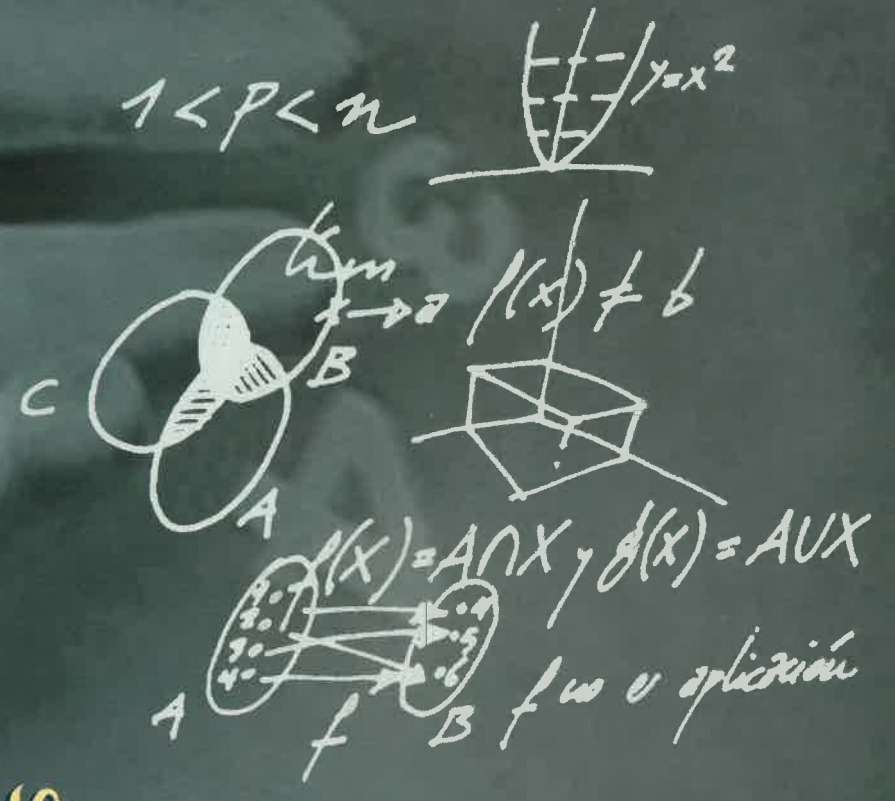
INTRODUCCIÓN AL MÉTODO MATEMÁTICO

F. Javier Pérez Fernández



Servicio de Publicaciones
Universidad de Cádiz

INTRODUCCIÓN AL MÉTODO MATEMÁTICO

F. Javier Pérez Fernández

UNIVERSIDAD DE CÁDIZ.

SERVICIO DE PUBLICACIONES.

1998

PÉREZ FERNÁNDEZ, F. Javier

Introducción al método matemático / F. Javier Pérez Fernández. -- Cádiz : Universidad, Servicio de Publicaciones, 1998. -- 218 p.

ISBN 84-7786-509-4

1. Lógica simbólica y matemática. I. Universidad de Cádiz. Servicio de Publicaciones. II. Título

510.6

Diseño y maquetación: CREASUR

Printed in Spain. Impreso en España

I.S.B.N.: 84-7786-509-4
Depósito Legal: S. 696-1998

Imprime:
Gráficas VARONA
Polígono "El Montalvo", parcela 49
37008-SALAMANCA

A mis padres

Prólogo

Habitualmente los estudiantes de Bachillerato identifican las matemáticas con la resolución de ecuaciones o de problemas cuya solución queda determinada a partir de la aplicación inmediata de algún algoritmo o regla. Así, entre otros, son ejercicios habituales: determinar la función derivada de una función dada, calcular el área bajo una curva, operar con matrices, determinar intersecciones de planos o rectas, o determinar valores que optimizan una determinada función.

Sin duda, cuestiones como las anteriores proporcionan un cierto bagaje matemático, de crucial importancia, pero no deja de ser una aproximación muy tangencial al mundo de las matemáticas como disciplina científica.

El alumno de Bachillerato, por lo general, ha tenido pocas oportunidades de aproximarse a problemas para los que no disponía previamente de un catálogo claro de técnicas a utilizar, ni al desarrollo y estudio de demostraciones de proposiciones matemáticas.

Desde el primer día de inicio de los estudios universitarios la situación va a ser bien distinta. Por una parte, las cuestiones a tratar contendrán no sólo números, sino también conjuntos abstractos y otros muchos objetos matemáticos con los que el alumno no tiene una familiaridad previa. Por otra parte, *el razonamiento deductivo* será imprescindible para encontrar respuesta a los diversos problemas con los que el alumno habrá de enfrentarse en su formación matemática.

El quehacer matemático requiere de la creatividad y de la deducción lógica. La primera resulta imprescindible para intuir caminos que nos lleven a las respuestas de los problemas que se nos plantean, y también para sondear con inagotable curiosidad nuevos campos a desbrozar del mundo matemático. La segunda, nos asegura que el camino emprendido es sólido y bien cimentado y la solución final cierta.

Toda ciencia tiene un objeto y un método. Este último es la forma en que se procede en la investigación de las cuestiones que aquella se plantea. Para que un matemático considere resuelto un problema ha de justificar sus conclusiones con un *razonamiento deductivo*, cuyo conjunto se conoce como *demostración* y que resulta una pieza esencial del método de las matemáticas: *el método axiomático-deductivo*. Sin éste no hay matemáticas, pero sin intuición creadora no hay ni matemáticas, ni matemático. Ambos son objeto de este trabajo.

Estas páginas tienen el propósito de acercar al lector al *método de las matemáticas* y por tanto trata de cómo se crean las matemáticas y de cómo se presentan una vez creadas.

Entre nuestros objetivos se encuentran: ayudar al desarrollo de la capacidad de razonamiento matemático del lector, familiarizarle con la lectura y realización de demostraciones, enseñarle las claves, la nomenclatura y la importancia del método de nuestra ciencia, y también enfrentarle a la actividad creadora, a reflexionar sobre sus procesos de pensamiento y el de sus colegas; en definitiva, enseñarle que el *pensamiento matemático* de cada uno de nosotros es mejorable y que su desarrollo es una pieza fundamental para hacer matemáticas.

