordamos es el complemento.

2.15 Definición. *El* complemento *de un subconjunto A del conjunto E es el conjunto de todos los elementos de E que no están en A. Se denota A^c y se puede describir como*

$$A^c = \{x \in E \,|\, x \notin A\}.$$

Gráficamente, lo vemos en la figura 2.2.

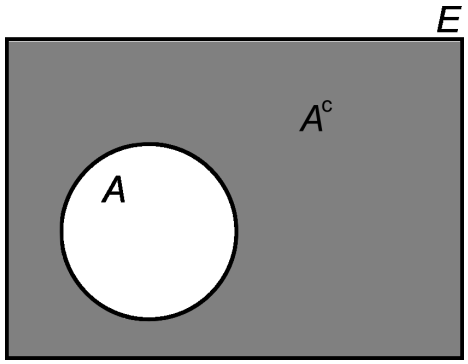


Figura 2.2: Representación gráfica del complemento

2.16 Ejemplo. En el conjunto $E = \{1, 2, 3, 4, 5\}$, el complemento del conjunto $A = \{1, 2\}$ es $A^c = \{3, 4, 5\}$.

A continuación nos ocupamos de la unión y la intersección. En la unión de dos conjuntos se consideran los elementos que están en, al menos, uno de los dos conjuntos. En la intersección, sin embargo, se consideran los elementos que están en ambos conjuntos.

2.17 Definición. *La* unión *de dos conjuntos A y B es el conjunto formado por los elementos que están en A o están en B. Se denota $A \cup B$.*

$$A \cup B = \{x \in E \,|\, (x \in A) \vee (x \in B)\}.$$

La figura 2.3 ilustra esta definición.

2.18 Definición. *La* intersección *de dos conjuntos A y B es el conjunto formado por los elementos que están en A y están en B. Se denota $A \cap B$.*

$$A \cap B = \{x \in E \,|\, (x \in A) \wedge (x \in B)\}.$$

Gráficamente, lo vemos en la figura 2.4.

2.19 Ejemplo. Dados los conjuntos $A = \{1, 2\}$ y $B = \{2, 3\}$ tenemos $A \cup B = \{1, 2, 3\}$ y $A \cap B = \{2\}$.

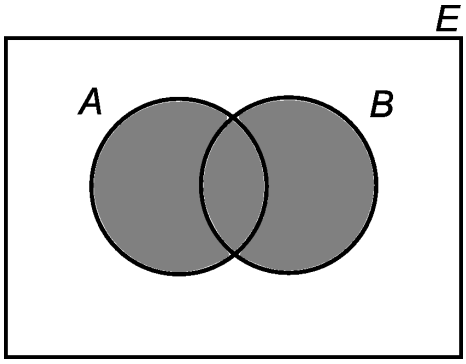


Figura 2.3: Representación gráfica del conjunto $A \cup B$.

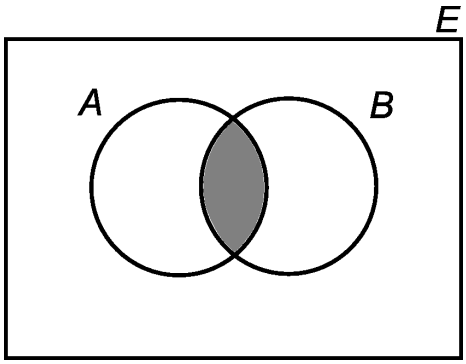


Figura 2.4: Representación gráfica del conjunto $A \cap B$.

Si dos conjuntos verifican $A \cap B = \varnothing$ se dice que son disjuntos porque no tienen elementos en común.

Las operaciones de diferencia y diferencia simétrica consisten, como indica el nombre, en quitar elementos a un conjunto.

2.20 Definición. *La* diferencia *del conjunto A menos el conjunto B es el conjunto formado por los elementos que están en A pero no en B. Se denota $A \setminus B$.*

$$A \setminus B = \{x \in E \,|\, (x \in A) \wedge (x \notin B)\}.$$

En la figura 2.5 se representa esta operación.

2.21 Ejemplo. Las diferencias de los conjuntos $A = \{1, 2\}$ y $B = \{2, 3\}$ son $A \setminus B = \{1\}$, $B \setminus A = \{3\}$.

La diferencia de conjuntos, como en los números, no es conmutativa; en general $A \setminus B \neq B \setminus A$. Sin embargo, la diferencia simétrica se construye de forma que sí lo es.

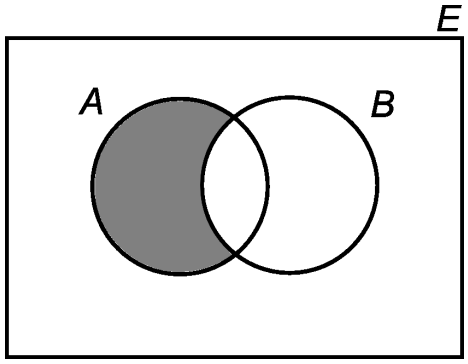


Figura 2.5: Representación gráfica del conjunto $A \setminus B$.

2.22 Definición. *La* diferencia simétrica *de dos conjuntos A y B es el conjunto formado por los elementos que están en A o están en B excepto los comunes a ambos. Se denota $A\triangle B$ y se puede escribir como*

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

Gráficamente, lo vemos en la figura 2.6.

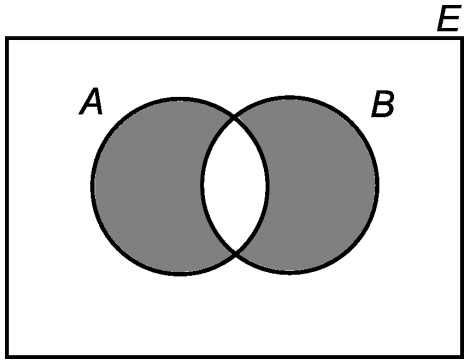


Figura 2.6: Representación gráfica del conjunto $A\triangle B$.

2.23 Ejemplo. La diferencia simétrica de los conjuntos $A = \{1, 2\}$ y $B = \{2, 3\}$ es $A\triangle B = B\triangle A = \{1, 3\}$.

Después de ver las definiciones de las operaciones estudiemos algunas propiedades que satisfacen: las llamadas leyes del álgebra de conjuntos.

Para empezar veamos que la diferencia y la diferencia simétrica se pueden escribir en función de unión, intersección y complemento. Como en el caso de

proposiciones lógicas, también la unión se puede expresar en términos del complemento y la intersección, o la intersección en función del complemento y la unión pero es habitual considerar estas tres por el paralelismo con las proposiciones (ver ejercicio 2.9).

2.24 Teorema. *Dado un conjunto E y subconjuntos A y B del mismo*

$$A \setminus B = A \cap B^c,$$

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

Demostración. Para probar la primera igualdad escribimos la definición de cada miembro y comprobamos que son iguales:

$$A \setminus B = \{x \in E \,|\, (x \in A) \wedge (x \notin B)\},$$

$$A \cap B^c = \{x \in E \,|\, (x \in A) \wedge (x \in B^c)\} = \{x \in E, (x \in A) \wedge (x \notin B)\},$$

donde se ha sustituido $x \in B^c$ por su proposición equivalente $x \notin B$ (dada por la definición 2.15).

Para probar la segunda igualdad basta usar la definición de diferencia simétrica. □

Entonces, las leyes del álgebra de conjuntos son las leyes del álgebra de las operaciones complemento, unión e intersección. A continuación enumeramos algunas de tales leyes. No son todas, pues se pueden deducir otras nuevas a partir de éstas. Tampoco son independientes entre ellas, pues algunas de la lista se pueden deducir de otras. Es una elección arbitraria de las más útiles y habituales.

2.25 Teorema. *Sea E un conjunto y A, B y C subconjuntos arbitrarios de él. Entonces se cumple:*

1. *Ley del doble complemento:*
   $(A^c)^c = A.$
2. *Leyes de idempotencia:*
   $A \cup A = A,$
   $A \cap A = A.$
3. *Leyes conmutativas:*
   $A \cup B = B \cup A,$
   $A \cap B = B \cap A.$
4. *Leyes asociativas:*
   $(A \cup B) \cup C = A \cup (B \cup C),$
   $(A \cap B) \cap C = A \cap (B \cap C).$

5. *Elementos neutros de la unión y la intersección: el vacío es neutro de la unión y el conjunto E es neutro de la intersección:*

   $A \cup \varnothing = A$,

   $A \cap E = A$.

6. *Elementos dominantes de la unión y la intersección: el conjunto E es dominante en la unión y el vacío lo es en la intersección:*

   $A \cup E = E$,

   $A \cap \varnothing = \varnothing$.

7. *Leyes del complemento:*

   $A \cup A^c = E$,

   $A \cap A^c = \varnothing$.

8. *Leyes distributivas:*

   $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,

   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

9. *Leyes de absorción:*

   $A \cup (A \cap B) = A$,

   $A \cap (A \cup B) = A$.

10. *Leyes de De Morgan:*

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

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

Demostración. Las diecinueve propiedades enunciadas se demuestran similarmente y se pueden trazar hasta las propiedades equivalentes de proposiciones del capítulo anterior. Por ejemplo, la propiedad del doble complemento no es más que la propiedad de la doble negación, las propiedades que afectan sólo a la unión son exactamente las mismas que las de la disyunción y las de la intersección aquéllas de la conjunción.

Analicemos en detalle una de las propiedades como muestra: la primera ley de De Morgan. Escribimos el conjunto de la izquierda según su definición.

$$(A \cup B)^c = \{x \in E \mid x \notin (A \cup B)\}.$$

La proposición $x \notin (A \cup B)$ significa $\neg((x \in A) \vee (x \in B))$. Ahora aplicamos la ley de De Morgan de proposiciones lógicas y llegamos a que es equivalente a $(x \notin A) \wedge (x \notin B)$. Pero esta proposición define, precisamente, el conjunto $A^c \cap B^c$ y la propiedad queda demostrada. □

La existencia de la propiedad asociativa permite definir el símbolo $A \cup B \cup C$ como cualquiera de $A \cup (B \cup C)$ o bien $(A \cup B) \cup C$, pues son iguales. El conjunto $A \cup B \cup C$ está formado por los elementos que pertenecen, al menos, a uno de los tres conjuntos y, por tanto, coincide con la unión de la familia $\{A, B, C\}$ tal y como se enunción en el axioma de la unión. Una forma habitual de escribir la unión de una familia grande de conjuntos es mediante índices: $\{A_\alpha\}_{\alpha \in I}$ es una familia formada por los conjuntos A_α, donde el subíndice α toma diferentes valores (para cada valor de α, A_α es un conjunto). Los valores que puede tomar α forman el conjunto de índices, que hemos llamado I. Con esta notación la unión de esta familia se escribe $\bigcup_{\alpha \in I} A_\alpha$.

2.26 Ejemplo. Sea $I = \{1, 2, 3, 4, 5\}$ un conjunto de índices, y sea $\{A_k\}_{k \in I}$ una familia de intervalos de la recta real dada por $A_k = [k, 3k]$. Entonces $\bigcup_{k \in I} A_k = [1, 15]$.

Del mismo modo podemos pensar en la intersección de tres conjuntos, pues también hay asociatividad. El conjunto $A \cap B \cap C$ está formado por los elementos que pertenecen a todos y cada uno de los tres conjuntos. Análogamente, si $\{A_\alpha\}_{\alpha \in I}$ es una familia de conjuntos, definimos la intersección de la familia, escrita $\bigcap_{\alpha \in I} A_\alpha$, como el conjunto de los elementos que pertenecen a todos y cada uno de los A_α.

2.27 Ejemplo. Con los mismos datos del ejemplo anterior, $\bigcap_{k \in I} A_k = \varnothing$.

En las propiedades enunciadas se puede observar el llamado principio de dualidad. Éste asegura que dado un teorema de la teoría de conjuntos con los símbolos $\cup$, $\cap$, E ó $\varnothing$, su expresión dual (la que se obtiene al cambiar $\cup$ por $\cap$ y cambiar E por $\varnothing$) también es un teorema de la teoría.

2.3. Producto cartesiano

El producto cartesiano de dos conjuntos es el conjunto formado por parejas ordenadas, con un elemento de cada conjunto. Pero no hemos definido qué es una pareja ordenada. Obsérvese que el símbolo $\{a, b\}$ denota el conjunto cuyos elementos son a y b; es una pareja. Pero no es ordenada ya que, según el axioma 2.2, $\{a, b\} = \{b, a\}$ pues tienen los mismos elementos. Necesitamos definir el símbolo (a, b) en el que, en general, $(a, b) \neq (b, a)$. ¿Cómo hacerlo? Podemos usar el símbolo $\{a, b\}$ y añadir la información de cuál de los dos elementos es el primero. Una forma de hacerlo es la siguiente definición.

2.28 Definición. *La* pareja ordenada (a, b) *es el conjunto* $\{\{a\}, \{a, b\}\}$.

Es correcto llamar conjunto a (a, b) pues obsérvese que si $a \in A$ y $b \in B$, entonces $\{a, b\}$ es un subconjunto de $A \cup B$, es decir, un elemento de $\mathcal{P}(A \cup B)$. Entonces (a, b) es subconjunto de $\mathcal{P}(A \cup B)$ y, por tanto elemento de $\mathcal{P}(\mathcal{P}(A \cup B))$, todo ello apoyado en la existencia del conjunto potencia que asegura el axioma del mismo nombre.

Con el concepto de pareja ordenada, que es diferente del símbolo $\{a, b\}$ (ver ejercicio 2.14) podemos definir el producto cartesiano como un subconjunto de $\mathcal{P}(\mathcal{P}(A \cup B))$.

2.29 Definición. *El* producto cartesiano *de dos conjuntos A y B, denotado $A \times B$, es el conjunto formado por todas las parejas ordenadas cuyo primer elemento es del conjunto A y cuyo segundo elemento es del conjunto B.*

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

2.30 Ejemplo. Sean los conjuntos $A = \{1, 2\}$ y $B = \{a, b\}$. Entonces, su producto cartesiano es el conjunto $A \times B = \{(1, a), (1, b), (2, a), (2, b)\}$.

Obsérvese que, puesto que las parejas son ordenadas, $A \times B$ no es lo mismo que $B \times A$.

Ejercicios

2.1. Sean $U = \{a, b, c\}$ y su subconjunto $V = \{a, b\}$. Determinar si las siguientes proposiciones son verdaderas o falsas.

a) $V \subset \mathcal{P}(U)$.

b) $a \in \mathcal{P}(U)$.

c) $V \in U$.

d) $\varnothing \in U$.

e) $a \subset U$.

f) $a \subset V$.

2.2. Sean los siguientes conjuntos $A = \{1, 2\}$, $B = \{3, 4\}$, $C = \{A, B\}$. Determinar si cada una de las siguientes proposiciones es verdadera o falsa.

a) $1 \in A$.

b) $1 \in B$.

c) $1 \in C$.

d) $\{1, 2\} \in A$.

e) $\{1, 2\} \in B$.

f) $\{1, 2\} \in C$.

g) $\{1, 2\} \subset A$.

h) $\{1, 2\} \subset B$.

i) $\{1, 2\} \subset C$.

j) $\{1, 2, 3, 4\} = C$.

2.3. Escribir el conjunto potencia de los conjuntos $\varnothing$, $I_1 = \{1\}$, $I_2 = \{1, 2\}$, $I_3 = \{1, 2, 3\}$ e $I_4 = \{1, 2, 3, 4\}$.

Probar por inducción que el conjunto potencia de $I_n = \{1, 2, \ldots, n\}$ tiene 2^n elementos.

2.4. Consideramos el conjunto de los números naturales, $\mathbb{N}$, como referencia y definimos los siguientes subconjuntos del mismo: dado un natural m, el conjunto $m\mathbb{N}$ está formado por los números naturales múltiplos de m; por otro lado el conjunto P es el de los números naturales primos. Describir los conjuntos siguientes.

a) $2\mathbb{N}$ y $(2\mathbb{N})^c$.

b) $2\mathbb{N} \cap 4\mathbb{N}$ y $2\mathbb{N} \cup 4\mathbb{N}$.

c) $2\mathbb{N} \setminus 4\mathbb{N}$ y $4\mathbb{N} \setminus 2\mathbb{N}$.

d) $\bigcup_{k\in\mathbb{N}}(2k)\mathbb{N}$ y $\bigcap_{k\in\mathbb{N}}(2k)\mathbb{N}$.

e) $2\mathbb{N} \cap 3\mathbb{N}$ y $2\mathbb{N} \cup 3\mathbb{N}$.

f) $\bigcup_{p\in P} p\mathbb{N}$ y $\bigcap_{p\in P} p\mathbb{N}$.