Este libro tiene su origen en los cursos que, sobre la materia, imparte el autor a los alumnos de primer año de la Licenciatura en Ciencias Matemáticas de la Universidad de Cádiz, pero su contenido es igualmente apropiado para cualquier joven que, al culminar sus estudios de Bachillerato, desee cubrir el tránsito que hay entre las matemáticas preuniversitarias y las que encontrará en los estudios científicos o técnicos en la Universidad.

Los prerrequisitos para asimilar el contenido de este libro son francamente escasos, tal vez el único requisito necesario sea una cierta capacidad de abstracción y una elemental familiaridad con las matemáticas del Bachillerato. Por ello, pensamos que también es accesible para un público más amplio que el de los estudiantes universitarios.

El libro consta de nueve capítulos y un epílogo. La mayoría de las secciones, de los distintos capítulos, incorporan al final una relación de ejercicios, cuya finalidad es que el lector aumente su comprensión de los conceptos tratados, profundice en las relaciones entre ellos y adquiera una cierta pericia en los aspectos más instrumentales, a la vez que le sean útiles para mejorar su capacitación matemática general (es decir, mejorar: la *creatividad matemática*, el *rigor lógico* y la *corrección en la expresión* de los pensamientos matemáticos).

El primer capítulo es de carácter introductorio. Presenta en qué consiste el método de las matemáticas y su necesidad. Sobre las ideas que escuetamente se exponen, se desarrollará el resto del trabajo. Finaliza proponiendo veintidós *problemas* de variada, pero considerable dificultad para el novicio y que constituyen un eje vertebrador del discurso global del libro. Es francamente complicado hablar del proceso de *creación* en matemáticas si nuestro interlocutor no se ha enfrentado nunca a esta tarea. Recomendamos, encarecidamente, que se intenten resolver, paulatinamente, a la vez que se avanza en la lectura de otros capítulos. En el último cobrará completo significado esta propuesta metodológica.

El segundo capítulo se dedica a introducir algunas nociones de lógica, prestando especial atención a la importancia de efectuar un razonamiento correcto. Este punto es especialmente importante, por lo que, tanto en los ejercicios de éste como de otros capítulos, aparecerán *deducciones* matemáticas, sobre las que el lector deberá examinar su corrección. Una importante sección se dedica

a la familiarización con el significado de lo que es un axioma, un teorema, un corolario, un lema, una definición y otros términos de las matemáticas, así como al análisis de distintas técnicas de demostración, adecuadamente ejemplificadas.

Los capítulos tercero al octavo se dedican a la teoría de conjuntos, universalmente utilizada hoy día para la presentación de cualquier campo de las matemáticas. Se efectúa la exposición desde una óptica descriptiva, teniendo muy presente a nuestro potencial lector y sus necesidades, pero paulatinamente, y sólo tras una presentación informal (aunque rigurosa), se hace referencia a los requisitos necesarios para una presentación formal de aquellos conceptos. Nuestro propósito es doble: por una parte, ilustrar el significado del comúnmente denominado método axiomático–deductivo y, por otro, crear las intuiciones previas necesarias sobre las que en un futuro el lector pudiera abordar el estudio de la teoría axiomática de conjuntos. Los capítulos tercero al sexto se dedican a los conceptos básicos de la teoría de conjuntos, el séptimo a la inducción matemática y con el octavo pretendemos que el lector se asome al fascinante mundo del *infinito* matemático.

En el último capítulo volvemos al proceso de *creación matemática.* Para entonces el lector tendrá una experiencia cercana de lo que significa pelearse con un problema matemático y puede que una idea aproximada del complejo mundo de las intuiciones. Tras analizar el proceso de resolución de un problema, se abordan cuestiones generales para mejorar la capacitación matemática del lector.

Finalmente en el epílogo se efectúan algunas precisiones sobre las limitaciones del alcance del método axiomático–deductivo, y del significado de demostración en matemáticas, terminando con algunas consideraciones relevantes sobre los axiomas de la teoría de conjuntos.

Estoy en deuda con mis compañeros y a la vez amigos; sus sugerencias han sido valiosas y útiles. Expresamente deseo mencionar a los doctores Romero Romero, Díaz Moreno, Aizpuru Tomás, Benítez Trujillo y Pérez Cuéllar.

Contenido

Capítulo 1

Acerca del método de las matemáticas

¿Qué es una demostración? ¿Qué conocemos en matemáticas, y cómo lo conocemos? ¿Qué es el "rigor matemático"? ¿Qué es la "intuición matemática"? Al ir formulando estas preguntas me daba cuenta de que no conocía las respuestas. ... Lo que me inquietaba e incomodaba era que yo no sabía cuál era mi propia opinión acerca de ellas.
(DAVIS Y HERSH, 1988, PG. 21)

1.1 Primeras consideraciones

En matemáticas, creatividad y rigor son dos caras de una misma moneda. Es la curiosidad, el deseo de saber, típico de cualquier investigador, el que lleva al matemático a preguntarse el porqué de determinadas *regularidades*, si tras ellas se esconde un hecho matemático desconocido, o a formularse preguntas tales como ¿qué sucederá si ...?, ¿será cierto que...?, o escudriñar si propiedades conocidas en ciertos ámbitos valdrán en otros más generales, etc. Cada interrogante que se plantea, es un problema con enunciado aún impreciso, con horizonte imprevisible y del que no conoce los caminos conducentes a su solución.

Es la imaginación la que motiva el planteamiento de problemas y es también ella la que conduce la labor investigadora, de la que será un instrumento imprescindible e inapreciable el rigor lógico, la validez de las deducciones más allá de cualquier duda razonable.

Por otra parte, la precisión en el enunciado de las propiedades obtenidas, en

la definición de los conceptos tratados, permitirán avanzar en el conocimiento del campo de estudio en el que se inscribe el problema resuelto.

Inspiración, precisión y rigor son aspectos distintivos del *proceder matemático*. Veamos algunos ejemplos en relación a estas cuestiones.

Consideremos los números impares: 3, 5, ... Comprobemos que: $3 = 2^1 + 1$, $5 = 2^2 + 1$, $7 = 2^2 + 3$, $9 = 2^3 + 1$, $11 = 2^3 + 3$, $\ldots 21 = 2^4 + 5$. Todos ellos se pueden expresar como una potencia de dos más o bien 1, o bien un número primo[1]. ¿Será cierto para cualquier número impar mayor que 1? La suposición en sentido afirmativo o negativo de la respuesta a una tal interrogante se denomina, en matemáticas, *conjetura*. En principio podríamos conjeturar que cualquier número impar mayor que 1 se podrá expresar como una potencia de dos más uno o un número primo.

Si continuamos examinando casos particulares podremos ver cómo 127 no puede expresarse de la forma indicada, pues:

$$\begin{aligned}
127 &= 2 + 125 = 2 + 5 \cdot 25,\\
127 &= 4 + 123 = 2^2 + 3 \cdot 41,\\
127 &= 8 + 119 = 2^3 + 7 \cdot 17,\\
127 &= 16 + 111 = 2^4 + 3 \cdot 37,\\
127 &= 32 + 95 = 2^5 + 5 \cdot 19,\\
127 &= 64 + 63 = 2^6 + 3 \cdot 21,
\end{aligned}$$

y la siguiente potencia de dos es $2^7 = 128$, por lo que tenemos un caso particular que nos indica la incorrección de nuestra suposición; se dice que es un *contraejemplo* de la conjetura, cuya existencia establece que aquella es incorrecta.

Es evidente que $127 = 2^7 - 1$. Los números de la forma $M_n = 2^n - 1$, con n natural, se denominan *números de Mersenne(1588-1648)*. Examinando el comportamiento de estos números, Mersenne expresó diversas conjeturas. A la vista de la siguiente tabla

n	$2^n - 1$	¿es n primo?	¿es $2^n - 1$ primo?
2	3	si	si
3	7	si	si
4	15	no	no
5	31	si	si
6	63	no	no
7	127	si	si

es fácil efectuar estas dos conjeturas:

- **Conjetura 1:** Si n es primo, entonces $2^n - 1$ es primo.

[1]Recordemos que un número natural mayor que 1 se dice que es *primo* si no se puede escribir como producto de dos números naturales menores que él, en caso contrario se dice que es *compuesto*. Desde luego, si n es compuesto y $n = p \cdot q$, entonces $q > 1$ y $p > 1$.

- **Conjetura 2:** Si n es compuesto, entonces $2^n - 1$ es compuesto.

La primera conjetura es incorrecta. Prosiguiendo con las comprobaciones vemos que $2^{11} - 1 = 2047 = 23 \cdot 89$. Sin embargo no aparece contraejemplo alguno de la segunda conjetura, incluso para valores mayores de n, digamos, por ejemplo, $n = 50$. Pero, ¿será válida la conjetura?, ¿quién nos asegura que no aparecerá un contraejemplo para un valor de n suficientemente grande? Al fin y al cabo es imposible agotar la comprobación, pues, como es obvio, no es posible ensayar con todos los números naturales.

Por otra parte, encontrar contraejemplos no siempre es una tarea fácil. Fermat (1601–1665) conjeturó que los números de la forma $F_n = 2^{2^n} + 1$ (que se conocen como números de Fermat), eran primos; así lo ratificaban: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. Pero determinar si un número es primo no es tarea fácil y aún menos lo era antes de la existencia de los ordenadores. Hasta 1739 no se demuestra, por Euler (1707–1783), la incorrección de esta conjetura, proporcionando como contraejemplo, precisamente, el siguiente número de Fermat: $F_5 = 641 \cdot 6700417$.

Los contraejemplos son una forma de refutar conjeturas, pero el hecho de no encontrar un contraejemplo no garantiza la validez de aquella. El único camino para validar una conjetura es *demostrarla.*

Veamos que la segunda conjetura acerca de los números de Mersenne es correcta:

> *Si n es compuesto, entonces existen dos enteros positivos p y q tales que $1 < p < n$, $1 < q < n$ y $n = p \cdot q$.*
>
> *Ahora bien:*
>
> $$\begin{aligned} 2^n - 1 &= 2^{pq} - 1 \\ &= (2^p - 1)(1 + 2^p + 2^{2p} + \ldots + 2^{(q-1)p}), \end{aligned}$$
>
> *por lo que $2^n - 1$ se puede descomponer en producto de dos enteros.*
>
> *Ya que $p < n$, entonces $a = 2^p - 1 < 2^n - 1$ y, por otra parte, puesto que $p > 1$ se sigue que $a = 2^p - 1 > 2^1 - 1 = 1$. De $ab = 2^n - 1$ y $a > 1$, se sigue que $b = (1 + 2^p + \ldots + 2^{(q-1)p}) < 2^n - 1$.*
>
> *Concluimos que $2^n - 1$ es compuesto.*

Ahora que la conjetura ha sido probada la denominaremos *teorema* y lo enunciamos así:

Teorema 1.1.1 *Si n es un entero positivo compuesto, entonces $2^n - 1$ es un entero positivo compuesto.*

Y el proceso *deductivo* seguido anteriormente lo denominaremos *demostración* del teorema.

Algunos estudiantes tienen la impresión equivocada de que todas las matemáticas ya están hechas y que sólo queda estudiarlas y conocer los resultados a los que han llegado eminentes matemáticos de otras épocas.

Hemos visto que si n es primo, $2^n - 1$ puede ser primo o compuesto. Pero ¿cuáles son los números de la forma $2^n - 1$ que son primos y cuáles no?, ¿cuántos números primos de la forma $2^n - 1$ existen?, ¿son un número finito o hay infinitos? El 24 de Agosto de 1997 se dio a conocer el 36 primo de Mersenne, se trata de $M_{2976221} = 2^{2976221} - 1$, tiene 895932 dígitos; su transcripción ocuparía un libro de unas 400 páginas y si se escribiera en una sola línea, con un tamaño de fuente de 10 puntos (el mismo tamaño de estas letras) ésta tendría 3160 metros. El 27 de Enero de 1998 se anunciaba el 37 primo de Mersenne, que es el número primo más grande conocido hasta la fecha, es $M_{3021377} = 2^{3021377} - 1$, tiene 909526 dígitos y para la determinación de su primalidad se necesitaron 46 días con un Pentium a 200MHz. Las preguntas anteriores no tienen aún respuestas, son *problemas abiertos* de las matemáticas, fáciles de enunciar y entender, pero cuya resolución se viene resistiendo durante cientos de años.