2.5. Expresar el resultado de las siguientes operaciones entre intervalos abiertos y cerrados de la recta real en forma de intervalos y dibujarlo.

a) $[-1, 2] \cup]1, 2[$

b) $]-2, 0[\cap]-1, 2[$

c) $]-\infty, 3[\cap [0, \infty[$

d) $]-5, -1[\cap]-1, 1[$

e) $[-\sqrt{2}, 0[\cup [0, \sqrt{2}[$

f) $]0, 3[\cap]\frac{\pi}{2}, \pi[$

g) $[-1, 0]^c$

h) $[\sqrt{3}, \infty[^c$

i) $[0, 1] \setminus]\frac{1}{3}, \frac{2}{3}[$

j) $]0, \infty[\setminus]1, \infty[$

k) $[-1, 1] \setminus [0, 2]$

2.6. En el conjunto de los números complejos $\mathbb{C}$, que tomamos como referencia, definimos los siguientes conjuntos.

$$A = \{z \in \mathbb{C} \,|\, |z| \leq 1\},$$
$$B = \{z \in \mathbb{C} \,|\, |z| \geq 1\},$$
$$C = \{z \in \mathbb{C} \,|\, |z| = 1\},$$
$$D = \{z \in \mathbb{C} \,|\, z = ix, \text{para algún } x \in \mathbb{R}\}.$$

Dibújense dichos conjuntos en el plano complejo y el resultado de cada una de las siguientes operaciones.

a) A^c, B^c.

b) $A \cup B$, $A \cap B$.

c) $D \cup \mathbb{R}$, $D \cap \mathbb{R}$.

d) $C \cup (D \cup \mathbb{R})$, $C \cap (D \cup \mathbb{R})$.

e) $C \cup \mathbb{Z}$, $C \cap \mathbb{Z}$.

f) $A^c \cap \mathbb{N}$, $B^c \cap \mathbb{N}$.

2.7. Demuéstrese la equivalencia de las siguientes proposiciones.

i) $A \subset B$.

ii) $A \cap B = A$.

iii) $A \cup B = B$.

iv) $B^c \subset A^c$.

Por tanto, cualquiera de las otras tres puede ser utilizada para caracterizar un subconjunto. Sugerencia: basta con probar i) $\Rightarrow$ ii) $\Rightarrow$ iii) $\Rightarrow$ iv) $\Rightarrow$ i).

2.8. Probar que la unión de dos conjuntos es el menor conjunto que contiene a ambos. Es decir, si C es un conjunto tal que $A \subset C$ y $B \subset C$ entonces $A \cup B \subset C$.

Análogamente, probar que la intersección de dos conjuntos es el mayor conjunto contenido en ambos.

2.9. Exprésese la unión de conjuntos en términos del complemento y la intersección.

2.10. Demostrar por contradicción el teorema 2.8 que dice que el vacío es subconjunto de cualquier conjunto. Es decir, asumir que existe un conjunto A, distinto de $\varnothing$, para el cual no se cumple $\varnothing \subset A$, y deducir de ahí una contradicción.

2.11. Dados los conjuntos $I_m = \{1, \ldots, m\}$ e $I_n = \{1, \ldots, n\}$, describir los conjuntos $I_m \times I_n$ e $I_n \times I_m$.

2.12. Describir gráficamente los conjuntos $\mathbb{N}\times\mathbb{N}$, $[0,1]\times[0,1]$, $\mathbb{N}\times[0,1]$ y $[0,1]\times\mathbb{N}$, con $[0,1] \subset \mathbb{R}$ el intervalo unitario de la recta real, interpretando las parejas ordenadas como coordenadas de puntos del plano cartesiano.

2.13. Describir los conjuntos $\varnothing \times \varnothing$, $\varnothing \times A$, $A \times \varnothing$, donde A es un conjunto no vacío.

2.14. Usando la definición 2.28 de pareja ordenada y el axioma de igualdad, demostrar

$$(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d.$$

2.15. Demostrar que el producto cartesiano se distribuye sobre la operación unión, es decir, que para cualesquiera conjuntos A, B y C se cumple

$$A \times (B \cup C) = (A \times B) \cup (A \times C).$$

Sin embargo, la unión no se distribuye sobre el producto cartesiano, es decir, en general

$$A \cup (B \times C) \neq (A \cup B) \times (A \cup C).$$

2.16. Sea $\mathcal{D}$ el conjunto de las palabras que aparecen en un diccionario. Consideremos los siguientes subconjuntos que corresponden a los capítulos: A es el subconjunto de las palabras que comienzan con la letra a, B el de las palabras que comienzan con la letra b, etc. Además consideremos la familia de subconjuntos $\{L_n\}_{n\in\mathbb{N}}$ donde L_n contiene las palabras que tienen n o menos letras.

Describir el resultado de las siguientes operaciones.

a) $A \cup B$

b) $A \cap B$

c) $A \cap (B \cup C \cdots \cup Z)$

d) $(F \cap G)^c$

e) $(L_2)^c$

f) $(A \cup L_3)^c$

g) $(A \cap L_3)^c$

h) $L_n \cup L_{n+1}$

i) $L_n \cap L_{n+1}$

j) $\bigcup_{n\in\mathbb{N}} L_n$

k) $\bigcap_{n\in\mathbb{N}} L_n$

* 2.17. Para cada natural n definimos el intervalo cerrado de la recta real $A_n = \left[\frac{1}{n}, n\right]$, es decir, los números reales x que cumplen $\frac{1}{n} \leq x \leq n$. Consideramos la familia $\{A_n\}_{n\in\mathbb{N}}$. En ella se pide calcular

a) A_1, A_2 y A_3.

b) $A_2 \cup A_3$ y $A_2 \cap A_3$.

c) $A_n \cup A_{n+1}$.

d) $A_n \cap A_{n+1}$.

e) $\bigcup_{n\in\mathbb{N}} A_n$.

f) $\bigcap_{n\in\mathbb{N}} A_n$.

* 2.18. Para cada natural n definimos el intervalo abierto de la recta real $B_n = \left]\frac{n}{n+1}, \frac{n+1}{n}\right[$, es decir, los números reales x que cumplen $\frac{n}{n+1} < x < \frac{n+1}{n}$. Consideramos la familia $\{B_n\}_{n\in\mathbb{N}}$. Se pide calcular

a) B_1, B_2 y B_3.

b) $B_2 \cup B_3$ y $B_2 \cap B_3$.

c) $B_n \cup B_{n+1}$.

d) $B_n \cap B_{n+1}$.

e) $\bigcup_{n\in\mathbb{N}} B_n$.

f) $\bigcap_{n\in\mathbb{N}} B_n$.

* 2.19. Para cada valor de α en el intervalo abierto $]0, 1[$ definimos el intervalo cerrado $C_\alpha = \left[\alpha, \frac{1}{\alpha}\right]$, es decir, los números reales x que cumplen $\alpha \leq x \leq \frac{1}{\alpha}$. Consideramos la familia $\{C_\alpha\}_{\alpha\in]0,1[}$. Se pide calcular

a) $C_{0.1}$, $C_{0.5}$ y $C_{0.9}$.

b) $\bigcup_{\alpha\in]0,1[} C_\alpha$.

c) $\bigcap_{\alpha\in]0,1[} C_\alpha$.

* 2.20. El axioma de especificación construye el conjunto $B = \{x \in A \,|\, p(x)\}$ siempre como un subconjunto de A, que es un conjunto conocido pero, ¿no podría enunciarse simplemente como $B = \{x \,|\, p(x)\}$ sin necesidad del conjunto A? La respuesta es no, porque en ese caso aparece la *paradoja de Russell* que fue la que dio inicio al esfuerzo de axiomatizar rigurosamente la teoría de conjuntos.

La paradoja de Russell consiste en considerar como enunciado $p(x)$ el siguiente: $x \notin x$, donde x es cualquier conjunto. Construyamos el conjunto $B = \{x \,|\, x \notin x\}$, es decir, el formado por los conjuntos que no se contienen a sí mismos. Ahora preguntémonos ¿B se contiene a sí mismo ($B \in B$)?

Muéstrese que al intentar responder esta pregunta se comprueba que la existencia de este conjunto B es una contradicción. Es decir, si la respuesta es afirmativa, llegamos a contradicción y si la respuesta es negativa también llegamos a contradicción.

Compruébese ahora que, al definir el conjunto B con el axioma de especificación (exigiendo que haya un conjunto A), ya no hay contradicción.

Por último, pruébese que no puede existir un conjunto universal (el que contiene a todos los conjuntos) ya que de nuevo se cae en la paradoja de Russell.

Una familia de conjuntos indexada por los naturales se llama una sucesión de conjuntos: $\{A_n\}_{n\in\mathbb{N}}$. Se define el límite superior de una sucesión de conjuntos como

$$\limsup A_n = \bigcap_{n\in\mathbb{N}} \Big(\bigcup_{m\geq n} A_m \Big).$$

Análogamente, se define límite inferior como

$$\liminf A_n = \bigcup_{n\in\mathbb{N}} \Big(\bigcap_{m\geq n} A_m \Big).$$

Una sucesión se dice que tiene límite si ambos límites, superior e inferior, coinciden.

* 2.21. Determinar si las siguientes sucesiones de subconjuntos de $\mathbb{N}$ tienen límite.

a) $A_n = \{1\}$.

b) $A_n = \{n\}$.

c) $A_n = \{1, 2, \ldots, n\}$.

d) $A_n = \{n, n+1, \ldots, 2n\}$.

* 2.22. Determinar si las siguientes sucesiones de subconjuntos de $\mathbb{R}$ (todos ellos con forma de intervalo abierto de la recta) tienen límite.

a) $B_n =]-n, n[$.

b) $B_n = \left]-\frac{1}{n}, \frac{1}{n}\right[$.

c) $B_n = \left]\frac{-1}{n}, n\right[$.

d) $B_n = \left]-\frac{1}{n}, 1+\frac{1}{n}\right[$.

* 2.23. Probar que en toda sucesión de conjuntos $\{A_n\}_{n\in\mathbb{N}}$ se cumple

$$\liminf A_n \subset \limsup A_n.$$

* 2.24. Una sucesión de conjuntos $\{A_n\}_{n\in\mathbb{N}}$ es creciente si para todo $n \in \mathbb{N}$ se cumple $A_n \subset A_{n+1}$. Es decreciente si se cumple $A_{n+1} \subset A_n$.

a) Probar que toda sucesión creciente tiene límite y está dado por $\lim A_n = \bigcup_{n\in\mathbb{N}} A_n$.

b) Probar que toda sucesión decreciente tiene límite y está dado por $\lim A_n = \bigcap_{n\in\mathbb{N}} A_n$.

Capítulo 3

Relaciones

En la teoría desarrollada hasta este punto la única referencia que se ha hecho a los elementos de un conjunto es la pertenencia a dicho conjunto. No hay ninguna conexión entre los elementos de un conjunto (aparte de la de pertenecer al mismo) y, mucho menos, entre elementos de diferentes conjuntos. El papel de las relaciones y las funciones es, precisamente, establecer dichas conexiones.

Las relaciones son la forma más básica (y por ello de más alcance) de imponer una estructura en un conjunto. En este capítulo estudiamos la definición general de relación y enseguida nos concentramos en los dos tipos más importantes: las relaciones de equivalencia y las relaciones de orden.

Las equivalencias son las que permiten clasificar los elementos de un conjunto. El objetivo del estudio de las equivalencia es ver el resultado de que toda equivalencia da lugar a una clasificación de los elementos del conjunto y viceversa, toda clasificación (o partición) de un conjunto procede de una relación de equivalencia.

Los órdenes son los que ordenan los elementos de un conjunto. El objetivo del estudio de los órdenes es conocer diferentes tipos de órdenes que existen y, en particular, entender la estructura de orden de los naturales, de los enteros, de los racionales y de los reales. Para ello enunciaremos las propiedades que distinguen cada uno de estos órdenes de todos los demás.

3.1. Relaciones

Partamos de un ejemplo considerando el conjunto de habitantes de una ciudad. En él podemos relacionar entre sí a los habitantes que viven en el mismo barrio, con lo cual cada habitante estará conectado con algunos otros –sus vecinos– y no lo estará con algunos más. Podemos pensar en otro ejemplo en la misma ciudad si relacionamos a cada habitante con sus hijos, si los tiene y viven en la misma ciudad. Definimos relación como un objeto matemático para describir conexiones entre los elementos de un conjunto. En particular estudiamos dos tipos de especial importancia: las relaciones de equivalencia y las relaciones

de orden. Éstas son, respectivamente, la forma matemática de establecer clasificaciones, como ocurre en el caso de los barrios de la ciudad, y de ordenar objetos, que es lo que ocurre entre padres e hijos.

Se trata, por tanto, de decir qué elementos están relacionados con cuáles, y una forma es escribiendo parejas ordenadas (a, b) que signifiquen que el elemento a está relacionado con el b. Por los ejemplos anteriores vemos que el orden es importante (no es igual que a sea padre de b o que b lo sea de a). Por todo ello, damos la siguiente definición.

3.1 Definición. *Una relación R en un conjunto A es un subconjunto no vacío del producto cartesiano $A \times A$.*

Para denotar que un elemento a está relacionado con otro b por la relación R escribimos $(a, b) \in R$ o también aRb (y su negación $a \not R b$).

3.2 Ejemplo. En el conjunto $A = \{1, 2, 3\}$, $R_1 = \{(1, 2), (1, 3), (2, 3)\}$ es una relación que podríamos llamar la relación del orden habitual, ya que indica que el primer elemento del par precede al segundo según el orden habitual de los números. Otra relación es $R_2 = \{(1, 1), (1, 3), (2, 2), (3, 1), (3, 3)\}$, que podríamos llamar la relación de paridad, pues los elementos de cada pareja son ambos pares o ambos impares.

En la definición no se exige que todos los elementos del conjunto estén relacionados con algún otro, ni que todos reciban la relación de alguno. Por ello definimos el dominio y el contradominio a continuación.

3.3 Definición. *El* dominio *de una relación R en el conjunto A es el subconjunto de A de elementos que están relacionados con algún otro. Lo denotamos $\mathcal{D}(R)$ y lo podemos expresar como*

$$\mathcal{D}(R) = \{x \in A \mid \exists y, xRy\}.$$

3.4 Definición. *El* contradominio *de una relación R en el conjunto A es el subconjunto de A de elementos con los que alguno está relacionado. Lo denotamos $\mathcal{D}'(R)$ y lo escribimos como*

$$\mathcal{D}'(R) = \{x \in A \mid \exists y, yRx\}.$$

3.5 Definición. *La* relación inversa *de una relación R es la relación formada por las parejas de R invirtiendo el orden de los elementos en cada pareja. Se denota por R^{-1}. Es decir,*

$$R^{-1} = \{(a, b) \in A \times A \mid bRa\}.$$

De la definición se desprende inmediatamente que $\mathcal{D}(R^{-1}) = \mathcal{D}'(R)$ y $\mathcal{D}'(R^{-1}) = \mathcal{D}(R)$.

Hay una forma de representación gráfica para relaciones que es muy intuitiva e ilustrativa (cuando se puede poner en práctica). Se representa el conjunto y sus elementos como en un diagrama de Venn, y cada pareja (a, b) de la relación se representa por una flecha que nace en el punto a y muere en el punto b.

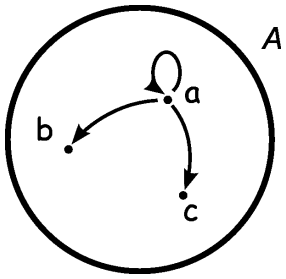


Figura 3.1: Representación de la relación del ejemplo 3.6.

3.6 Ejemplo. La figura 3.1 representa la relación $R = \{(a,a),(a,b),(a,c)\}$ definida en el conjunto $A = \{a,b,c\}$.

El estudio matemático de las relaciones se concentra en la estructura que impone la relación en el conjunto, independientemente de cómo se haya definido. Para ello estudia propiedades de las relaciones que se definen independientemente del significado de la relación. A continuación describimos formalmente tales propiedades.

3.7 Definición. *Una relación definida en un conjunto se llama* reflexiva *si cada elemento del conjunto está relacionado consigo mismo. Es* irreflexiva *si ningún elemento se relaciona consigo mismo.*

$$R \textit{ reflexiva } \Leftrightarrow \forall x \in A, xRx,$$

$$R \textit{ irreflexiva } \Leftrightarrow \forall x \in A, x \not R x.$$

3.8 Ejemplo. La relación "vivir en la misma ciudad" es reflexiva, ya que todo el mundo vive en la misma ciudad que sí mismo, mientras que "ser madre de", es irreflexiva, pues nadie es madre de sí mismo. Por otro lado, la relación "ser empleado de" no es ni una ni otra, pues algunos empresarios son empleados de sí mismos, mientras que muchos trabajadores son empleados de otra persona y no de ellos mismos.

3.9 Ejemplo. La figura 3.2 representa una relación reflexiva y una irreflexiva.

3.10 Definición. *Una relación es* simétrica *si para cada pareja de la relación, la pareja en orden inverso también forma parte de la relación. Es* asimétrica *si para toda pareja en la relación se cumple que su inversa no está en la relación. Por último, una relación* antisimétrica *es aquélla en que las únicas parejas cuyas inversas también son parte de la relación son las parejas de elementos iguales.*

$$R \textit{ simétrica } \Leftrightarrow \forall x, y(xRy \rightarrow yRx),$$

$$R \textit{ asimétrica } \Leftrightarrow \forall x, y(xRy \rightarrow y \not R x),$$

$$R \textit{ antisimétrica } \Leftrightarrow \forall x, y((xRy \wedge yRx) \rightarrow x = y).$$

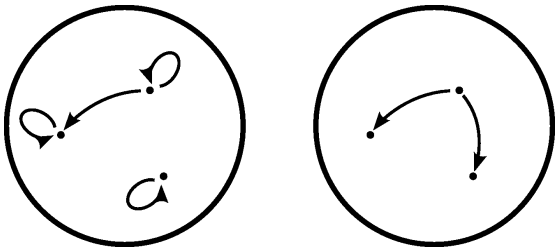


Figura 3.2: Una relación reflexiva y una relación irreflexiva

3.11 Ejemplo. La relación entre mercancías de una tienda de "tener el mismo precio" es simétrica. "Ser más caro que", es una relación asimétrica.