También antes hablamos de los números de Fermat. Actualmente se conjetura que F_n es compuesto para $n \geq 5$. Para observar la envergadura de este aparentemente trivial problema hemos de resaltar que en 1990, 251 años después de que Euler probara que F_5 era compuesto, el último número de Fermat factorizado era F_9.

Desde situaciones elementales a cuestiones muy complejas, el mundo de las matemáticas está lleno de interrogantes que esperan ser descubiertos. Es la inagotable curiosidad del ser humano la que crea los problemas, los retos y el avance de nuestra ciencia. Curiosidad, creatividad e intuición han de ser cuidadas con esmero.

Si usted lector es un novicio en las matemáticas, ante una demostración como la que vimos anteriormente, puede sentirse sorprendido: ¿cómo ha surgido?, incluso puede sentirse abrumado: ¿cómo se me va a ocurrir a mi tal camino?

Los procesos de pensamiento que son útiles para resolver problemas matemáticos han de ser un objeto preferente de nuestra atención si deseamos *hacer* matemáticas. Las intuiciones pertenecen al mundo de la psicología y son difícilmente explicables, pero estas tienen que ver con la capacidad que tenemos para interrelacionar conceptos y conocimientos, de aplicar técnicas conocidas o de extrapolarlas a situaciones diferentes. Vamos a ver un ejemplo de ésto, pero para ello necesitaremos previamente enunciar y demostrar un teorema, cuya existencia se remonta a Euclides (s. III a. C.), sobre los números primos.

Teorema 1.1.2 *Existe una infinidad de números primos.*

Demostración. Supongamos por el contrario que sólo hay un número finito de primos, sean éstos: $p_1, p_2, \ldots, p_k$. Formemos el número $n = p_1 p_2 \ldots p_k + 1$. Este número no puede ser divisible por p_i, con $i \in \{1, \ldots, k\}$, toda vez que el resto es 1. Ahora bien, o n es primo, en cuyo caso llegamos a contradicción, pues $n > p_k$

de forma obvia, o es compuesto, pero en este caso tendrá un divisor primo[2], necesariamente distinto de todos los p_i, $i \in \{1, \ldots, k\}$, obteniéndose nuevamente una contradicción con el hecho de que todos los primos eran: $p_1, \ldots, p_k$.

Si llegamos a contradicción esta surge de suponer que el número de primos es finito, por lo que estos han de ser infinitos[3].

■

Observemos ahora los siguientes números naturales: $3, 7, 11, 15, 19, \ldots$ que son números de la forma $4k + 3$, con k natural. Vemos que sólo con escribir unos cuantos, inmediatamente aparecen algunos que son primos. Es natural preguntarse: ¿existirá un número finito de números primos que son múltiplos de 4 más 3? o, por el contrario, ¿habrá un número infinito de ellos?

No es aventurado conjeturar que existe una infinidad de números primos de la anterior forma; al fin y al cabo hay una infinidad de números primos, ¿por qué no podría obtenerse a su vez una infinidad mediante la expresión $4k + 3$?

A continuación reproducimos la narración, realizada por un alumno, del proceso que siguió para probar la conjetura[4]. Es pertinente advertir que él conocía la demostración, anteriormente expuesta, de la existencia de infinitos números primos.

> *"Mi idea fue proceder de forma análoga al teorema de existencia de infinitos números primos: suponer que hay un conjunto finito que contiene a los primos de la forma $4k+3$ e intentar construir un número que fuese primo y mayor que todos ellos. De la contradicción deduciríamos la validez de nuestra conjetura.*
>
> *Considero que hay un número finito de primos $4k + 3$ y que* [5] *son $p_1, \ldots, p_k$. Ahora no puedo, como en el teorema, hacer uso de $p_1 \ldots p_k + 1$ y considerar que de no ser primo tendrá un divisor primo distinto de los p_i, pues aunque ello es verdad, no obtengo contradicción alguna, pues el factor primo no tiene por qué ser múltiplo de 4 más 3, bueno al menos que yo sepa.*
>
> *Así pues, tenía que intentar alguna variación, en función de la particularidad de mi problema: 'múltiplos de 4 más 3'.*

[2] Aunque este hecho nos es muy familiar desde la enseñanza elemental, en Teoría de Números se demuestra que cualquier entero mayor que 1 o es primo o se puede descomponer en producto de factores primos, que no es otro que el conocido Teorema Fundamental de la Aritmética.

[3] Esta situación desde la Lógica se conoce como *principio del tercio excluso*: "Una proposición es cierta o lo es su contraria", y que tendremos la oportunidad de estudiar en el capítulo dedicado a la Lógica.

[4] Hemos efectuado una reproducción *tal cual*, pues entendemos que así resulta más relevante, aunque ello implique una redacción descuidada y ciertas imprecisiones en el lenguaje.

[5] **Comentario:** Hay que advertir que no es muy afortunado indicar los múltiplos de 4 más 3 mediante $4k + 3$ y denotar el supuesto último primo de tal naturaleza como p_k, pues se presta a confusión. Entiéndase aquí que el alumno no está vinculando un k al otro.

Por lo pronto, parece razonable que considere $n = p_1 \dots p_k + 3$ *a fin de que el número construido tenga más facilidad para que resulte* $\dot{4} + 3$. *Me di cuenta de que si* k *es múltiplo de* 3, *entonces* $4k + 3$ *también y por tanto no me vale. Esto introduce una exigencia más: he de quitar el* 3, *así que he de considerar:* $7 \cdot 11 \cdot \ldots \cdot p_k + 3$. *Ahora tenía otro problema,* $7 \cdot \ldots \cdot p_k$ *es impar (por ser producto de primos mayores que* 2*), luego no puede ser múltiplo de* 4, *por ello consideré:* $n = 4 \cdot 7 \cdot \ldots \cdot p_k + 3$. *Este si es de la forma* $\dot{4} + 3$.

Si ahora divido por los p_k *obtengo siempre de resto* 3, *por lo que* n *es primo con* $\{7, 11, \ldots, p_k\}$. *Pero podría ser divisible por algún número primo que no es de la forma* $\dot{4}+3$, *es decir de la forma* $\dot{4}+1$.

En este punto me desanimé y pensé que tal vez el camino no me llevaba a ninguna parte o que tal vez hubiera un número finito de tales primos. Aquí lo dejé.

Estuve reinando en el tema. Cuando volví al problema tenía claro que los números que son primos[6] *o son* $\dot{4} + 3$ *o son* $\dot{4} + 1$, *luego si los de un tipo son un número finito, los del otro han de ser infinitos, y lo más probable es que los dos sean infinitos, en cualquier caso ha de haber una infinidad de los de un tipo. Así que decidí continuar por donde iba.*

¿Qué es lo que tengo? Sé que $n = 4 \cdot 7 \cdot \ldots \cdot p_k + 3$ *no es múltiplo de* 2 *por ser impar, no es múltiplo de* 3, *por no ser el primer sumando múltiplo de* 3, *y que cualquiera que sea el número,* $7, \ldots, p_k$, *múltiplo de* 4 *más* 3, *considerado,* n *no es múltiplo de él (el resto es siempre* 3*). Sólo he de probar que* n *además es primo. Si lo es y supongo lo contrario habré de llegar a un absurdo.*

Supuse que $n = 4 \cdot 7 \cdot \ldots \cdot p_k + 3$ *era compuesto. En ese caso* n *se puede descomponer en factores primos y todos no pueden ser de la forma* $\dot{4} + 1$, *pues en ese caso el producto de todos ellos es también de la forma* $\dot{4}+1$, *pero esto es imposible porque* n *es* $\dot{4}+3$. *Así que* n *tiene un factor, que lo llamo* q, *que es primo y es de la forma* $\dot{4}+3$, *pero entonces* q *ha de ser uno de los números* $\{7, 11, \ldots, p_k\}$, *pero ello es imposible pues* n *no es múltiplo de ninguno de los números:* $7, 11, \ldots, p_k$.

Ya tenía que n *es primo y que* $n > p_k$, *es decir* $n \notin \{7, \ldots, p_k\}$. *Ya tenía la contradicción, por tanto hay infinitos primos de la forma múltiplo de cuatro más tres."*

Hagamos algunos comentarios sobre el proceso seguido por el alumno:

[6] **Comentario:** La siguiente afirmación no es realmente cierta, pues 2 es primo y no se encuentra en ninguno de los dos grupos. En todo caso, por el discurso, es evidente que el alumno estaba pensando en primos mayores que 2.

1. Ha utilizado técnicas que fueron útiles en problemas similares, para resolver el que se le planteaba.
2. Ha examinado la naturaleza específica de su problema y ha comprendido donde radicaba la dificultad del mismo.
3. Ha *vuelto atrás* continuamente, para validar el proceso.
4. No ha desesperado: ha peleado con el problema.
5. Ha sido cuidadoso en sus razonamientos, en los sucesivos pasos.

Esta sería la forma de presentar el anterior resultado y demostración.

Teorema 1.1.3 *Existe una infinidad de números primos que son múltiplos de cuatro más tres.*

Demostración. Supongamos que existe un número finito de primos que son múltiplos de cuatro más tres. Sean éstos, una vez ordenados de menor a mayor, $\{3, p_1, \ldots, p_k\}$, con $p_1 = 7$.

Consideremos el número natural $n = 4 \cdot 7 \cdot 11 \cdot \ldots \cdot p_k + 3$, que de forma obvia es

$$n = \dot{4} + 3 \quad \text{y} \quad n > p_k. \tag{1.1}$$

Y n no es múltiplo de 2, por ser impar, tampoco es múltiplo de 3 y

$$n \neq \dot{p}_i, \quad p_i \in \{p_1, \ldots, p_k\}, \tag{1.2}$$

ya que al dividir n por cualquier $p_i \in \{p_1, \ldots, p_k\}$, el resto es 3.

Ahora bien, si n es compuesto, como $n = \dot{4} + 3$, al menos uno de los factores de su descomposición factorial ha de ser de la forma $\dot{4} + 3$, sea éste q, luego $q \in \{3, p_1, \ldots, p_k\}$. Pero ello se contradice con que $n \neq \dot{3}$ y (1.2). Por tanto,

$$n \text{ es primo.} \tag{1.3}$$

Ahora bien, (1.3) y (1.1) se contradicen, por lo que existe una infinidad de primos que son múltiplos de cuatro más tres.

■

Como podemos observar, en la demostración queda oculto el tipo de razonamiento que ha hecho posible la misma. Éste ha de ser desvelado por el lector (y es especialmente instructivo efectuar este ejercicio). De hecho comprender un teorema es mucho más que seguir el razonamiento lógico–deductivo presente en su demostración.

Otra demostración del mismo teorema es:

Demostración. Supongamos que existe un número finito de primos de la forma $\dot{4} + 3$, siendo éstos: $p_1 < \ldots < p_k$. Sea $n = 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8 \cdot 10 \cdot \ldots \cdot p_k + 3$, donde

entre los factores del primer sumando se han excluidos los múltiplos de 3. Es claro que $n = \dot{4} + 3$ y que $n > p_k$, de donde se tiene que

$$n \text{ es compuesto.} \tag{1.4}$$

Ahora bien:

$$n \neq \dot{2}, \tag{1.5}$$

toda vez que n es claramente impar.

$$n \neq \dot{3}, \tag{1.6}$$

pues el primer sumando que integra n no lo es.

$$n \neq \dot{p}, \qquad \text{si} \quad 3 < p \leq p_k, \tag{1.7}$$

toda vez que p figura en el primer sumando y por tanto el resto será 3.

De (1.5), (1.6) y (1.7) se sigue que n no es divisible por ningún primo $p \leq p_k$, de donde

$$n \text{ es primo.} \tag{1.8}$$

(1.4) y (1.8) se contradicen. Por tanto, existe una infinidad de primos que son múltiplos de cuatro más tres.

■

Compare el lector las dos demostraciones y advierta la sutil diferencia de ambas.