3.12 Ejemplo. La figura 3.3 representa una relación simétrica, una asimétrica y una antisimétrica.

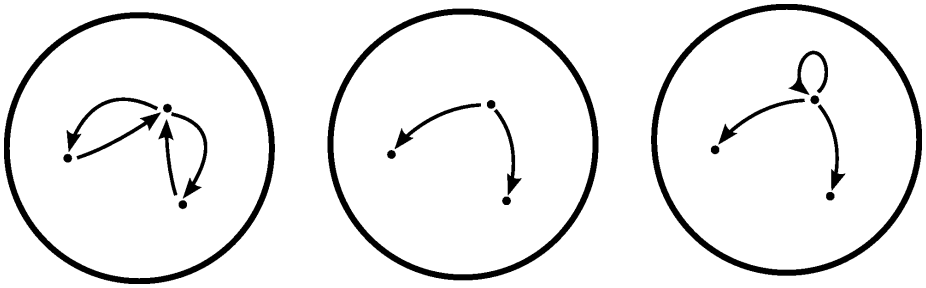


Figura 3.3: Una relación simétrica, una asimétrica y una antisimétrica.

3.13 Definición. *Una relación es* transitiva *si siempre que un elemento se relaciona con un segundo elemento, y éste con un tercero, entonces el primero está relacionado con el tercero.*

$$R \text{ transitiva } \Leftrightarrow \forall x, y, z((xRy \wedge yRz) \rightarrow xRz).$$

3.14 Ejemplo. La relación de parentesco "ser descendiente de" es una relación transitiva. Sin embargo, "ser padre de" no lo es.

3.15 Ejemplo. La figura 3.4 representa una relación transitiva y otra que no lo es.

Estas propiedades no son todas independientes. Para empezar, por ejemplo, las propiedades reflexiva e irreflexiva son incompatibles, al igual que las propiedades de simetría y antisimetría. Además, tenemos las dependencias que se indican en el ejercicio 3.3

En las siguientes secciones estudiamos los dos tipos más importantes de relaciones.

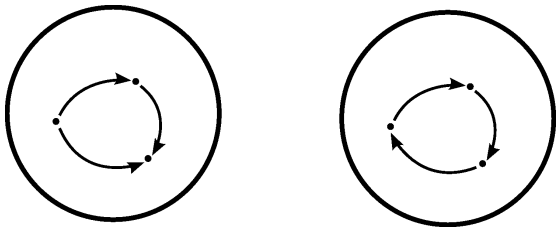


Figura 3.4: Una relación transitiva y una que no lo es.

3.2. Relaciones de equivalencia

La relación de equivalencia, o simplemente equivalencia, es la herramienta matemática para hacer clasificaciones. Primero definimos equivalencia; luego definimos clasificación o, como se le suele llamar, partición; finalmente vemos el teorema fundamental, que afirma que ambas son la misma cosa.

3.16 Definición. *Una relación es una* equivalencia *si es reflexiva, simétrica y transitiva. Si el elemento a está relacionado con b, lo denotamos $a \sim b$.*

3.17 Ejemplo. Consideremos el conjunto de los polígonos regulares y la relación de semejanza, en la que un polígono se relaciona con otro si tienen el mismo número de lados, sus ángulos respectivos son iguales y sus lados proporcionales. Es una relación reflexiva, pues un polígono es semejante a sí mismo. Es simétrica, pues si un polígono es semejante a otro, el otro lo es al uno ya que los ángulos son iguales y los lados proporcionales con el factor de proporcionalidad inverso del primero. Por último, si un polígono es semejante a un segundo y éste a un tercero, el primero es semejante al tercero, pues tienen el mismo número de lados, ángulos iguales y lados proporcionales con factor el producto de los dos factores originales.

3.18 Teorema. *La relación inversa de una equivalencia es ella misma.*

$$R \text{ equivalencia } \Rightarrow R^{-1} = R.$$

Demostración. En realidad es un resultado más general, pues vale para cualquier relación simétrica. Por ser R simétrica, $\mathcal{D}(R) = \mathcal{D}'(R) = \mathcal{D}(R^{-1}) = \mathcal{D}'(R^{-1})$, y para cada pareja $(a, b) \in R$ también $(b, a) \in R$ y, por tanto, ambas están en R^{-1}. □

Representando gráficamente una equivalencia (por ejemplo la figura 3.5) se observa enseguida que los elementos se agrupan en subconjuntos disjuntos entre sí. Este es el resultado central de la teoría de equivalencias. Una equivalencia produce una clasificación de los elementos del conjunto. Cada clase contiene elementos que están relacionados todos entre sí y no están relacionados con ningún otro fuera de su clase. Estas clases se denominan clases de equivalencia.

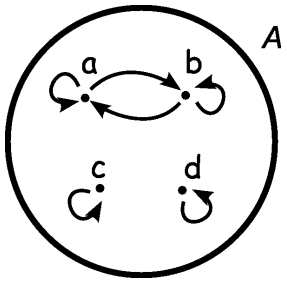


Figura 3.5: Una equivalencia en el conjunto $A = \{a, b, c, d\}$. Aparecen tres clases de equivalencia: $\{a, b\}$, $\{c\}$, $\{d\}$.

3.19 Definición. *Dada una equivalencia R definida en A y un elemento a del conjunto A, la* clase de equivalencia *de a es el subconjunto de los elementos relacionados con él. La denotamos por $[a]$, y decimos que a es un representante de dicha clase. Se puede escribir como*

$$[a] = \{b \in A \,|\, a \sim b\}.$$

El representante de una clase es parte de la clase (como era de esperar), ya que la relación es reflexiva. Pero, por otro lado, cualquier elemento de la clase puede ser un representante. Finalmente, elementos no relacionados entre sí están en clases diferentes. Escribimos estas ideas en un teorema.

3.20 Teorema. *Sea R una equivalencia definida en un conjunto A, entonces*

1. *cada elemento del conjunto está en la clase que representa, es decir $\forall a \in A$,*

$$a \in [a],$$

2. *dos elementos están relacionados si, y sólo si, están en la misma clase de equivalencia, es decir $\forall a, b \in A$,*

$$a \sim b \Leftrightarrow [a] = [b].$$

Demostración. El primer punto es consecuencia inmediata de que toda equivalencia es reflexiva y la defición de clase de equivalencia. Para el segundo punto, separamos en dos la doble implicación.

Primero veamos que $a \sim b \Rightarrow [a] = [b]$ demostrando la igualdad de $[a]$ y $[b]$ por una doble contención. Si un elemento c está en $[b]$ es porque $b \sim c$. Ahora bien, por ser la relación transitiva y tener $a \sim b$ por hipótesis, entonces se cumple $a \sim c$, con lo cual $c \in [a]$. Hemos probado $[b] \subset [a]$. Como, además, la relación es simétrica, entonces $b \sim a$ y el mismo argumento nos lleva a $[a] \subset [b]$. Por tanto $[a] = [b]$.

Por último veamos que $[a] = [b] \Rightarrow a \sim b$. Como $[a]$ y $[b]$ son una misma clase, entonces a y b están en dicha clase, por el primer punto de este teorema. Entonces, por definición de los símbolos $[a]$ y $[b]$, se cumple tanto $a \sim b$ como $b \sim a$. □

3.2.1. Equivalencias y particiones

El principal resultado de la teoría de equivalencias, como se ha dicho, es que las clases de equivalencia constituyen una clasificación de los elementos del conjunto. Es decir, todo elemento está en una clase de equivalencia y sólo en una. Enunciamos primero una definición precisa del concepto de clasificación o partición para, después, enunciar y demostrar el teorema. Nótese que la definición de partición no habla de elementos, sino de subconjuntos, pero es equivalente a decir que cada elemento está en uno, y sólo uno, de tales subconjuntos.

3.21 Definición. *Una* partición *de un conjunto A es una familia de subconjuntos de A, $\{A_\alpha\}_{\alpha\in I}$, donde I es un conjunto de índices, tal que la unión de todos los subconjuntos es el conjunto A y la intersección de dos diferentes cualesquiera es vacía.*

Es decir, $\{A_\alpha\}_{\alpha\in I}$ es una partición de A si

1. $\forall\alpha \in I, A_\alpha \subset A$,
2. $\bigcup_{\alpha\in I} A_\alpha = A$ *y*
3. $\forall\alpha, \beta \in I(\alpha \neq \beta \rightarrow A_\alpha \cap A_\beta = \varnothing)$.

3.22 Ejemplo. Dado el conjunto $A = \{1, 2, 3, 4, 5, 6\}$, las familias $P_1 = \{\{1, 2\}, \{3, 4, 5\}, \{6\}\}$ y $P_2 = \{\varnothing, A\}$ son particiones de A, mientras que $P_3 = \{\{1, 2, 3, 4\}, \{4, 5, 6\}\}$ y $P_4 = \{\{1, 2\}, \{6\}\}$ no lo son.

3.23 Teorema. *Si R es una equivalencia en el conjunto A, sus clases de equivalencia constituyen una partición de A.*

Demostración. Debemos probar que las clases de equivalencia verifican las tres condiciones de la definición 3.21 de partición.

1. Las clases de equivalencia son, obviamente por su definición, subconjuntos de A.
2. Todo elemento de A está en alguna clase de equivalencia pues, por el teorema anterior, $a \in [a]$. Entonces, es claro que la unión de todas las clases de equivalencia contiene todos los elementos de A, y no más, por el punto anterior.
3. Para probar que clases de equivalencia diferentes son disjuntas nos fijamos en la contrapositiva: si tienen un elemento en común, entonces son iguales. Pero, precisamente esta implicación también se ha probado en el teorema anterior.

□

3.24 Ejemplo. En el conjunto de polígonos del plano definimos la relación "tener el mismo número de lados". Se trata de una relación de equivalencia que crea en el conjunto de polígonos la partición en triángulos, cuadriláteros, pentágonos, ...

La conexión entre equivalencias y particiones que establece el teorema anterior queda totalmente complementada por el siguiente teorema, que es su recíproco. En definitiva, toda equivalencia produce una partición y toda partición procede de una equivalencia.

3.25 Teorema. *Dada una partición de un conjunto, existe una equivalencia definida en dicho conjunto cuyas clases de equivalencia son los subconjuntos que constituyen la partición.*

Demostración. Sea el conjunto A en el que hay definida una partición. Definamos en A la relación R de modo que dados dos elementos $a, b \in A$, a está relacionado con b si a está en el mismo subconjunto de la partición que b.

Primero veamos que esta relación es una equivalencia. Es reflexiva, pues, obviamente, cualquier elemento está en el mismo subconjunto que él mismo. Es simétrica, pues si a está en el mismo subconjunto que b, entonces b está en el mismo subconjunto que a. Es transitiva, pues si $a \sim b$ y $b \sim c$ significa que tanto a como c están en el mismo subconjunto que b, y b sólo puede estar en uno, ya que los subconjuntos de una partición son disjuntos. Entonces a y c están en el mismo subconjunto y por tanto $a \sim c$.

Ahora veamos que las clases de equivalencia de esta relación son exactamente los subconjuntos de la partición. Por la definición de la relación, la clase $[a]$ está formada por los elementos que se hallan en el mismo subconjunto que a. Es, pues, dicho subconjunto. □

3.26 Ejemplo. Podemos partir la recta real en intervalos de la forma $\mathbb{R} = \bigcup_{n\in\mathbb{Z}}[n, n+1[= \ldots [-1, 0[\cup [0, 1[\cup [1, 2[\ldots$. Esta partición define en $\mathbb{R}$ la relación de equivalencia "tener la misma parte entera".

Finalizamos el estudio de las equivalencias introduciendo un concepto muy sencillo pero de gran alcance en matemáticas: el conjunto cociente. Este concepto atrapa la esencia de la estructura adquirida por un conjunto cuando se define en él una equivalencia: su partición en clases. El conjunto cociente es, precisamente, el conjunto de las clases de equivalencia en que queda dividido el conjunto original (por ello el término cociente).

3.27 Definición. *Dada una equivalencia R definida en un conjunto A, el* conjunto cociente*, denotado A/R (o también $A/\sim$) es el conjunto de las clases de equivalencia de la relación, esto es*

$$A/R = \{[a] \in \mathcal{P}(A) \mid a \in A\}.$$

3.28 Ejemplo. En el conjunto de los números enteros definimos la relación de congruencia módulo 3 (ver ejercicio 3.4) en la que dos números enteros están relacionados si tienen el mismo residuo al dividirlos entre 3. Se trata de una equivalencia con tres clases de equivalencia: los enteros múltiplos de 3, cuyo residuo en la división es cero y que podemos denotar $\overline{0}$, los enteros cuyo residuo en la división es uno, que denotamos $\overline{1}$, y los enteros cuyo residuo es dos, $\overline{2}$.

El conjunto cociente es, por tanto, $\{\overline{0}, \overline{1}, \overline{2}\}$ que se suele denotar $\mathbb{Z}_3$.

3.3. Relaciones de orden

Como su nombre indica, la relación de orden, o simplemente orden, es la herramienta matemática diseñada para ordenar los elementos de un conjunto. Recordemos que en la teoría básica de conjuntos (capítulo anterior) los elementos de un conjunto no están ordenados, y $\{1, 2, 3\}$ es el mismo conjunto que el $\{3, 2, 1\}$ debido al axioma 2.2. El orden supone una estructura añadida al conjunto, y se adquiere mediante la definición en él de una relación apropiada.

Para establecer un orden hemos de señalar qué elementos preceden a cuáles, lo cual se indica mediante la relación: si a precede a b, entonces $(a, b) \in R$. Claramente la pareja inversa no puede ser parte de la relación, por lo cual pediremos que ésta sea asimétrica. Además, si un elemento precede a otro y éste a un tercero, entonces el primero debe preceder al tercero para evitar relaciones cíclicas (ver ejercicio 3.2), por lo cual exigiremos transitividad.

3.29 Definición. *Una relación R definida en un conjunto A es un* orden *si todo elemento de A está en el dominio o en el contradominio y es asimétrica y transitiva. El símbolo $a < b$ se usa para denotar $(a, b) \in R$. El par (A, R) se llama* conjunto ordenado.

El símbolo $a < b$ se lee "a precede a b", "b sucede a a", "a es menor que b" o "b es mayor que a".

3.30 Ejemplo. En el conjunto de los polígonos del plano decimos que un polígono es menor que otro si tienen el mismo número de lados y su área es menor. Se trata de un orden. Obsérvese que no se define ninguna prelación entre, por ejemplo, un triángulo y un cuadrado.

Se puede sustituir en las dos definiciones precedentes la condición de asimetría por la de antisimetría. Se tiene entonces un orden no estricto, y el símbolo utilizado es $\leq$ (ver ejercicio 3.9). Este símbolo también se puede definir como $a \leq b \Leftrightarrow a < b \vee a = b$.

Un resultado muy sencillo y esperable es el siguiente referido a la relación inversa de un orden.

3.31 Teorema. *La relación inversa de un orden es también un orden, denominado orden inverso.*

Demostración. Sea R un orden. Por ser R asimétrica es claro que R^{-1} también lo es. Veamos que también es transitiva. Si $(a, b) \in R^{-1}$ y $(b, c) \in R^{-1}$ es porque $(b, a), (c, b) \in R$. Entonces, por ser R transitiva, $(c, a) \in R$, luego $(a, c) \in R^{-1}$. □

La estructura que impone un orden en un conjunto hace destacar algunos elementos del mismo, por ejemplo, un elemento que sea mayor que todos los demás, un máximo; o un elemento que, aunque no sea mayor que todos los demás, no tenga a nadie por encima de él, un maximal. Veamos con detalle todos estos elementos destacados. En las siguientes definiciones asumimos que A es un conjunto ordenado.

3.32 Definición. *Un elemento de A es* maximal *si no precede a ningún elemento, es decir*

$$a \text{ maximal} \Leftrightarrow \forall x, a \not< x.$$

Análogamente se define elemento minimal *como aquél que no sucede a ningún elemento.*

3.33 Ejemplo. En el orden "ser descendiente de" establecido en un conjunto de personas, todas las personas que no han tenido hijos son elementos minimales. Y todas las personas cuyos ascendientes hayan fallecido, son elementos maximales.

Consideremos otro ejemplo en el conjunto de parejas formadas por una letra y un número del 0 al 9, y supongamos que lo ordenamos fijándonos únicamente en la cifra numérica. Así, tenemos por ejemplo $(f, 3) < (a, 5)$ mientras que $(b, 7)$ y $(r, 7)$ no son comparables, es decir, no establecemos ningún orden entre ellos. Entonces todas las parejas cuya cifra sea 0 son elementos minimales, mientras que todas las parejas con la cifra 9 son maximales.