1.2 Algunos problemas

La creatividad en matemáticas se pone de manifiesto en la resolución de problemas. Los que seguidamente se relacionan, aunque de variada complejidad, son abordables con la capacitación matemática que se tiene al culminar los estudios de Bachillerato. En este sentido son accesibles a cualquier lector que verifique aquél requisito, pero ha de advertirse que son *problemas* y que le supondrán (al menos eso deseamos) un desafío. Saber que son difíciles pero a la vez accesibles constituye un reto al que el lector no debiera sustraerse; en el proceso de resolución descubrirá muchos aspectos interesantes de la forma de *hacer matemáticas.*

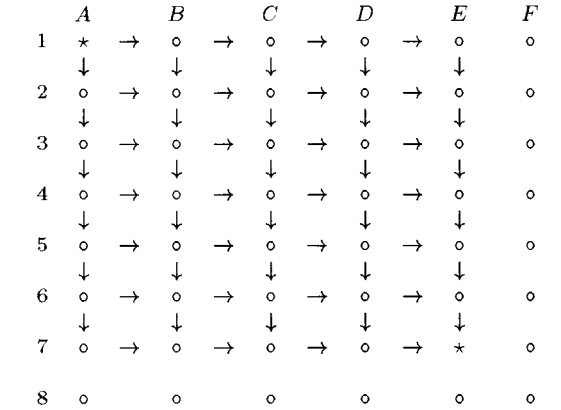
Recomendamos vivamente que se vayan abordando paralelamente a la lectura de estas páginas, para la que no es requisito en modo alguno (incluso no es recomendable desde nuestros propósitos) haber resuelto todos los problemas que se relacionan. En el capítulo 9 volveremos a tratar sobre la resolución de problemas y para entonces esperamos que del contenido de los capítulos anteriores y de la "pelea" con estos problemas el lector tenga una idea ajustada del método de las matemáticas.

Problemas

1. Observemos que $5^2 = 25$, $7^2 = 49$, $11^2 = 121$, etc. Y también que $25 = 24+1$, $49 = 2\cdot 24+1$, $121 = 5\cdot 24+1$. ¿Será verdad que el cuadrado de todo número primo mayor que 3 es múltiplo de veinticuatro más uno?

2. Si multiplicamos tres números enteros positivos y consecutivos observaremos que nunca nos sale como resultado del producto un cubo perfecto (es decir, el cubo de un número natural). ¿Se anima el lector a demostrarlo?

3. Las calles de una ciudad forman una cuadrícula, como se indica en la figura:



¿Cuántos caminos distintos de longitud mínima pueden seguirse para ir de $A-1$ a $E-7$?

4. ¿Cuánto vale la suma $\sum_{i=1}^{n} i^k$, siendo $k \in \mathbb{N}$?

5. ¿Cuántos poliedros convexos se pueden formar si todas sus caras son triángulos equiláteros?

6. Si ordenamos de mayor a menor las cifras del número 6174, luego de menor a mayor y restamos ambos, obtenemos: $7641 - 1467 = 6174$. ¡Bueno, tampoco es para tanto! Tomemos ahora el número 3677 y hagamos lo mismo: $7763 - 3677 = 4086$; repetimos el proceso: $8640 - 0468 = 8172$, y ahora otra vez $8721 - 1278 = 7443$. Continuemos: $7443 - 3447 = 3996$, $9963 - 3699 = 6264$, $6642 - 2466 = 4176$, $7641 - 1467 = 6174$. De nuevo 6174. El lector debiera ensayar con otros números

   Probar que cualquiera que sea el número de cuatro cifras (no todas iguales) elegido, el procedimiento anterior conduce al número 6174 en, a lo más, siete pasos.

7. ¿Es posible inscribir en un triángulo dado un cuadrado de forma que un lado del cuadrado esté sobre la base del triángulo y los otros dos vértices cada uno en uno de los otros dos lados del triángulo?

8. Una cabra está atada por una cuerda de 21 metros a la esquina exterior de un redil, que tiene forma de exágono regular de 6 metros de lado, rodeado por un campo de hierba. ¿En qué área puede pastar la cabra?

9. Se tienen dos semicircunferencias iguales que son tangentes entre sí y de modo que sus diámetros se encuentran en una misma recta. Trazamos a éstas una tangente común, paralela a la recta anterior, e inscribimos una circunferencia tangente a las semicircunferencias y a la recta tangente. Luego inscribimos una segunda circunferencia tangente con las dos semicircunferencias y con la primera circunferencia, etc. Así sucesivamente vamos obteniendo circunferencias cada vez más pequeñas.

   Determinar "alguna relación" entre los radios de éstas circunferencias y el radio de las semicircunferencias originales.

10. Determinar la probabilidad de que dos números positivos x e y, menores que 1, elegidos al azar, constituyan, junto con 1, una terna de números $(x, y, 1)$ que puedan ser lados de un triángulo obtusángulo.

11. Se llama parte alícuota de un entero positivo n a todo divisor positivo suyo menor que él. Dos números se dicen *amigos* si cada uno es la suma de las partes alícuotas del otro. Por ejemplo, 220 y 284 son números amigos. Demostrar que un par de números naturales m y n son amigos si y sólo si las sumas de las partes alícuotas, tanto de m como de n, son iguales a $m + n$.

12. Determinar todos los números naturales n tales que $n(n+1)(n+2)(n+3)$ tenga exactamente tres divisores primos.

13. Un padre tiene cuatro importantes cuadros (un bodegón, una marina, un retrato, un cuadro abstracto) y decide regalárselos a sus hijos: Alberto, Juan y Eva. ¿De cuántas formas diferentes puede regalar los cuadros a sus hijos? Entre otras posibilidades podría dar todos los cuadros a un mismo hijo.

14. Demostrar que cualesquiera que sean $a, b, c, d \in \mathbb{R}$ verificando que $a^2 + b^2 + c^2 + d^2 = ab + bc + cd + da$, entonces $a = b = c = d$.

15. Si por p_n denotamos el n–ésimo número primo (por ejemplo, $p_4 = 7$), probar que ningún número de la forma $p_1 \cdot p_2 \cdots p_n + 1$ es un cuadrado.

16. Demostrar que cualquiera que sea $n \in \mathbb{N}$, las fracciones

$$\frac{n-1}{n}, \quad \frac{n}{2n+1}, \quad \frac{2n+1}{2n^2+2n}$$

   son irreducibles.

17. Un número n se dice que es *perfecto* si es igual a la suma de todas sus partes alícuotas, por ejemplo el 6. Se dice que n es *abundante* si es menor

que esta suma, por ejemplo el 12. Se dice que n es *deficiente* si n es mayor que la suma de sus partes alícuotas, por ejemplo el 11. Probar que todas las potencias de primos son números deficientes.

18. El 12 es un número abundante. ¿Hay algún número abundante que sea impar? y, en su caso, ¿cuántos números abundantes impares habrá?

19. Elijamos un entero positivo N, por ejemplo 6. Determinemos los divisores positivos de N. Para N=6 son $\{1, 2, 3, 6\}$. Calculemos ahora el número de divisores de los divisores determinados anteriormente; en este caso será $\{1, 2, 2, 4\}$. Este conjunto tiene la siguiente propiedad:

$$1^3 + 2^3 + 2^3 + 4^3 = 1 + 8 + 8 + 64 = 81 = (1 + 2 + 2 + 4)^2.$$

Tomemos ahora 12, cuyos divisores son $\{1, 2, 3, 4, 6, 12\}$. El número de divisores de cada uno de los números anteriores es $\{1, 2, 2, 3, 4, 6\}$. Resulta que:

$$1^3 + 2^3 + 2^3 + 3^3 + 4^3 + 6^3 = (1 + 2 + 2 + 3 + 4 + 6)^2.$$

¿Será este resultado válido cualquiera que sea N?

20. Demostrar que si $ABCD$ es un cuadrilátero convexo cualquiera, inscrito en una circunferencia, entonces se verifica que el producto de las diagonales es igual a la suma de los productos de los lados opuestos:

$$\overline{AC} \cdot \overline{BD} = \overline{AB} \cdot \overline{CD} + \overline{BC} \cdot \overline{AD}.$$

21. Sean p y q primos distintos y sea $n = p \cdot q$. ¿Cuántos son los enteros positivos menores o iguales que n que tienen factores comunes con n?

22. Una tripleta de números primos la forman tres números primos de la forma p, $p + 2$ y $p + 4$, como, por ejemplo, 3, 5 y 7. ¿Existen infinitas tripletas de números primos?

Capítulo 2

Nociones de Lógica

2.1 Proposición. Conectivos lógicos. Tablas de verdad

Con frecuencia, en nuestra vida cotidiana tenemos la necesidad de "argumentar", de "justificar" nuestras acciones y omisiones, de "convencer" a otros de nuestras posiciones, etc. Por ejemplo, un padre puede recriminar a su "díscolo" hijo que no ha estudiado: "Sabes que si estudias, apruebas. No has aprobado, luego no has estudiado". Un amigo puede "convencer" a otro de que él trabaja más que un tercero, Pepe, así: "Tú estás más horas en la oficina que Pepe y yo estoy más horas que tú, luego yo estoy más tiempo que Pepe trabajando". Y muchos más: "A ti te gustan todas las rubias, Marisa es rubia, luego te gusta", "el vecino del quinto no paga la comunidad, luego al menos uno de los vecinos es moroso", "si Pedro se entera, le pega; se enteró Pedro y le pegó", "si pierdo el autobús, no puedo ir a la primera clase; perdí el autobús, luego me quedé sin la primera clase".

Variados "argumentos" tienen la misma estructura, por ejemplo, los dos últimos citados anteriormente, responden a la estructura: *"si se verifica p entonces se verifica q; se tiene p, luego también q"*. En el primer caso p sería "Pedro se entera" y q "le pega"; en el segundo p sería "pierdo el autobús" y q "no asisto a la primera clase". Haciendo abstracción del contenido de ambos "argumentos", se trata de uno sólo (una misma forma o estructura).

La lógica simbólica tiene por objeto el análisis formal de los "argumentos" o "deducciones", simbolizando tanto las oraciones variables (Pedro se entera, pierdo el autobús; en estos casos mediante la letra p) como las partículas lingüísticas constantes ("si ... entonces" mediante una flecha $\longrightarrow$, "todo" mediante el símbolo $\forall$, etc.).

A continuación abordaremos el estudio de las nociones básicas de lógica

simbólica que nos son de utilidad para analizar los procesos "deductivos" en Matemáticas y para interpretar correctamente la comunicación matemática.

Definición 2.1.1 *Llamaremos* proposición *a toda oración con sentido lógico, respecto de la que puede decirse si es verdadera o falsa, denominados valores de verdad o valores lógicos de la proposición.*

Ejemplo 2.1.2 "Cállese" y "¿Qué día es hoy?" no son proposiciones, pues de ellas no podemos afirmar que sean ni verdaderas ni falsas. Tampoco lo es "$7x = 5$", pues será verdadera o falsa, dependiendo del valor de x. Si son proposiciones: "3 es mayor que 5", "todas las rectas son paralelas", "existe un ángulo θ tal que $\cos\theta = \theta$", "dos rectas diferentes en un plano o son paralelas o se cortan en un punto". □

Por simplificar, cuando una proposición es verdadera, decimos que su valor lógico es V y si es falsa diremos que F es su valor lógico. De forma genérica las proposiciones se denotarán mediante letras: p, q, r, ...

Podemos formar nuevas proposiciones, que llamaremos compuestas, a partir de otras, que llamaremos simples, combinándolas mediante partículas tales como "y", "o", ... Por ejemplo: "Euler vivió en San Petesburgo", "Euler vivió en el siglo XIX", que podemos combinar mediante "Euler vivió en San Petesburgo o Euler vivió en el siglo XIX" y también en la forma "Euler vivió en San Petesburgo y Euler vivió en el siglo XIX". Las conjunciones gramaticales y otras partículas que nos sirven para componer proposiciones los llamaremos *conectivos lógicos* o *juntores*, y son: "no", "y", "o", "si ... entonces", "si y sólo si", "o bien ... o bien ...", que estudiaremos seguidamente.

Al formar, mediante los conectivos lógicos, una proposición compuesta a partir de otras simples cuyos valores lógicos se conocen, deberemos determinar el valor lógico de la proposición resultante. El análisis de las distintas posibilidades se hace mediante lo que denominaremos una *tabla de verdad.* Ésta refleja los posibles valores lógicos de la proposición compuesta, sobre la base de contemplar todas las posibles combinaciones de los valores lógicos de las proposiciones simples que la integran. Consecuentemente si una proposición compuesta queda integrada por n proposiciones simples, habrá que determinar 2^n combinaciones.