3.34 Definición. *Un elemento de A es* máximo *si sucede, o es igual, a cada elemento del conjunto. Se denota* $\max A$.

$$a = \max A \Leftrightarrow \forall x, x \leq a.$$

Análogamente definimos elemento mínimo *como aquél que precede, o es igual, a todo elemento, denotado* $\min A$.

Conviene hacer notar que no siempre existen máximos y mínimos en un conjunto ordenado, ni tampoco maximales o minimales, como se ve en el siguiente ejemplo.

3.35 Ejemplo. En el orden "ser descendiente de" del ejemplo anterior, normalmente no hay mínimo ni máximo. Si en el conjunto hay dos hermanos sin hijos, ambos son minimales, pero ninguno es mínimo.

En el conjunto de los números naturales, $\mathbb{N}$, con su orden habitual, hay un mínimo, el 1, pero no hay máximo ni maximales. En el conjunto de los números enteros, $\mathbb{Z}$, no hay mínimo, ni máximo, ni minimales ni maximales.

En los ejemplos se ha visto que un conjunto ordenado puede tener varios maximales y varios minimales. Esto no puede ocurrir con el máximo o con el mínimo, si existen. El siguiente resultado da la relación precisa entre maximal y máximo, minimal y mínimo.

3.36 Teorema. *Todo elemento máximo es maximal y, si existe, el máximo es único. Análogamente, todo elemento mínimo es minimal y, si existe, es único.*

Demostración. Probamos la parte del máximo, pues la del mínimo es similar. Si a es máximo entonces $(x < a) \vee (x = a)$ para cualquier x en el conjunto. Si se da la primera instancia, es claro que $a \not< x$, por la propiedad asimétrica del orden. Si se da la segunda, de nuevo tenemos $a \not< x$, pues de lo contrario también se violaría la propiedad asimétrica. Por tanto a es maximal.

Para ver que es único supongamos que hay dos elementos que sean máximos en A: a y b. Puesto que a es máximo, entonces $b \leq a$ y, puesto que b es máximo, $a \leq b$. Ya que $a < b$ es incompatible con $b < a$, por asimetría, sólo queda la posibilidad $a = b$. Esto justifica que se hable del máximo y se le dé un símbolo. □

Otro concepto estrechamente relacionado con el de máximo es el de supremo (y el ínfimo con el mínimo). Para definir supremo e ínfimo hay que definir primero cota superior y cota inferior.

3.37 Definición. *Sea B un subconjunto de A. Decimos que B está acotado superiormente si existe un elemento de A que es mayor o igual que cualquier elemento de B, lo cual podemos escribir como*

$$B \text{ acotado superiormente } \Leftrightarrow \exists a, \forall b, (b \in B \rightarrow b \leq a).$$

El elemento a se llama una cota superior de B.

Análogamente se define conjunto acotado inferiormente y cota inferior.

Un subconjunto acotado puede tener muchas cotas superiores. En ocasiones existe una que se distingue de las demás, la menor de todas ellas, llamada supremo.

3.38 Definición. *Sea B un subconjunto de A, acotado superiormente. Si el conjunto de cotas superiores de B tiene mínimo, éste elemento se llama supremo de B, denotado* $\sup B$.

Sea B un subconjunto de A, acotado inferiormente. Si el conjunto de cotas inferiores de B tiene máximo, éste elemento se llama ínfimo de B, denotado $\text{ínf}\, B$.

Puesto que no todo conjunto tiene máximo o mínimo, no todo conjunto tiene supremo o ínfimo. Pero lo que sí es cierto es que, si el supremo o el ínfimo existen, entonces son únicos. En el siguiente ejemplo vemos un conjunto que tiene supremo e ínfimo, aunque no máximo ni mínimo, un conjunto que tiene tanto supremo como máximo e ínfimo y mínimo y un conjunto sin supremo ni ínfimo.

3.39 Ejemplo. Consideremos el conjunto de los números racionales (pero no como subconjunto de los reales, sino los racionales solamente). El intervalo cerrado $[0, 1]$, es decir, los racionales entre 0 y 1, éstos incluídos, es un subconjunto acotado. Tiene máximo, el 1, que es también el supremo, y tiene mínimo, el 0, que es ínfimo.

Sin embargo el intervalo abierto $]0, 1[$ de los racionales, es decir, el anterior pero quitando el 0 y el 1, es de nuevo un conjunto acotado. Tiene supremo, el 1, pero no tiene máximo porque 1 ya no pertenece al subconjunto. Igualmente tiene ínfimo, el 0, que no es mínimo por la misma razón.

Algo más complicado es describir un subconjunto acotado pero que no tenga supremo o ínfimo. Un ejemplo clásico es el subconjunto de los números racionales

cuyo cuadrado es menor que 2. Es un conjunto acotado ya que, por ejemplo $\frac{3}{2}$ cumple que su cuadrado es mayor que 2 con lo cual es una cota superior, y $\frac{-3}{2}$ sirve como cota inferior. Es fácil ver que no tiene máximo ni mínimo, porque se define el subconjunto con la condición $r^2 < 2$ en lugar de, por ejemplo $r^2 \leq 2$. Lo interesante es que tampoco tiene supremo ni ínfimo. El supremo debería ser un número racional cuyo cuadrado fuese exactamente 2, el cual no existe (ejercicio 1.19). En el ejercicio 3.17 se estudia con más detalle este ejemplo.

Veamos un ejemplo más sencillo de subconjunto acotado pero sin supremo. Para ello primero ordenamos los números naturales de un modo especial: cualquier número impar precede a cualquier número par, entre los impares se mantiene el orden habitual, mientras que en los pares se invierte el orden habitual. Es decir, queda el orden representado por

$$1, 3, 5, 7, \ldots, \ldots 8, 6, 4, 2.$$

En este conjunto fijémonos en el subconjunto de los números impares: Es acotado superiormente, ya que cualquier par es una cota superior. No tiene máximo, ya que no hay ningún número impar que sea el mayor de todos los impares. Tampoco tiene supremo, porque no hay un número par menor que todos los demás.

La relación precisa entre supremo y máximo de un subconjunto (así como ínfimo y mínimo) se da en el siguiente resultado.

3.40 Teorema. *Un subconjunto acotado superiormente tiene máximo si, y sólo si, tiene supremo y éste pertenece a dicho subconjunto.*

Un subconjunto acotado inferiormente tiene mínimo si, y sólo si, tiene ínfimo y éste pertenece a dicho subconjunto.

Demostración. Probamos la relación entre máximo y supremo, pues la otra es similar. Primero la implicación directa. Sea b el máximo de B. Entonces $x \leq b$ para todo elemento x en B y, por tanto, b es una cota superior de B. Ahora sea c otra cota superior de B. Entonces, como b está en B tenemos $b \leq c$, luego b es mínimo del conjunto de cotas superiores, es decir, b es el supremo de B.

Ahora la implicación inversa. Sea b el supremo de B, el cual cumple además $b \in B$. Por ser supremo es cota superior, luego todo elemento x de B cumple $x \leq b$. Entonces b cumple la definición de máximo de B. □

3.3.1. Orden total

Hemos visto ejemplos de conjuntos ordenados donde existen elementos que no son comparables. Esta situación no se da en el ejemplo más común de conjunto ordenado en matemáticas: los conjuntos numéricos. En ellos todos los elementos son comparables. Esta propiedad le da características especiales al orden y por ello recibe un nombre.

3.41 Definición. *Un orden R en el conjunto A es* total *si dados dos elementos cualesquiera, o bien son iguales, o bien uno precede al otro.*

$$\forall x, y \in A, (x = y) \vee (x < y) \vee (y < x).$$

Esta propiedad también recibe el nombre de tricotomía, por las tres opciones que permite a cada pareja de elementos x, y. Cuando un orden no es total, para recalcar la ausencia de esta propiedad a veces se denomina orden parcial.

3.42 Ejemplo. En un conjunto E de al menos dos elementos, el orden definido por la inclusión de conjuntos es un orden parcial (ejercicio 3.10).

El orden habitual de los números naturales, $\mathbb{N}$, de los enteros, $\mathbb{Z}$, de los racionales, $\mathbb{Q}$, y de los reales, $\mathbb{R}$, son todos órdenes totales.

Una diferencia notable entre los órdenes parciales y totales es la relación de elementos máximos con maximales (y mínimos con minimales). En el teorema 3.36 se estableció que todo máximo es maximal; en un orden total tenemos también el recíproco: todo maximal es máximo. Por tanto, ambos son la misma cosa.

3.43 Teorema. *En un orden total todo maximal es máximo y, por tanto, único y todo minimal es mínimo y, por tanto, único.*

Demostración. Sea a un elemento maximal, y sea x un elemento arbitrario. Por ser a maximal tenemos $a \not< x$ pero, por ser el orden total, a y x son comparables, luego debe ser $x \leq a$, de donde a es máximo. □

Los cuatro conjuntos numéricos aludidos, a pesar de ser todos órdenes totales, tienen propiedades que diferencian sus estructuras de orden. En los próximos párrafos vamos a describir las propiedades que diferencian cada uno de los cuatro órdenes (algunas de estas propiedades no son exclusivas de los órdenes totales, pero hemos preferido enunciarlas aquí para aplicarlas directamente al caso de los conjuntos numéricos).

La primera propiedad es la del buen orden, y diferencia a los naturales de los otros conjuntos.

3.44 Definición. *Un conjunto está* bien ordenado *si todo subconjunto tiene mínimo.*

3.45 Ejemplo. El conjunto de los naturales está bien ordenado. Sin embargo los enteros, racionales y reales no tienen un buen orden pues, por ejemplo, $\mathbb{Z}$ no tiene mínimo.

La siguiente propiedad que estudiamos es la que diferencia el orden en los naturales o los enteros del orden en racionales y reales. En los primeros cada elemento tiene un inmediato sucesor, mientras que en los segundos no es así. Para ello primero definimos inmediato sucesor e inmediato antecesor.

3.46 Definición. *En un conjunto totalmente ordenado A el elemento y es inmediato sucesor del elemento x si y sucede a x y cualquier otro elemento que sucede a x también sucede a y, es decir, si*

$$(x < y) \wedge \forall z, (x < z \to y \leq z).$$

En este caso, decimos que x es inmediato antecesor de y.

Es fácil demostrar que, en caso de existir, el inmediato sucesor de un elemento es único (ejercicio 3.11).

El comportamiento de los conjuntos numéricos respecto a la existencia de inmediatos sucesores se recoge en las siguientes dos propiedades: las propiedades del inmediato sucesor y del inmediato antecesor y el orden lineal.

3.47 Definición. *Un orden total tiene la propiedad de inmediato sucesor si todo elemento que no sea máximo tiene un inmediato sucesor. Análogamente, un orden total tiene la propiedad de inmediato antecesor si todo elemento que no sea mínimo tiene un inmediato antecesor.*

3.48 Definición. *Un orden total R en A es lineal si para cualquier pareja de elementos diferentes existe un elemento situado entre los dos. Es decir, R es lineal si*

$$\forall x, y \in A, (x < y \rightarrow \exists z, x < z < y).$$

Esta propiedad es incompatible con las anteriores en un conjunto (aunque pueden coexistir si cada una se verifica en un subconjunto diferente) como se indica en el siguiente resultado.

3.49 Teorema. *En un conjunto con más de un elemento, si un orden total es lineal, entonces no verifica las propiedades del inmediato sucesor ni del inmediato antecesor.*

Demostración. Probamos su contrapositiva, que es equivalente: si se cumple la propiedad del inmediato sucesor o del inmediato antecesor, entonces no es lineal. Efectivamente, sea x un elemento que no es máximo (existe porque el conjunto tiene más de un elemento) y sea y su inmediato sucesor (con el antecesor es similar). Por definición de inmediato sucesor no existe un z tal que $x < z < y$, luego el orden no es lineal. □

3.50 Ejemplo. Los órdenes en los naturales y en los enteros tienen la propiedad del inmediato sucesor y del inmediato antecesor.

Los órdenes en los racionales y en los reales son lineales: si $x < y$, basta considerar el número $z = \frac{1}{2}(x + y)$.

Falta definir una propiedad que permita diferenciar el orden en los racionales y el orden en los reales: la propiedad del supremo.

3.51 Definición. *Un orden total verifica la propiedad del supremo si todo subconjunto acotado superiormente tiene supremo.*

Un orden total verifica la propiedad del ínfimo si todo subconjunto acotado inferiormente tiene ínfimo.

La propiedad del supremo y la del ínfimo son equivalentes como se exhibe a continuación.

3.52 Teorema. *Un orden total verifica la propiedad del supremo si, y sólo si, verifica la propiedad del ínfimo.*

Demostración. Supongamos que un orden total satisface la propiedad del supremo. Sea un subconjunto acotado inferiormente y consideremos el conjunto de las cotas inferiores de dicho subconjunto. Claramente este conjunto está acotado superiormente y, por hipótesis, tiene supremo. Es fácil ver que el supremo de las cotas inferiores es el ínfimo del subconjunto original. Por tanto se satisface la propiedad del ínfimo.

Igualmente se razona a la inversa probando así la equivalencia. □

3.53 Ejemplo. El orden de los números racionales no satisface la propiedad del supremo, como se mencionó en el ejemplo 3.39. Sin embargo el orden de los números reales sí verifica esta propiedad. De hecho el conjunto de los reales se construye precisamente con este fin.

Ejercicios

3.1. Sea el conjunto $A = \{a, b, c, d\}$. Estudiar las propiedades de las siguientes relaciones definidas en él. En particular, describir sus dominios y contradominios y verificar si son reflexivas, irreflexivas, simétricas, asimétricas, antisimétricas y/o transitivas.

a) $R_1 = \{(a,a), (a,b), (b,a), (b,b), (b,c), (c,b), (c,c)\}$.

b) $R_2 = \{(a,b), (a,c), (a,d)\}$.

c) $R_3 = \{(a,a), (a,b), (a,c), (b,a), (b,b), (b,c), (c,a), (c,b), (c,c), (d,d)\}$.

d) $R_4 = \{(a,c), (a,d), (b,a), (b,c), (b,d), (c,d)\}$.

3.2. En el conocido juego infantil *Piedra, papel o tijera* se establece una relación en el conjunto { piedra, papel, tijera } que determina el vencedor de cada encuentro. Describir esta relación y estudiar sus propiedades. ¿Es una equivalencia? ¿Es un orden?

3.3. Demuéstrense los siguientes teoremas, que señalan algunas dependencias entre las propiedades definidas en las relaciones.

a) Toda relación asimétrica es antisimétrica.

b) Toda relación asimétrica es irreflexiva.

c) Si R es una relación reflexiva en el conjunto A, su dominio y contradominio coinciden y son todo el conjunto A.

3.4. Dado un entero n definimos en el conjunto de los números enteros la relación de congruencia módulo n diciendo que a es congruente con b módulo n si ambos tienen el mismo residuo al dividirlos entre n.

a) Probar que la congruencia es una equivalencia.

b) Para la congruencia módulo 4, hallar la clase de equivalencia de los números 8 y 13. Describir el conjunto cociente.

c) Describir el conjunto cociente en el caso general de la congruencia módulo n.

3.5. En el conjunto de los números enteros sin el cero, $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$, definimos la relación R por la siguiente expresión:

$$x \sim y \Leftrightarrow xy > 0.$$

Se pide:

a) Probar que es una equivalencia.

b) Hallar las clases de equivalencia de los números 1, 7, -4 y -5.

c) Describir el conjunto cociente $\mathbb{Z}^*/R$.

3.6. En el conjunto de parejas de números reales, $\mathbb{R} \times \mathbb{R}$, definimos varias relaciones. En cada una de ellas se pide razonar si es o no una equivalencia y, en caso afirmativo, representar gráficamente en el plano cartesiano las clases de equivalencia y describir el conjunto cociente.

a) $(x_1, y_1) \sim (x_2, y_2) \Leftrightarrow x_1 = y_2$.

b) $(x_1, y_1) \sim (x_2, y_2) \Leftrightarrow x_1 = x_2$.

c) $(x_1, y_1) \sim (x_2, y_2) \Leftrightarrow x_1 - y_1 = x_2 - y_2$.

d) $(x_1, y_1) \sim (x_2, y_2) \Leftrightarrow x_1^2 - y_1 = x_2^2 - y_2$.

3.7. En el conjunto de los números complejos, $\mathbb{C}$, definimos varias relaciones. En cada una de ellas se pide razonar si es o no una equivalencia y, en caso afirmativo, representar gráficamente en el plano complejo las clases de equivalencia y describir el conjunto cociente.

a) $z_1 \sim z_2 \Leftrightarrow |z_1| = |z_2|$.

b) $z_1 \sim z_2 \Leftrightarrow \arg z_1 = \arg z_2$, donde $\arg z$ es el argumento del número complejo z.

c) $z_1 \sim z_2 \Leftrightarrow z_1 = \overline{z_2}$, donde $\overline{z}$ denota el conjugado de z.

d) $z_1 \sim z_2 \Leftrightarrow z_1 + z_2 = 0$.

3.8. En el conjunto de los números reales, $\mathbb{R}$, definimos la relación S por la siguiente expresión:

$$x \sim y \Leftrightarrow x - y \in \mathbb{Z}.$$

Se pide:

a) Probar que es una equivalencia.

b) Hallar las clases de equivalencia de los números 1.67, 3 y π.

c) Describir el conjunto cociente $\mathbb{R}/S$.

d) Intentar repetir el problema cambiando $\mathbb{Z}$ por $\mathbb{N}$.

e) Intentar repetir el problema cambiando $\mathbb{Z}$ por $\mathbb{Q}$.

3.9. ¿Qué estructura resulta de una relación reflexiva, antisimétrica y transitiva?

3.10. Sea un conjunto E y definamos una relación en su conjunto potencia $\mathcal{P}(E)$. Dados dos elementos del conjunto potencia, $A, B \subset E$, A está relacionado con B si $A \subset B$. Demostrar que es una relación de orden. Y demostrar que, si E tiene más de un elemento, entonces el orden no es total (éste es un ejemplo muy habitual de orden parcial).

3.11. Probar que en un orden total, si un elemento tiene inmediato sucesor, éste es único.

3.12. Indicar si los siguientes subconjuntos de $\mathbb{R}$ son acotados superior o inferiormente y, en caso afirmativo, hallar el supremo o el ínfimo correspondientes, señalando si son máximo y mínimo respectivamente.

a) $A = \{x \in \mathbb{R} \,|\, |x| < 2\}$.

b) $B = \{x \in \mathbb{R} \,|\, x^2 < 2\}$.

c) $C = B^c$.

d) $D = \bigcup_{n\in\mathbb{N}}[2n, 2n+1]$.

3.13. En un conjunto totalmente ordenado A definimos los conceptos de intervalo abierto y de intervalo cerrado como sigue: si $a, b \in A$

$$]a, b[= \{x \in A \,|\, a < x < b\}, \text{ intervalo abierto,}$$

$$[a, b] = \{x \in A \,|\, a \leq x \leq b\}, \text{ intervalo cerrado.}$$

a) Describir los siguientes intervalos del conjunto de los enteros: $]-5, 5[$, $[0, 1]$, $]0, 1[$, $]2, 8[$, $[4, 1]$.

b) Probar que, si $a < b$, entonces $[a, b]$ está acotado, tiene supremo e ínfimo que son máximo y mínimo respectivamente.

c) El caso del intervalo abierto no es tan sencillo. Si $a < b$ y b no es inmediato sucesor de a, entonces $]a, b[$ está acotado, tiene supremo e ínfimo pero, si el orden es lineal, no tiene máximo ni mínimo. Si el orden cuenta con las propiedades del inmediato sucesor y el inmediato antecesor entonces sí tiene máximo y mínimo.

3.14. Orden del diccionario. Dados dos conjuntos totalmente ordenados $(A, <_A)$ y $(B, <_B)$, definimos la relación $<_D$ en el conjunto $A \times B$ del siguiente modo: para cualesquiera dos parejas $(a_1, b_1), (a_2, b_2) \in A \times B$, $(a_1, b_1) <_D (a_2, b_2)$ si $a_1 <_A a_2$ o, en caso de que $a_1 = a_2$, si $b_1 <_B b_2$. Comprobar que esta relación define un orden total en $A \times B$, llamado orden del diccionario.

3.15. Consideremos los conjuntos $\mathbb{Z} \times \mathbb{R}$ y $\mathbb{R} \times \mathbb{Z}$ cada uno con el orden del diccionario correspondiente construido a partir de los órdenes habituales de $\mathbb{Z}$ y de $\mathbb{R}$. Estudiar si estos órdenes son lineales, y si tienen las propiedades del inmediato sucesor, del inmediato antecesor, del supremo y del ínfimo.

3.16. Consideremos el conjunto de los naturales, $\mathbb{N}$, ordenado del siguiente modo: cualquier impar precede a cualquier par, entre los impares se mantiene el orden habitual, y entre los pares, también el orden habitual. Es decir, el orden queda de la forma

$$1, 3, 5, \ldots, 2, 4, 6, \ldots$$

Se pide:

a) Probar que se trata de un buen orden.

b) Demostrar que todo buen orden cumple la propiedad del inmediato sucesor (por tanto este orden cumple dicha propiedad).

c) Mostrar que este orden no satisface la propiedad del inmediato antecesor, lo cual prueba que ambas propiedades (sucesor y antecesor) son independientes.

* 3.17. En este ejercicio se pide probar que el conjunto de los números racionales no verifica la propiedad del supremo. Consideremos el conjunto de los racionales cuyo cuadrado es menor que 2, al que llamamos A.

a) Muéstrese que el conjunto A es acotado, tanto superior como inferiormente.

b) Sea r una cota superior de A que no está en A y, por tanto, debe cumplir $2 \leq r^2$. Por el ejercicio 1.19 sabemos que $r^2 \neq 2$, luego tenemos $2 < r^2$. Consideremos entonces el racional $s = \frac{1}{2}(r + \frac{2}{r})$. Pruébese que verifica $s < r$ y $2 < s^2$.

c) Sea ahora r un elemento de A que cumple $\frac{1}{2} < r^2$ (existen, por ejemplo $r = 1$) pruébese que el racional $s = \frac{2}{3}(r + \frac{1}{r})$ cumple $r < s$ y $s^2 < 2$, con lo cual $s \in A$.

Arguméntese que uniendo los dos últimos incisos podemos concluir que el conjunto A no tiene supremo.

* 3.18. El orden de los naturales. La estructura de orden en $\mathbb{N} = \{1, 2, 3, \ldots\}$ se define habitualmente después de haber definido la suma del siguiente modo:

$$a < b \Leftrightarrow \exists n, a + n = b.$$

a) Probar que, efectivamente, es una relación de orden en $\mathbb{N}$.

b) Probar que, además, es un orden compatible con las operaciones de suma y producto. Es decir, que se satisfacen las siguientes dos propiedades: $\forall a, b, c$,

$$a < b \Rightarrow a + c < b + c,$$
$$a < b \Rightarrow ac < bc.$$

* 3.19. Para ver la importancia del concepto de relación de equivalencia y conjunto cociente así como las relaciones de orden, en este ejercicio y el siguiente ilustramos cómo estas herramientas sirven para construir los números enteros y los racionales a partir de los naturales $\mathbb{N} = \{1, 2, 3, \dots\}$.

a) Definición de $\mathbb{Z}$: Consideremos la relación R_1 en el conjunto $\mathbb{N} \times \mathbb{N}$ de parejas de naturales dada por $(m_1, n_1) \sim (m_2, n_2)$ si $m_1 + n_2 = m_2 + n_1$. El conjunto de números enteros se define como el conjunto cociente $(\mathbb{N} \times \mathbb{N})/R_1$. Comprobar que, efectivamente, R_1 es una equivalencia en $\mathbb{N} \times \mathbb{N}$ e identificar en el conjunto cociente las clases de equivalencia correspondientes a los números enteros 1, 3, 0, y -5.

b) Orden en $\mathbb{Z}$: Una vez definido $\mathbb{Z}$ definimos un orden en él utilizando el orden ya definido en los naturales (ejercicio 3.18). Consideramos dos números enteros p_1 y p_2 que, por el inciso anterior, tienen la forma de clases de equivalencia que escribimos $p_1 = [(m_1, n_1)]$. Entonces,

$$p_1 < p_2 \Leftrightarrow m_1 + n_2 < m_2 + n_1.$$

Esta definición tiene el problema de que utiliza un representante de la clase de equivalencia, por ejemplo la pareja (m_1, n_1) para representar el número p_1. Por tanto, lo primero es demostrar que la definición, en realidad, no depende del representante elegido. Una vez hecho eso, demostrar que define una relación de orden en $\mathbb{Z}$.

* 3.20. En este ejercicio definimos el conjunto de los racionales, $\mathbb{Q}$, a partir del de los enteros, $\mathbb{Z}$, con el que se ha trabajado en el ejercicio anterior y del que asumimos que se tienen definidas, además del orden, las operaciones de suma y producto.

a) Definición de $\mathbb{Q}$: Consideremos la relación R_2 en el conjunto $\mathbb{Z} \times \mathbb{Z}^*$ de parejas de enteros (donde el segundo no es cero) dada por $(p_1, q_1) \sim (p_2, q_2)$ si $p_1\, q_2 = p_2\, q_1$. El conjunto de números racionales se define como el conjunto cociente $(\mathbb{Z} \times \mathbb{Z}^*)/R_2$. Comprobar que, efectivamente, R_2 es una equivalencia en $\mathbb{Z} \times \mathbb{Z}^*$ e identificar en el conjunto cociente las clases de equivalencia correspondientes a los números racionales 1, $\frac{1}{2}$, y $\frac{-2}{3}$.

b) Orden en $\mathbb{Q}$: Una vez definido $\mathbb{Q}$ definimos un orden en él utilizando el orden ya definido en los enteros. Consideramos dos números racionales r_1

y r_2 que, por el inciso anterior, tienen la forma de clases de equivalencia que escribimos $r_1 = [(p_1, q_1)]$. Entonces,

$$r_1 < r_2 \Leftrightarrow p_1 q_2 < p_2 q_1.$$

Esta definición tiene el problema, al igual que en el caso de los enteros, de que utiliza un representante de la clase de equivalencia, por ejemplo la pareja (p_1, q_1) para representar el número r_1. Por tanto, lo primero es demostrar que la definición, en realidad, no depende del representante elegido. Una vez hecho eso, demostrar que define una relación de orden en $\mathbb{Q}$.

* 3.21. Una de las diferencias entre el conjunto $\mathbb{C}$ de los números complejos y el resto de conjuntos numéricos habituales ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$) es que los complejos no tienen una relación de orden natural como sí ocurre con los otros conjuntos mencionados. Aunque se pueden definir muchos órdenes en $\mathbb{C}$, ninguno es compatible con las operaciones de suma y producto de números complejos, en el siguiente sentido: $\forall x, y, z$,

$$x < y \to x + z < y + z,$$
$$x < y \wedge 0 < z \to x\, z < y\, z.$$

Probar que es imposible ordenar totalmente $\mathbb{C}$ de forma que, además, se satisfagan las dos condiciones. Sugerencia: estudiar si el número i es mayor o menor que 0.

Capítulo 4

Funciones

Las funciones son herramientas para relacionar elementos de un conjunto, llamado inicial, con elementos de otro conjunto, llamado final. El concepto es parecido al de relación, donde se relacionan elementos de un conjunto entre sí. Sin embargo hay una diferencia esencial. En una función se exige que cada elemento del conjunto inicial esté relacionado sólo con uno del conjunto final. La consecuencia inmediata es que la inversa de una función (es decir los elementos del conjunto final asociados con los que les corresponden del inicial) no es, en general, una función.

Este capítulo tiene dos objetivos, que se alcanzan a través de los conceptos de función inyectiva, función suprayectiva y función biyectiva. El primero es caracterizar las funciones que tienen inversa, que resultan ser las biyectivas. El segundo es mostrar la descomposición canónica de una función como composición de una función inyectiva, una biyectiva y una suprayectiva.

4.1. Definición de función

Queremos utilizar las funciones como herramientas para asignar a cada elemento de un conjunto un elemento de otro. Como en el caso de las relaciones, vamos a expresar esta asignación por parejas, pero ahora formadas por un elemento del conjunto inicial y un elemento del conjunto final. Como se ha dicho, exigiremos además que a cada elemento del conjunto inicial no se le asigne más de uno del final.

4.1 Definición. *Una* función *f del conjunto A al conjunto B es un subconjunto del producto cartesiano $A \times B$ en el que no hay dos parejas que tengan el mismo primer elemento. El conjunto A se llama inicial, y el conjunto B, final y se denotan con el símbolo $f : A \longrightarrow B$.*

4.2 Ejemplo. Sea $A = \{a, b, c\}$ y consideremos los subconjuntos de $A \times A$, $f = \{(a, a), (b, b), (b, c)\}$, $g = \{(a, b), (b, c), (c, a)\}$, $h = \{(a, a), (b, a)\}$. Los tres conjuntos son relaciones en A, pero f no es una función porque el elemento

b aparece como primer elemento en dos parejas. Sin embargo, g y h sí son funciones.

Como otro ejemplo pensemos en el subconjunto de $\mathbb{R}\times\mathbb{R}$, representado como el plano cartesiano con ejes X, Y, dado por los puntos de la circunferencia de radio 1 centrada en el origen (figura 4.1). Este subconjunto no define una función $\mathbb{R} \longrightarrow \mathbb{R}$ ya que las parejas de puntos (x, y_+) y (x, y_-) tienen la primera coordenada igual. Sin embargo sí podemos definir una función si nos restringimos a la semicircunferencia superior. En este caso no hay dos parejas de puntos (x, y) en las que coincida la primera coordenada. Como sabemos que las coordenadas cumplen la ecuación $x^2+y^2 = 1$, podemos igualmente describir esta función como la que asocia a cada número real x entre -1 y 1 el número real $\sqrt{1-x^2}$. (Si hubiésemos considerado la semicircunferencia inferior, hubiera sido $-\sqrt{1-x^2}$).

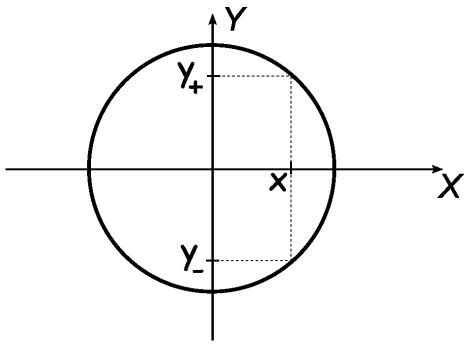


Figura 4.1: Una circunferencia no permite definir una función pues a cada coordenada x le corresponden dos coordenadas y.

Como en el caso de las relaciones, no se ha exigido en la definición que todo elemento del conjunto inicial esté relacionado con alguno del final ni que todo elemento del final reciba la relación de alguno del inicial. Por ello definimos los conceptos de dominio y contradominio de una función, que tendrán mucha más importancia que en el contexto de las relaciones.

4.3 Definición. *El* dominio *de una función $f : A \longrightarrow B$ es el subconjunto de A de elementos relacionados con algún elemento de B. Lo denotamos $\mathcal{D}(f)$.*

$$\mathcal{D}(f) = \{x \in A \,|\, \exists y \in B, (x, y) \in f\}.$$

4.4 Definición. *El* contradominio *de una función $f : A \longrightarrow B$ es el subconjunto de B de elementos con los que algún elemento de A está relacionado. Lo denotamos $\mathcal{D}'(f)$.*

$$\mathcal{D}'(f) = \{y \in B \,|\, \exists x \in A, (x, y) \in f\}.$$

4.5 Ejemplo. Sea la función $f : A \longrightarrow B$, donde $A = \{1, 2, 3\}$, $B = \{a, e, i, o, u\}$ dada por $f = \{(1, e), (3, e)\}$. Entonces $\mathcal{D}(f) = \{1, 3\}$ y $\mathcal{D}'(f) = \{e\}$.

En la función $f : \mathbb{R} \longrightarrow \mathbb{R}$ que a cada número real x asocia el número real $\frac{1}{\sqrt{x-1}}$, el dominio está formado por los reales mayores que 1 ya que si $x < 1$ la raíz cuadrada no está definida como número real, y si $x = 1$ el denominador sería nulo, lo cual tampoco está definido. Por otro lado el contradominio lo constituyen todos los reales positivos.

Existe una representación gráfica intuitiva que ilustra bien algunos conceptos de la teoría de funciones (igual que en el capítulo de conjuntos y en el de relaciones), aunque no sirve como medio de demostración. En ella se representan por diagramas de Venn los conjuntos inicial y final, enfrentados, y por flechas las parejas que forman la función. El dominio es el subconjunto de puntos del conjunto inicial de los que parte una flecha. El contradominio es el subconjunto de puntos del conjunto final que reciben alguna flecha. La figura 4.2 representa la función del ejemplo anterior.

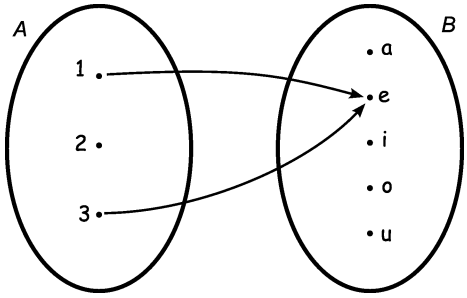


Figura 4.2: Representación gráfica de la función del ejemplo 4.5 del texto.

Merece la pena dedicar unas líneas a comentar cómo se define una función (una en concreto, no el concepto de función). Lo que hay que definir son las parejas de $A \times B$ que la conforman. En la práctica esto se lleva a cabo de dos formas que corresponden a las dos maneras de definir conjuntos (axiomas 2.2 y 2.6): primera, por enumeración de todos los elementos del dominio indicando qué elemento del conjunto final le corresponde a cada uno; segunda, dando una regla o fórmula que permita saber qué elemento corresponde a cada uno.

4.6 Ejemplo. Entre los conjuntos $A = \{0, 1, 2\}$ y $\mathbb{R}$ definamos la función que asocia a cada número su cuadrado. Podemos definirla por enumeración: $f = \{(0, 0), (1, 1), (2, 4)\}$. También podemos escribirla como $f = \{(x, y) \in A \times \mathbb{R} \,|\, y = x^2\}$.

Una vez establecidas las definiciones de partida, introduzcamos los conceptos de imagen y preimagen, que permiten simplificar mucho el discurso de las funciones. Puesto que cada elemento del dominio aparece en una sola pareja de la función, el elemento del conjunto final que le corresponde está determinado sin ambigüedad y se le da un nombre: imagen.

4.7 Definición. *Dada una función $f : A \longrightarrow B$, la* imagen *bajo f de un elemento x del dominio es el único elemento y del contradominio con el que x está relacionado. Se denota $y = f(x)$ o bien $x \longmapsto y$.*

Generalizando el concepto anterior definimos ahora la imagen de un subconjunto, que no es otra cosa que reunir las imágenes de sus elementos.

4.8 Definición. *Dada una función $f : A \longrightarrow B$, la* imagen *bajo f de un subconjunto X del dominio es el subconjunto del contradominio formado por las imágenes de los elementos de X. Se denota $f(X)$. Es decir,*

$$f(X) = \{y \in B \mid \exists x \in X, f(x) = y\}.$$

Análogamente podemos definir la preimagen de un conjunto. Pero, cuidado, no podemos definir la preimagen de un elemento.

4.9 Definición. *Dada una función $f : A \longrightarrow B$, la* preimagen *bajo f de un subconjunto Y de B es el subconjunto del dominio de los elementos cuyas imágenes están en Y. Se denota $f^{-1}(Y)$. Esto es,*

$$f^{-1}(Y) = \{x \in A \mid f(x) \in Y\}.$$

4.10 Ejemplo. Consideremos la función $f : \mathbb{R} \longrightarrow \mathbb{R}$ que relaciona cada número real con su cuadrado. Entonces, por ejemplo, $f(0) = 0$, $f(2) = 4$, $f(-\pi) = \pi^2$. Siguiendo la idea de los ejemplos podemos escribir $\forall x, f(x) = x^2$.

Por otro lado, tenemos $f([0,1]) = [0,1]$, $f([-1,0]) = [0,1]$, $f(\mathbb{R}^-) = \mathbb{R}^+$.

Por último, algunos ejemplos de preimágenes: $f^{-1}(\{0\}) = \{0\}$, $f^{-1}(\{4\}) = \{-2,2\}$, $f^{-1}([0,1]) = [-1,1]$, $f^{-1}([-2,-1]) = \varnothing$.

Con la notación introducida podemos escribir las siguientes relaciones entre dominio y contradominio.

$$f(\mathcal{D}(f)) = \mathcal{D}'(f) \quad \wedge \quad f^{-1}(\mathcal{D}'(f)) = \mathcal{D}(f).$$

Presentamos dos funciones muy sencillas de definir y que sirven como ejemplos muy versátiles: la función constante (definible entre dos conjuntos cualesquiera) y la función identidad (definible entre un conjunto cualquiera y él mismo).

4.11 Definición. *Una función se llama* función constante *si su dominio coincide con el conjunto inicial y su contradominio contiene un único elemento, es decir, $f : A \longrightarrow B$ es constante si*

$$\mathcal{D}(f) = A \wedge \mathcal{D}'(f) = \{y\}$$

para algún elemento de B.

4.12 Definición. *La* función identidad *de un conjunto A, denotada id_A es la función del conjunto A a sí mismo, cuyo dominio es todo el conjunto A y en la que la imagen de cada elemento es él mismo, lo que podemos escribir como $\mathcal{D}(\mathrm{id}_A) = A$ y $f(x) = x$ para todo elemento x de A.*

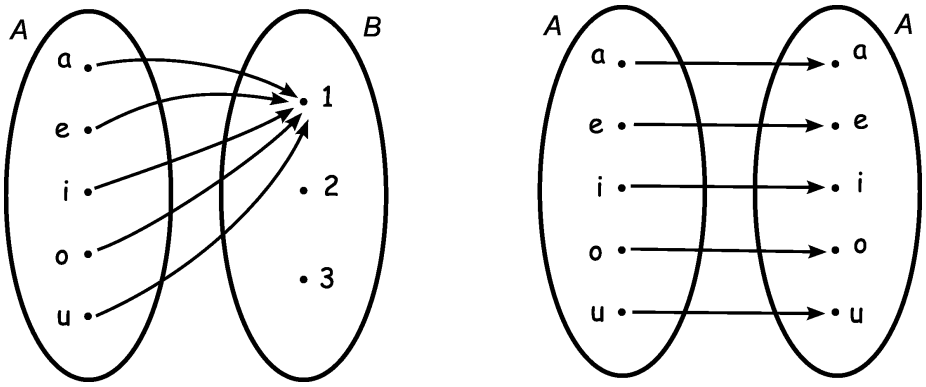


Figura 4.3: Una función constante y una función identidad.

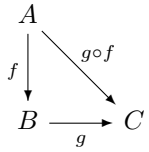
Gráficamente, la función constante y la función identidad tienen el aspecto mostrado en la figura 4.3.

Por último en esta sección vamos a introducir la composición de funciones, que a partir de dos funciones permite construir otra nueva. Si una función lleva los elementos de A a B y otra función, a su vez, lleva los elementos de B a C, entonces la función compuesta es la que lleva los elementos de A a C haciendo el camino a través de B. En la definición hay que tener en cuenta un detalle respecto a los dominios de las funciones, para asegurar que un elemento de A pueda hacer el viaje completo hasta C pasando primero por B.

4.13 Definición. *Dadas las funciones $f : A \longrightarrow B$ y $g : B \longrightarrow C$ donde el contradominio de f está incluido en el dominio de g, la composición de f con g es una función, denotada $g \circ f$, que tiene por conjunto inicial a A, por final a C y asocia a cada elemento de $\mathcal{D}(f) \subset A$ el elemento de $\mathcal{D}'(g) \subset C$ que es la imagen bajo g de su imagen bajo f. Es decir,*

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

Existe una forma de representar la composición de funciones gráficamente mediante los llamados diagramas conmutativos. El diagrama que representa la composición de f y g es el siguiente.



Este diagrama ilustra los dos caminos para ir desde A hasta C; se llama diagrama conmutativo porque ambos caminos tienen el mismo resultado, que es lo que expresa la composición.

4.14 Ejemplo. Sean los conjuntos $A = \{1, 2, 3\}$, $B = \{a, b, c, d\}$, $C = \{X, Y\}$ y las funciones $f : A \longrightarrow B$ y $g : B \longrightarrow C$ dadas por

$$\begin{array}{ll} f(1) = a & g(a) = X, \\ f(2) = b & g(b) = Y, \\ & g(c) = Y. \end{array}$$

Entonces se cumplen las condiciones de la definición, pues $\mathcal{D}'(f) = \{a, b\} \subset \mathcal{D}(g)$, y la función compuesta está definida para los elementos de $\mathcal{D}(f) = \{1, 2\} \subset A$.

$$(g \circ f)(1) = g(f(1)) = g(a) = X,$$
$$(g \circ f)(2) = g(f(2)) = g(b) = Y.$$

La representación gráfica de este ejemplo está en la figura 4.4.

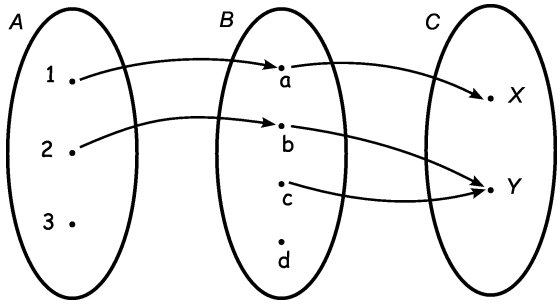


Figura 4.4: Representación gráfica de la composición de funciones del ejemplo 4.14.

4.15 Ejemplo. Sean las funciones $f : \mathbb{R} \longrightarrow \mathbb{R}$ y $g : \mathbb{R} \longrightarrow \mathbb{R}$ dadas por

$$f(x) = x^2 + 1, \quad g(x) = \operatorname{sen}(x).$$

Se cumple $\mathcal{D}'(f) \subset \mathcal{D}(g)$ y por tanto tiene sentido definir la composición $g \circ f$ que resulta

$$(g \circ f)(x) = g(f(x)) = \operatorname{sen}(x^2 + 1).$$

4.2. Función inyectiva, suprayectiva y biyectiva

Dada una función $f : A \longrightarrow B$, ya sabemos cómo es su dominio: un subconjunto del conjunto inicial donde cada elemento tiene una imagen, y sólo una, en B. En esta sección nos ocupamos del contradominio.

Según sea la relación entre el contradominio y el conjunto final tenemos tres tipos de funciones especialmente interesantes: inyectivas, suprayectivas y biyectivas. Estos tipos de funciones son fundamentales pues veremos que toda función se puede escribir como la composición de una función inyectiva, una biyectiva y una suprayectiva.

4.16 Definición. *Una función es inyectiva si su dominio es todo el conjunto inicial y las imágenes de elementos diferentes son diferentes, que lo expresamos como*

$$x \neq y \rightarrow f(x) \neq f(y)$$

para elementos x, y de A.

4.17 Definición. *Una función $f : A \longrightarrow B$ es suprayectiva si el contradominio coincide con el conjunto final:*

$$\mathcal{D}'(f) = B.$$

4.18 Definición. *Una función es biyectiva si es inyectiva y suprayectiva.*

En otras palabras, una función es inyectiva si el dominio es todo el conjunto inicial y cada elemento del conjunto final es imagen de, a lo sumo, un elemento del inicial. Es suprayectiva si todo elemento del conjunto final es imagen de, al menos, un elemento del inicial. Es biyectiva si cada elemento del final es imagen de exactamente un elemento del dominio (que coincide con el inicial).

4.19 Ejemplo. Sean los siguientes conjuntos y funciones con dominio en $A = \{1, 2, 3\}$:

$$\begin{aligned}
f_1 : A \longrightarrow B_1 \quad & \text{donde } B_1 = \{a, b, c, d\} \\
& f_1(1) = b \\
& f_1(2) = c \\
& f_1(3) = a \\
f_2 : A \longrightarrow B_2 \quad & \text{donde } B_2 = \{a, b\} \\
& f_2(1) = a \\
& f_2(2) = a \\
& f_2(3) = b \\
f_3 : A \longrightarrow B_3 \quad & \text{donde } B_3 = \{a, b, c\} \\
& f_3(1) = c \\
& f_3(2) = b \\
& f_3(3) = a \\
f_4 : A \longrightarrow B_4 \quad & \text{donde } B_4 = \{a, b, c, d\} \\
& f_4(1) = b \\
& f_4(2) = b \\
& f_4(3) = a
\end{aligned}$$

Entonces, la función f_1 es inyectiva, pero no es suprayectiva. La función f_2 es suprayectiva, pero no es inyectiva. En tercer lugar, f_3 es biyectiva. Por último, f_4 no es ninguno de los tres tipos. Gráficamente se aprecia en la figura 4.5.

Veamos otro ejemplo, pero ahora con conjuntos mayores.

4.20 Ejemplo. Consideremos las siguientes funciones de $\mathbb{N} = \{1, 2, \dots\}$ a $2\mathbb{N} =$

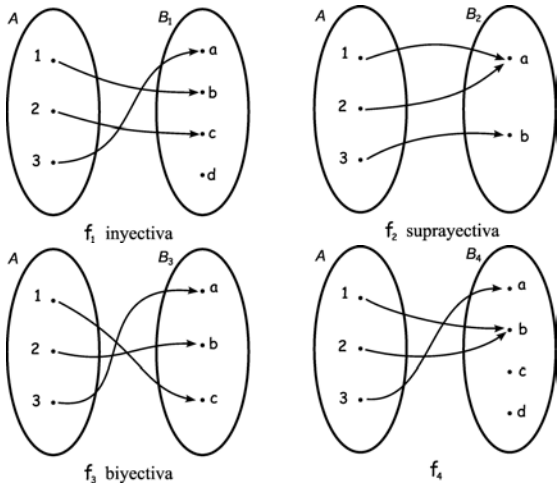


Figura 4.5: Representación gráfica de las funciones del ejemplo 4.19.

$\{2, 4, \dots\}$, en las que el dominio coincide con el conjunto inicial.

$$f_1 : \mathbb{N} \longrightarrow 2\mathbb{N} \quad \text{definida por } f_1(n) = 4n.$$
$$f_2 : \mathbb{N} \longrightarrow 2\mathbb{N} \quad \text{definida por } f_2(n) = \begin{cases} n, & \text{si } n \text{ es par,} \\ n+1, & \text{si } n \text{ es impar.} \end{cases}$$
$$f_3 : \mathbb{N} \longrightarrow 2\mathbb{N} \quad \text{definida por } f_3(n) = 2n.$$
$$f_4 : \mathbb{N} \longrightarrow 2\mathbb{N} \quad \text{definida por } f_4(n) = \begin{cases} n+2, & \text{si } n \text{ es par,} \\ n+1, & \text{si } n \text{ es impar.} \end{cases}$$

Entonces, f_1 es inyectiva, pero no es suprayectiva. Por contra, f_2 no es inyectiva pero sí es suprayectiva. La función f_3 es biyectiva y, finalmente, f_4 no es de ninguno de los tres tipos.

Para finalizar esta sección enunciamos un teorema sobre la composición de funciones inyectivas y suprayectivas

4.21 Teorema. *La composición de funciones inyectivas es inyectiva, la de funciones suprayectivas es suprayectiva, y la de funciones biyectivas es biyectiva.*

Demostración. En el primer caso, el dominio de $g \circ f$ es el de f pero, por ser f inyectiva, éste es todo el conjunto inicial. Por otro lado, dados dos elementos $x, y \in A$, $x \neq y$, sus imágenes bajo f cumplen $f(x) \neq f(y)$, pues f es inyectiva. Igualmente, por ser g inyectiva, $g(f(x)) \neq g(f(y))$, que es lo mismo que escribir $(g \circ f)(x) \neq (g \circ f)(y)$. Por tanto, es inyectiva.

Sean ahora $f : A \longrightarrow B$ y $g : B \longrightarrow C$ dos funciones suprayectivas donde $\mathcal{D}'(f) = B = \mathcal{D}(g)$. Dado un elemento $z \in C$, existe un elemento $y \in B$ tal que $g(y) = z$, debido a que g es suprayectiva. Puesto que f también es suprayectiva, existe $x \in A$ tal que $f(x) = y$. Combinando ambas expresiones, tenemos que existe $x \in A$ tal que $(g \circ f)(x) = z$, luego $g \circ f$ es suprayectiva.

Por último, si f y g son biyectivas, entonces ambas son inyectivas y suprayectivas y por tanto $g \circ f$ también es biyectiva. □

4.3. Función inversa

En esta sección alcanzamos el primer objetivo de este capítulo. Primero definimos función inversa y función invertible, es decir, aquélla que tiene inversa. Después mostramos el teorema que identifica las funciones invertibles con las funciones biyectivas.

Como en el caso de las relaciones, es de esperar que la función inversa esté formada por las parejas de una función con los elementos en orden inverso. El problema es que el conjunto de las parejas con los elementos en orden inverso no es, en general, una función. El siguiente ejemplo muestra el porqué.

4.22 Ejemplo. Sea la función $f : A \longrightarrow B$, donde $A = \{1, 2, 3\}$ y $B = \{a, b, c, d\}$ dada por $f = \{(1, a), (2, a), (3, b)\}$. Entonces, el conjunto de las parejas con los elementos en orden inverso es $\{(a, 1), (a, 2), (b, 3)\}$, que no es una función porque el elemento a aparece en dos parejas, es decir, tendría dos imágenes.

Voltear las parejas, en general, no sirve. Hay que estudiar antes cuándo sí es válido. Para ello, sin embargo, enunciamos la idea de función inversa de otro modo. Queremos una función que deshaga lo que hace la original. Una función que permita volver desde el conjunto final hasta el inicial y dejar las cosas como estaban.

4.23 Definición. *Dada una función $f : A \longrightarrow B$, una función $g : B \longrightarrow A$ es* inversa *de f si la composición de f con g y la composición de g con f son ambas funciones identidad. Es decir, si*

$$g \circ f = \mathrm{id}_A \wedge f \circ g = \mathrm{id}_B.$$

Obsérvese que ambas composiciones son funciones diferentes, pues $g \circ f : A \longrightarrow A$ mientras que $f \circ g : B \longrightarrow B$. Por ello es necesario exigir las dos condiciones. De hecho se pueden distinguir los conceptos de inversa derecha e inversa izquierda (ver ejercicios 4.10 al 4.13). También hay que hacer notar que la definición exige $\mathcal{D}(f) = A$ y $\mathcal{D}(g) = B$, pues de otro modo no se consigue la función identidad en A o la identidad en B.

Veamos ahora un primer resultado importante respecto a la función inversa: su unicidad.

4.24 Teorema. *Si una función tiene inversa, entonces ésta es única.*

Demostración. Dadas $f : A \longrightarrow B$, $g : B \longrightarrow A$ y $h : B \longrightarrow A$ tales que tanto g como h son inversas de f, debemos probar que $g = h$. Consideremos las composiciones $h \circ (f \circ g)$ y $(h \circ f) \circ g$. En el ejercicio 4.4 se pide comprobar que son la misma función: $h \circ (f \circ g) = (h \circ f) \circ g$. Ahora bien, como $f \circ g = \mathrm{id}_B$ y $h \circ f = \mathrm{id}_A$ resulta $h \circ \mathrm{id}_B = \mathrm{id}_A \circ g$, de donde $h = g$ puesto que una función compuesta con la identidad es ella misma (ejercicio 4.5). □

Entonces podemos dar un símbolo a la función inversa. También un nombre a las funciones que tienen inversa.

4.25 Definición. *Si una función f tiene inversa se dice que es* invertible*, y denotamos por f^{-1} la única función que es inversa de f.*

El símbolo f^{-1} es el mismo que se ha usado para la preimagen de un subconjunto del final, pero no hay ambigüedad pues el contexto indica qué acepción usar. Conviene tener claro, en cualquier caso, que f^{-1} como preimagen se puede usar en cualquier función, mientras que como inversa, sólo en las invertibles. Además, si la función es invertible, las dos acepciones del símbolo f^{-1} coinciden en su significado.

Acabamos de ver que si una función tiene inversa, es única y podemos asignarle un nombre. Es el problema de la unicidad. El siguiente paso es el de la existencia, es decir, saber si la función inversa existe. El teorema central de esta sección responde a la pregunta anterior diciendo que las funciones biyectivas son invertibles y son las únicas funciones invertibles.

4.26 Teorema. *Una función es invertible si, y sólo si, es biyectiva.*

Demostración. Empecemos por la implicación directa. Sea $f : A \longrightarrow B$ una función invertible. Entonces existe $f^{-1} : B \longrightarrow A$ de modo que $f \circ f^{-1} = \mathrm{id}_B$ y $f^{-1} \circ f = \mathrm{id}_A$. También sabemos que $\mathcal{D}(f) = A$ y $\mathcal{D}(f^{-1}) = B$.

Veamos que f es inyectiva usando la contrapositiva de la definición 4.16. Sean x, y dos elementos de A que cumplen $f(x) = f(y)$. Debemos mostrar que estos elementos son iguales. Para ello actuamos con la función inversa, con lo cual $f^{-1}(f(x)) = f^{-1}(f(y))$, pero por definición de inversa $f^{-1}(f(x)) = x$ y $f^{-1}(f(y)) = y$, de donde $x = y$ y f es inyectiva.

Ahora veamos que f es suprayectiva. Sea $y \in B$, entonces $f^{-1}(y)$ es un elemento de A y cumple que su imagen es $f(f^{-1}(y)) = y$. Por tanto todo elemento de B es imagen de alguno de A.

En segundo lugar hay que probar la otra implicación. Sea, pues, $f : A \longrightarrow B$ una función biyectiva. Por definición de biyectividad, dado un elemento cualquiera de B existe un, y sólo un, elemento de A cuya imagen es el elemento dado de B. Demostramos que tal función es invertible construyendo explícitamente la función inversa: $f^{-1} : B \longrightarrow A$ es la función que a cada elemento de B asocia el único elemento de A cuya imagen por f es dicho elemento de B. Por su construcción es una función y es una inversa de f, por lo tanto es la inversa de f y f es invertible. □

Como consecuencia inmediata de este resultado podemos observar que si una función es biyectiva, y por tanto invertible, entonces su inversa también es biyectiva.

4.27 Ejemplo. La función $f : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $f(x) = x^2$ no es inyectiva, pues hay elementos diferentes con la misma imagen, por ejemplo $f(2) = f(-2) = 4$. Tampoco es suprayectiva, pues su contradominio no contiene a los reales negativos. Por tanto, no es biyectiva y no es invertible. Ésta es la causa de

que al intentar utilizar como supuesta función inversa la raíz cuadrada nos encontramos con la disyuntiva de que hay dos posibles respuestas: $\sqrt{4} = \pm 2$.

Sin embargo $g : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $g(x) = x^3$ sí es biyectiva y, por tanto, sí admite inversa que es $g^{-1}(x) = x^{1/3}$.

Ahora recordamos que la composición de funciones biyectivas también es biyectiva y, por tanto, invertible. ¿Es posible expresar la inversa de una composición a partir de las inversas de cada función que se compone? La respuesta es el último teorema de esta sección.

4.28 Teorema. *La composición de funciones invertibles es invertible y su inversa es la composición de las inversas en orden opuesto.*

Esto es, si $f : A \longrightarrow B$ y $g : B \longrightarrow C$ son invertibles, entonces $g \circ f$ es invertible y

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Demostración. Sean $f : A \longrightarrow B$ y $g : B \longrightarrow C$ invertibles. Por ser invertibles $\mathcal{D}'(f) = B = \mathcal{D}(g)$, la composición $g \circ f$ está bien definida y es invertible (por ser composición de funciones biyectivas).

Ahora probemos que $f^{-1} \circ g^{-1}$ es, efectivamente, la inversa de $g \circ f$. Sea $x \in A$ al que aplicamos la composición $(f^{-1} \circ g^{-1}) \circ (g \circ f)$. La aplicación de la definición de inversa nos lleva directamente a $(f^{-1} \circ g^{-1}) \circ (g \circ f)(x) = x$, luego es la identidad en A. Del mismo modo se ve que la composición en el otro orden es la identidad en B. Por tanto, $f^{-1} \circ g^{-1}$ es la inversa de $g \circ f$. □

4.4. Descomposición canónica de una función

En esta última sección vamos a ver otro resultado de la teoría de funciones, donde se aprecia aún más el papel destacado de las funciones inyectivas, las suprayectivas y las biyectivas.

4.4.1. El prototipo de función biyectiva

La función identidad de un conjunto es una función biyectiva (ver ejercicio 4.17). Su inversa es ella misma.

En teoría de conjuntos se dice que dos conjuntos son equivalentes, o coordinables, si existe una función biyectiva entre ellos. En este caso, todas las propiedades como conjunto que tenga uno de ellos también las tiene el otro, y viceversa. La función biyectiva que los relaciona se puede ver como un cambio de nombre de los elementos de un conjunto por los del otro, de modo que se ven iguales.

4.29 Ejemplo. Los conjuntos $A = \{1, 2, 3, 4\}$ y $B = \{a, b, c, d\}$ son coordinables pues existe una función biyectiva entre ellos, por ejemplo $1 \longmapsto a$, $2 \longmapsto b$, $3 \longmapsto c$, $4 \longmapsto d$. Se puede interpretar esta función como un cambio de nombre de los elementos de A y, entonces, identificar A con B.

Sin embargo A no es coordinable con $C = \{x, y, z\}$ pues no existe ninguna función biyectiva entre ellos (hay 81 funciones de la forma $A \longrightarrow C$ y 64 funciones $C \longrightarrow A$, pero ninguna biyectiva). Entonces A y C tienen propiedades diferentes, por ejemplo, A puede separarse en dos subconjuntos disjuntos coordinables entre sí, pero C no puede.

Si identificamos dos conjuntos coordinables a través de una función biyectiva, entonces dicha función biyectiva aparece como una función identidad. Por ello, sin que sea una definición ni un resultado, consideramos la función identidad como el prototipo de función biyectiva.

4.4.2. El prototipo de función inyectiva

Como prototipo de función inyectiva proponemos la función inclusión, que definimos a continuación.

4.30 Definición. *Sea A un subconjunto de B. La función inclusión de A en B, denotada $i : A \hookrightarrow B$ es la que asigna a cada elemento de A el mismo elemento en B.*

Simbólicamente, si $A \subset B$,

$$\begin{array}{rccc} i: & A & \hookrightarrow & B \\ & x & \longmapsto & x. \end{array}$$

Obśervese que esta función no es la función identidad porque los conjuntos inicial y final no coinciden. Es claro que esta función es inyectiva (ejercicio 4.17).

Ahora veamos que cualquier función inyectiva tiene el aspecto de una función inclusión.

4.31 Teorema. *Si $f : A \longrightarrow B$ es una función inyectiva, entonces existe una función biyectiva $\tilde{f} : A \longrightarrow \mathcal{D}'(f)$ tal que, junto con la función inclusión $i : \mathcal{D}'(f) \hookrightarrow B$ cumple*

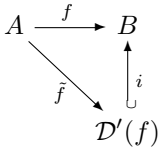
$$f = i \circ \tilde{f}.$$

Demostración. Sea $f : A \longrightarrow B$ una función inyectiva. Por definición se cumple $\mathcal{D}(f) = A$, pero no sabemos nada sobre el contradominio de f. La idea es restringir el conjunto final para hacerla suprayectiva sin perder la inyectividad. Definimos pues una nueva función del conjunto A al conjunto $\mathcal{D}'(f)$, que llamaremos $\tilde{f}$, del siguiente modo

$$\begin{array}{rccc} \tilde{f}: & A & \longrightarrow & \mathcal{D}'(f) \\ & x & \longmapsto & f(x). \end{array}$$

Es decir, la función $\tilde{f}$ asocia a cada elemento de A el mismo que f, y la única diferencia es el conjunto final. Ahora, $\tilde{f}$ es suprayectiva y mantiene la propiedad de inyectividad de f, luego tenemos que $\tilde{f}$ es biyectiva. Por último sólo resta comprobar que la función f que teníamos es la misma que $\tilde{f}$ compuesta con la función inclusión $i : \mathcal{D}'(f) \hookrightarrow B$. Efectivamente, es claro que la composición es una función de la forma $i \circ \tilde{f} : A \longrightarrow B$ y, además, si $x \in A$, $(i \circ \tilde{f})(x) = i(\tilde{f}(x)) = f(x)$. □

Usando un diagrama conmutativo podemos enunciar este teorema diciendo que existe una función $\tilde{f}$ biyectiva tal que el siguiente diagrama commuta.



Este resultado se puede interpretar de este modo: puesto que $\tilde{f}$ es biyectiva, es decir, análoga a una función identidad, la propiedad de inyectividad de f recae totalmente en la función inclusión i. De ahí la lectura de que la función inclusión es el prototipo de función inyectiva.

También podemos hacer la siguente asociación: puesto que todo subconjunto lleva asociada una función inclusión, la cual es inyectiva, y toda función inyectiva es, en el fondo, una función inclusión, los conceptos de subconjunto y de función inyectiva resultan indisolublemente ligados. Si $f : A \longrightarrow B$ es inyectiva decimos que f inyecta A en B y, abusando un poco del lenguaje, podemos considerar que A es subconjunto de B (formalmente, identificamos A con $f(A)$ el cual sí es subconjunto de B).

4.4.3. El prototipo de función suprayectiva

El prototipo de función suprayactiva se define entre un conjunto en el que se ha establecido una relación de equivalencia y su conjunto cociente. Se denomina proyección canónica y es la que asocia a cada elemento la clase de equivalencia a la que pertenece.

4.32 Definición. *Sea A un conjunto en el que se ha definido una equivalencia R. Llamamos proyección canónica de A sobre el conjunto cociente A/R, denotada $p : A \longrightarrow\!\!\!\!\!\rightarrow A/R$, a la función*

$$\begin{array}{rccc} p: & A & \longrightarrow\!\!\!\!\!\rightarrow & A/R \\ & x & \longmapsto & [x]. \end{array}$$

Es un ejercicio sencillo probar que esta función es suprayectiva (ejercicio 4.17).

Como en el caso anterior, vamos a argumentar que toda función suprayectiva se puede ver como la proyección canónica de una equivalencia.

4.33 Teorema. *Si $f : A \longrightarrow B$ es una función suprayectiva con $\mathcal{D}(f) = A$, la relación R definida por $x \sim y$ si $f(x) = f(y)$ es una equivalencia en A y existe una función biyectiva $\tilde{f} : A/R \longrightarrow B$ tal que, junto con la proyección canónica $p : A \longrightarrow\!\!\!\!\!\rightarrow A/R$, cumple*

$$f = \tilde{f} \circ p.$$

Demostración. Sea $f : A \longrightarrow B$ una función suprayectiva que verifica $\mathcal{D}(f) = A$. Que la relación R definida en el teorema es una equivalencia se pide en el ejercicio 4.18.

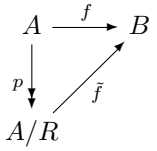
El conjunto cociente A/R está formado por las clases de equivalencia y cada una de ellas está formada por elementos que tienen la misma imagen. Esto nos permite definir una nueva función, que llamaremos $\tilde{f} : A/R \longrightarrow B$, que asocia a cada clase de equivalencia la imagen de alguno de sus elementos.

$$\begin{array}{rccc} \tilde{f}: & A/R & \longrightarrow & B \\ & [x] & \longmapsto & f(x). \end{array}$$

Esta definición tiene un detalle delicado y es que para asignar la imagen a la clase de equivalencia $[x]$ usamos el elemento x, el cual no es más que un representante de esta clase. Parece, pues, que la definición depende del representante que elijamos en cada clase. Sin embargo no es un problema porque todos los elementos de la clase $[x]$ tienen la misma imagen que x. Veamos que $\tilde{f}$ es biyectiva. Sean $[x]$, $[y]$ dos clases de equivalencia tales que $\tilde{f}([x]) = \tilde{f}([y])$; entonces $f(x) = f(y)$ y, por tanto $x \sim y$, en cuyo caso $[x] = [y]$. Por tanto $\tilde{f}$ es inyectiva. Ahora tomemos un elemento b de B. Puesto que la función original f es suprayectiva, existe $x \in A$ tal que $f(x) = b$, y su clase de equivalencia cumple $\tilde{f}([x]) = b$, de donde $\tilde{f}$ es suprayectiva.

Por último consideremos la composición de $p : A \longrightarrow\!\!\!\!\!\rightarrow A/R$, la proyección canónica, y $\tilde{f} : A/R \longrightarrow B$. Es una función de la forma $\tilde{f} \circ p : A \longrightarrow B$ y, si x es elemento de A, verifica $(\tilde{f} \circ p)(x) = f(x)$, luego ambas funciones son la misma. □

En forma de diagrama podemos enunciar el resultado diciendo que existe una función biyectiva $\tilde{f}$ tal que el siguiente diagrama es conmutativo.



En el mismo espíritu de antes, puesto que $\tilde{f}$ es biyectiva, la propiedad de suprayectividad de f puede verse completamente recogida en la proyección canónica p, de ahí que interpretemos dicha función como el prototipo de función suprayectiva.

También de modo análogo a la identificación que se hizo arriba entre subconjuntos y funciones inyectivas, nos vemos obligados ahora a ligar indisolublemente los conceptos de relación de equivalencia y función suprayectiva.

4.4.4. Descomposición canónica

Reuniendo los dos resultados anteriores podemos dar una descomposición de cualquier función en una proyección canónica, una función biyectiva y una inclusión. Se denomina descomposición canónica.

4.34 Teorema. *Dada una función $f : A \longrightarrow B$ con $\mathcal{D}(f) = A$, la relación R definida por $x \sim y$ si $f(x) = f(y)$ es una equivalencia en A y existe una función*

biyectiva $\tilde{f} : A/R \longrightarrow \mathcal{D}'(f)$ *tal que*

$$f = i \circ \tilde{f} \circ p,$$

donde i *es la función inclusión* $i : \mathcal{D}'(f) \hookrightarrow B$ *y* p *es la proyección canónica* $p : A \twoheadrightarrow A/R$.

Demostración. Definimos una función auxiliar $g : A \longrightarrow \mathcal{D}'(f) : x \longmapsto f(x)$. Por su construcción es claro que tenemos la identidad $f = i \circ g$, donde i es la función inclusión del enunciado del teorema. Igualmente por su construcción g es suprayectiva y verifica $\mathcal{D}(g) = A$, por tanto se puede aplicar el teorema 4.33 que dice que existe $\tilde{f} : A/R \longrightarrow \mathcal{D}'(f)$ biyectiva tal que $g = \tilde{f} \circ p$, con p la proyección canónica. Uniendo ambos resultados tenemos $f = i \circ \tilde{f} \circ p$. □

El teorema también se puede enunciar diciendo que existe una función biyectiva $\tilde{f}$ tal que el siguiente diagrama es conmutativo.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ A/R & \xrightarrow{\tilde{f}} & \mathcal{D}'(f) \end{array}$$

4.35 Ejemplo. Realicemos la descomposición canónica de la función $f : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $f(x) = x^2$, de la cual ya hemos dicho que no es ni inyectiva ni suprayectiva. Buscamos, pues, el contradominio de f, la relación de equivalencia R y la función biyectiva $\tilde{f}$ que el teorema anterior nos describe.

La equivalencia R relaciona dos números reales x_1 y x_2 si $f(x_1) = f(x_2)$, es decir $x_1^2 = x_2^2$; por tanto tenemos $x_1 = \pm x_2$. Por ejemplo 2 está relacionado con sí mismo y con -2 pues cumplen $f(2) = f(-2)$. Las clases de equivalencia son, pues, de la forma $\{2, -2\}, \{\frac{4}{3}, \frac{-4}{3}\}, \{\pi, -\pi\}, \ldots$ El conjunto cociente está formado por parejas de números opuestos $\mathbb{R}/R = \{\{x, -x\} : x \in [0, \infty)\}$ y la función de proyección canónica $p : \mathbb{R} \longrightarrow\!\!\!\!\!\rightarrow \mathbb{R}/R$ lleva cada número real x a la pareja $\{x, -x\}$.

Puesto que todo número real al cuadrado es positivo o cero y que todo real positivo tiene raíz cuadrada, el contradominio de f es $\mathcal{D}'(f) = [0, \infty)$. Entonces la función $\tilde{f} : \mathbb{R}/R \longrightarrow\!\!\!\!\!\rightarrow \mathcal{D}'(f)$ del teorema es la que asocia cada clase de equivalencia $\{x, -x\}$ con el número x^2, que es la imagen de cualquiera de los dos elementos de la clase. Esta función es biyectiva.

Finalmente la función inclusión $i : [0, \infty) \hookrightarrow \mathbb{R}$ lleva cada número real positivo o cero a él mismo dentro de la recta real completa.

Reuniéndolo todo tenemos que la acción de f la podemos descomponer como, primero, la proyección de cada número real x a su clase $\{x, -x\}$, que es suprayectiva; segundo, la biyección de cada clase $\{x, -x\}$ al número x^2 y, tercero, la inclusión de este número en la recta real, que es inyectiva.

Ejercicios

4.1. Para cada una de las siguientes parejas de conjuntos A y B, escribir explícitamente todas las funciones posibles de la forma $A \longrightarrow B$, donde el dominio debe coincidir con el conjunto inicial A, e indicar, justificadamente, cuáles de ellas son inyectivas, cuáles suprayectivas, y cuáles biyectivas. En los casos de funciones biyectivas, además, escribir la función inversa.

a) $A_1 = \{1, 2, 3\}$, $B_1 = \{a\}$

b) $A_1 = \{1, 2, 3\}$, $B_1 = \{a, b\}$

c) $A_1 = \{1, 2\}$, $B_1 = \{a, b, c, d\}$

d) $A_1 = \{1, 2, 3\}$, $B_1 = \{a, b, c\}$

4.2. Sea P el conjunto de todos los polígonos, y consideremos la función $f : P \longrightarrow \mathbb{N}$ que asocia a cada polígono su número de lados.

a) Estudiar si la función es inyectiva, si es suprayectiva y si es biyectiva.

b) Hallar las imágenes de los siguientes subconjuntos de P: T, el subconjunto de los triángulos; R el subconjunto de los polígonos regulares; Q, el subconjunto de los polígonos cuyos lados son paralelos dos a dos.

c) Hallar las siguientes imágenes inversas: $f^{-1}(\{3\})$, $f^{-1}(\{2\})$, $f^{-1}(\{3, 4, 5\})$, $f^{-1}(\{2, 3\})$.

4.3. En cada inciso razonar si la función correspondiente es inyectiva, si es suprayectiva y si es biyectiva.

a) $f : \mathbb{Z} \longrightarrow \mathbb{Z} : m \longmapsto m + 1$.

b) $f : \mathbb{N} \longrightarrow \mathbb{N} : m \longmapsto m + 1$.

c) $f : [0, 1] \longrightarrow [0, 1] : x \longmapsto \frac{1}{2}x$, donde $[0, 1] \subset \mathbb{R}$ es el intervalo unitario cerrado de la recta real.

d) $f : \mathbb{R} \longrightarrow \mathbb{R} : x \longmapsto x^2$.

e) $f : \mathbb{N} \longrightarrow \mathbb{N} : n \longmapsto n^2$.

f) $f : \mathbb{N} \longrightarrow P \cup \{1\}$, donde P es el conjunto de los números primos, que a cada natural asocia el menor primo que aparece en su factorización en primos, y al 1 asocia el 1.

g) $f : \mathbb{R} \longrightarrow \mathbb{Z} : x \longmapsto \lfloor x \rfloor$, donde $\lfloor x \rfloor$ es el piso de x, es decir, el mayor entero menor o igual a x.

h) $f : \mathbb{C} \longrightarrow \mathbb{R} : a + bi \longmapsto a + b$.

i) $f : \mathbb{C} \longrightarrow \mathbb{C} : z \longmapsto \overline{z}$, donde $\overline{z}$ es el conjugado de z.

4.4. Probar que la composición de funciones es asociativa. Es decir, dadas las funciones $f : A \longrightarrow B, g : B \longrightarrow C$ y $h : C \longrightarrow D$ que cumplen $\mathcal{D}'(f) \subset \mathcal{D}(g)$ y $\mathcal{D}'(g) \subset \mathcal{D}(h)$, entonces

$$(h \circ g) \circ f = h \circ (g \circ f).$$

4.5. Probar que la composición de una función con la función identidad tanto por la derecha como por la izquierda (en cada caso con la función identidad adecuada) es la misma función.

4.6. En cada inciso argumentar si las funciones f y g son inyectivas, si son suprayectivas y si son biyectivas. Además calcular la función $g \circ f$ indicando los conjuntos inicial y final y la imagen de un elemento arbitrario y señalar igualmente si es inyectiva y si es suprayectiva. Dibujar un diagrama conmutativo de cada composición.

a) $\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & \mathbb{Z} \\ & n & \longmapsto & -n \end{array} \qquad \begin{array}{rccc} g: & \mathbb{Z} & \longrightarrow & \mathbb{Q} \\ & m & \longmapsto & \frac{1}{3}m \end{array}$

b) $\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & \mathbb{Z} \\ & n & \longmapsto & n-5 \end{array} \qquad \begin{array}{rccc} g: & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & m & \longmapsto & m^2 \end{array}$

c) $\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & |n|+1 \end{array} \qquad \begin{array}{rccc} g: & \mathbb{N} & \longrightarrow & \mathbb{Z} \\ & m & \longmapsto & m-1 \end{array}$

donde $|n|$ denota el valor absoluto de n.

d) $\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & \lfloor x \rfloor \end{array} \qquad \begin{array}{rccc} g: & \mathbb{Z} & \longrightarrow & \{0,1\} \\ & m & \longmapsto & \begin{cases} 0, & \text{si } m \text{ es par,} \\ 1, & \text{si } m \text{ es impar,} \end{cases} \end{array}$

donde $\lfloor x \rfloor$ es la función piso de x.

e) $\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{C} \\ & x & \longmapsto & ix \end{array} \qquad \begin{array}{rccc} g: & \mathbb{C} & \longrightarrow & \mathbb{C} \\ & z & \longmapsto & \overline{z} \end{array}$

donde $\overline{z}$ es el conjugado de z.

* 4.7. Dada una función $f : A \longrightarrow B$ y los subconjuntos del dominio X_1, X_2, probar las siguientes relaciones.

a) $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$.

b) $f(X_1 \cap X_2) \subset f(X_1) \cap f(X_2)$, pero en general $f(X_1 \cap X_2) \neq f(X_1) \cap f(X_2)$.

c) $f(X_1 \backslash X_2) \supset f(X_1) \backslash f(X_2)$, pero en general $f(X_1 \backslash X_2) \neq f(X_1) \backslash f(X_2)$.

Esto indica que las imágenes no se comportan bien respecto a las operaciones de conjuntos. Sin embargo las preimágenes sí tienen un comportamiento óptimo. Si ahora Y_1, Y_2 son subconjuntos de B, probar las siguientes igualdades.

d) $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$.

e) $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$.

f) $f^{-1}(Y_1 \setminus Y_2) = f^{-1}(Y_1) \setminus f^{-1}(Y_2)$.

4.8. Funciones monónotas. Sean A y B conjuntos totalmente ordenados. Una función $f : A \longrightarrow B$ se llama monónota si cumple $\forall x, y \in A$

$$x < y \rightarrow f(x) < f(y).$$

Dicho con otras palabras, la función f preserva el orden. Probar que una función monótona es inyectiva. (Esta es una forma rápida de comprobar la inyectividad de algunas funciones.)

4.9. Sean A un conjunto totalmente ordenado con la propiedad del inmediato sucesor y B un conjunto con un orden total lineal.

a) Si $f : A \longrightarrow B$ es una función monótona, pruébese que $\mathcal{D}'(f)$ es un subconjunto de B con la propiedad del inmediato sucesor.

b) ¿Existe una función monótona de la forma $B \longrightarrow A$?

4.10. Se llama función inversa por la derecha de una función dada $f : A \longrightarrow B$ a una función $g : B \longrightarrow A$ que verifica $f \circ g = \mathrm{id}_B$. El problema de la función inversa derecha es que no es única.

Consideremos la función $f : A \longrightarrow B$, donde $A = \{1, 2, 3, 4\}$ y $B = \{a, b, c\}$, dada por $f(1) = f(2) = a$, $f(3) = b$ y $f(4) = c$. Hállense dos funciones diferentes que sean inversas derechas de f.

4.11. Se llama función inversa por la izquierda de una función dada $f : A \longrightarrow B$ a una función $g : B \longrightarrow A$ que verifica $g \circ f = \mathrm{id}_A$. Como en el caso de la inversa derecha, el problema es que una función inversa izquierda no es única.

Consideremos la función $f : A \longrightarrow B$, donde $A = \{1, 2, 3\}$ y $B = \{a, b, c, d\}$, dada por $f(1) = a$, $f(2) = b$ y $f(3) = c$. Hállense dos funciones diferentes que sean inversas izquierdas de f.

* 4.12. Recogiendo los resultados de los dos ejercicios precedentes como observaciones, parece intuitivo que una función tiene inversa izquierda si, y sólo si, es inyectiva, mientras que tiene inversa derecha si, y sólo si, es suprayectiva. Pruébese este resultado.

* 4.13. Por último, el resultado definitivo para tratar con inversas izquierdas y derechas. Pruébese el siguiente teorema: Si una función tiene inversa izquierda e inversa derecha, entonces ambas son la misma función, que es inversa de la función dada y, por tanto, es única.

4.14. Dados dos conjuntos A_1 y A_2, consideramos su producto cartesiano $A_1 \times A_2$ y definimos las funciones de proyección:

$$\begin{array}{rccc} \pi_1 : & A_1 \times A_2 & \longrightarrow & A_1 \\ & (a_1, a_2) & \longmapsto & a_1 \end{array} \qquad \begin{array}{rccc} \pi_2 : & A_1 \times A_2 & \longrightarrow & A_2 \\ & (a_1, a_2) & \longmapsto & a_2 \end{array}$$

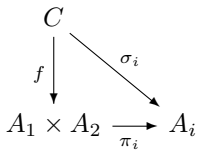
a) Probar que ambas funciones son suprayectivas.

b) Si a_2 es un elemento de A_2, probar que el conjunto $\pi_1^{-1}(\{a_2\})$ es equivalente a A_1 (es decir, que existe una función biyectiva entre ambos).

c) Análogamente, si $a_1 \in A_1$, el conjunto $\pi_2^{-1}(\{a_1\})$ es equivalente a A_2.

Si consideramos el conjunto $\mathbb{R} \times \mathbb{R}$, representado por el plano cartesiano, representar el punto $(\sqrt{3}, 5)$, sus imágenes $\pi_1(\sqrt{3}, 5)$ y $\pi_2(\sqrt{3}, 5)$ y los conjuntos $\pi_1^{-1}(\{\sqrt{3}\})$ y $\pi_2^{-1}(\{5\})$.

* 4.15. Consideremos de nuevo el producto cartesiano $A_1 \times A_2$ y las funciones de proyección π_1 y π_2 definidas en el ejercicio anterior. Sea C un conjunto cualquiera acompañado de dos funciones $\sigma_1 : C \longrightarrow A_1$ y $\sigma_2 : C \longrightarrow A_2$. Probar que existe una única función $f : C \longrightarrow A_1 \times A_2$ tal que $\sigma_i = \pi_i \circ f$ para $i = 1, 2$. Dicho de otro modo, tal que, para cada $i = 1, 2$, el siguiente diagrama conmuta.



* 4.16. Consideramos el producto cartesiano por tercera ocasión, esta vez para dar una caracterización en base a las funciones de proyección. Sea un conjunto D junto con dos funciones $\rho_1 : D \longrightarrow A_1$ y $\rho_2 : D \longrightarrow A_2$ que cumple que, dado cualquier conjunto C acompañado de dos funciones $\sigma_1 : C \longrightarrow A_1$ y $\sigma_2 : C \longrightarrow A_2$, existe una única función $f : C \longrightarrow D$ tal que $\sigma_i = \rho_i \circ f$ para $i = 1, 2$. Probar que, en tal caso, el conjunto D es equivalente a $A_1 \times A_2$, es decir, que existe una función biyectiva entre ellos.

En conclusión, el ejercicio anterior muestra que el producto cartesiano cumple esta propiedad, mientras que este ejercicio muestra que, en esencia, es el único conjunto que la cumple.

4.17. Probar que los prototipos de funciones mencionados en el texto son, efectivamente, del tipo adecuado:

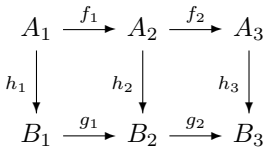
a) La función identidad es biyectiva.

b) La función inclusión es inyectiva.

c) La proyección canónica sobre el conjunto cociente es suprayectiva.

4.18. Sea $f : A \longrightarrow B$ una función con $\mathcal{D}(f) = A$. Definimos la relación R en A mediante $x \sim y \Leftrightarrow f(x) = f(y)$. Probar que es una equivalencia en A y describir las clases de equivalencia. Obsérvese que es imprescindible la condición sobre el dominio de la función.

* 4.19. Consideremos el siguiente diagrama, en el que todas las funciones tienen su dominio igual a su conjunto inicial.



El diagrama es conmutativo si cualquier par de caminos que inicien en un mismo punto y terminen también en un mismo punto dan resultados iguales. Supongamos que el diagrama es conmutativo: escribir todas las relaciones entre las funciones f_i, las funciones g_i y las funciones h_i que de ello se derivan. Comprobar que sólo hay dos relaciones independientes (es decir, que cualquier otra se puede obtener a partir de esas dos).

Lista de símbolos

Bibliografía

[1] Mosterín J., *Teoría axiomática de conjuntos*, Ariel, Segunda edición 1980.

Este libro es una exposición completa de la teoría de conjuntos con un riguroso esquema de axiomas, definiciones y teoremas, estos últimos seguidos sin excepción por su demostración. La exposición de resultados y pruebas se realiza en el más puro lenguaje lógico, sólo con símbolos lógicos y con apenas algunos textos explicativos al comienzo de cada capítulo. No es un libro de texto, sino de referencia. Su lectura puede parecer difícil en un primer contacto, pero una vez acostumbrado al lenguaje lógico formal, el lector puede seguir con facilidad todos los enunciados y disfrutar de la quintaesencia del rigor lógico y matemático.

[2] Suppes P., *Axiomatic Set Theory*, Dover, 1972.

Es un texto más ameno que el anterior sobre el desarrollo axiomático de la teoría de conjuntos, abundando en la necesidad de cada nuevo teorema para justificar su introducción.

[3] Lipschutz S., *Teoría de conjuntos y temas afines*, McGraw-Hill (Serie Schaumm), 1996.

Como todos los libros de la serie Schaumm de esta editorial, es un texto muy práctico con la teoría reducida al mínimo (pero bien expuesta) y una ingente cantidad de ejercicios resueltos y otros propuestos.

[4] Fraenkel A., *Teoría de los conjuntos y lógica*, Universidad Nacional Autónoma de México, 1976.

Un texto de uno de los creadores del sistema axiomático actual de la teoría de conjuntos, publicado originalmente en 1959 como *Mengenlehere und logik*. Es un libro fácil de leer que describe el desarrollo de la teoría de conjuntos, los obstáculos que se han ido encontrando históricamente y cómo se solucionaron.

[5] Halmos P., *Naive Set Theory*, D. Van Nostrand Company, Inc., 1960.

Como el título indica, es un libro que expone las ideas de forma intuitiva. Sin embargo, no por ello deja de ser riguroso. Dedica un buen espacio a describir algunos de los axiomas de la teoría, explicando porqué su necesidad y su utilidad.

[6] Kamke E., *Theory of sets*, Dover Publications, 1950.

Comentamos este libro como ejemplo de un texto que no utiliza el desarrollo axiomático y presenta la teoría de conjuntos prácticamente en la forma en que lo hizo Cantor. Sus resultados son correctos pero los argumentos son débiles en muchos puntos por utilizar conceptos no definidos o mal definidos y carecer de una base firme desde la que empezar la deducción como es la de una familia de axiomas.

[7] Jech T., *Set Theory*, Springer-Verlag, 2nd. edition, 2002,

Es la segunda edición, que es la primera con una corrección de erratas, de un libro muy extenso sobre teoría de conjuntos. En él se puede encontrar todo acerca de la teoría de conjuntos, incluidos temas de investigación actual. Pero su nivel es elevado, sólo accesible a lectores que ya conozcan las bases de la teoría.

[8] Landau L., *Foundations of Analysis*, Chelsea Publishing Company, tercera edición 1966.

[9] Landau L., *Differential and Integral Calculus*, Chelsea Publishing Company, tercera edición 1980.

Estos dos libros de Landau son ejemplos de cómo es una teoría matemática desnuda de cualquier contenido superfluo (por ejemplo, explicaciones aclarativas para el lector). Efectivamente, se reducen a una colección de axiomas y de teoremas, uno tras otro, cada teorema seguido por su prueba rigurosa. El libro de fundamentos del análisis parte de los axiomas de Peano sobre los números naturales para, sobre ellos, construir toda la aritmética de estos números, luego construir los enteros, racionales, reales y complejos, cada uno con sus operaciones de suma y producto y su relación de orden. El libro de cálculo expone prácticamente todos los resultados del cálculo real de una variable.

Índice alfabético