Definición 2.1.3 *Dada una proposición p llamaremos proposición negación de p y la denotaremos por $\neg p$, a una nueva proposición que es cierta cuando p es falsa y falsa cuando p es verdadera. Se lee "no p".*

La correspondiente tabla de verdad es:

p	$\neg p$
V	F
F	V

Ejemplo 2.1.4 Si p es "3 es mayor que 5", $\neg p$ será "3 no es mayor que 5", que es obviamente verdadera, ya que p era falsa. Si p es "$10 = 23$", $\neg p$ será "$10 \neq 23$", cuyos respectivos valores de verdad son obvios. □

Definición 2.1.5 *Dadas dos proposiciones p y q, llamaremos proposición disyunción de ambas, y lo denotaremos mediante $p \vee q$, a una nueva proposición que será verdadera cuando lo sea p, o lo sea q o lo sean ambas y falsa cuando lo son también ambas. Se lee "p o q".*

Su tabla de verdad es

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Ejemplo 2.1.6 Sean p y q, respectivamente, "3 es mayor que 5" y "10 es un múltiplo de 5"; resultando que $p \vee q$ es "3 es mayor que 5 o 10 es múltiplo de 5", que es una proposición cuyo valor de verdad es verdadero. □

En el lenguaje ordinario la conjunción "o" puede ser incluyente; así si decimos "estos asientos del autobús están reservados para ancianos o personas minusválidas", entendemos que también tiene prioridad un anciano con minusvalía. Del mismo modo si en la puerta de una discoteca leemos que "mujeres o menores de 21 años pagarán el 75% de la entrada", entendemos que también tienen derecho a un descuento del 25% las mujeres menores de 21 años (incluso diríamos que por partida doble). Es decir, la conjunción "o" uniendo dos frases "A" y "B", puede interpretarse como que es "A" o bien es "B", o bien son ambos "A y B"; éste es el sentido que tiene el conectivo lógico "$\vee$".

El juntor "$\vee$" tiene el sentido incluyente señalado y sólo ese, lo que lo diferencia de la "o" del lenguaje ordinario, que a veces puede tener un significado excluyente: "o es A o bien es B, pero no ambos". Por ejemplo si decimos: "el asiento está reservado para ancianos o embarazadas", es claro que "o" es excluyente; de la misma forma al iniciarse un juicio el imputado puede ser declarado "culpable o inocente", pero no ambas cosas a la vez.

Cuando en matemáticas usamos una "o" excluyente debemos especificarlo con precisión indicando que "o bien es A, o bien es B, pero no ambos" y ello se corresponde con otro símbolo lógico que veremos más tarde.

Definición 2.1.7 *Dadas dos proposiciones p y q, llamamos proposición conjunción de ambas, y escribimos $p \wedge q$, a una proposición que sólo es verdadera cuando lo son p y q. Se lee "p y q".*

Tenemos la siguiente tabla de verdad para la conjunción:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Ejemplo 2.1.8 Si p y q, respectivamente, son "3 es mayor que 5" y "10 es un múltiplo de 5", entonces $p \wedge q$ es "3 es mayor que 5 y 10 es múltiplo de 5", que se trata de una proposición falsa. □

Definición 2.1.9 *Dadas dos proposiciones, p y q, la implicación lógica de q a partir de p es una proposición que denotamos por $p \longrightarrow q$, que es falsa cuando p es verdadera y q falsa, siendo verdadera en otro caso. Se lee "p implica q" y también "si p entonces q".*

La correspondiente tabla de verdad es:

p	q	$p \longrightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

La proposición p suele denominarse con algunos de estos nombres: antecedente, premisa, hipótesis o condición suficiente ("es suficiente que se verifique p, para que tenga lugar q"). La proposición q suele denominarse de alguna de estas maneras: consecuente, conclusión, tesis o condición necesaria ("si se verifica p, entonces necesariamente también se verifica q").

Ejemplo 2.1.10 La proposición "si tres es mayor que cinco, entonces diez es múltiplo de cinco" es una proposición verdadera; como también lo es "si tres es mayor que cinco, entonces diez no es múltiplo de cinco". Es también verdadera: "si tres es menor o igual que cinco, entonces diez es múltiplo de cinco". Y es falsa la proposición: "si tres es menor o igual que cinco, entonces diez no es múltiplo de cinco". □

El ejemplo anterior resulta chocante respecto del uso en el lenguaje ordinario de la partícula "si ... entonces ...". En nuestro discurso diario carece de sentido frases como "si la tierra no gira alrededor del sol, entonces usted está leyendo estas líneas", aunque desde un punto de vista lógico la proposición anterior es verdadera. Esta circunstancia puede explicarse si se tiene en cuenta que desde una perspectiva lógica lo que interesa es el valor de verdad de las proposiciones y no el significado de las mismas, ni si la proposición compuesta tiene un

significado coherente. De esta manera la proposición "si 3 es un número compuesto, entonces 5 es un número primo" es verdadera, mientras que "si tres es un número primo, entonces 5 es un número compuesto" es falsa.

Hay otra diferencia con el lenguaje ordinario. En éste, no siempre la partícula "si ... entonces ..." tiene el significado de una consecuencia lógica, no siempre q necesariamente se verifica si lo hace p. Así, por ejemplo, si decimos: "si viene Juan, entonces déjale la silla", pues no podríamos decir que "si yo no le dejé la silla, es porque Juan no vino". Otras matizaciones cabe realizar con respecto al lenguaje ordinario y a ellas nos referiremos en la sección tercera de este capítulo.

Aún siendo diferentes la implicación lógica del condicional del lenguaje usual, vamos a servirnos de éste último para "justificar" la definición de la primera. Supongamos que he dicho: "si me toca la lotería, entonces me compro un coche". Si me toca la lotería y me compro un coche, es claro que no mentí y si no me toca la lotería, tanto me compre un coche, como si no me lo compro, tampoco miento; sólo mentiría si tocándome la lotería no me comprase el coche. Bien es verdad, y ésta es otra diferencia con el lenguaje ordinario, que aun no diciéndolo, mi interlocutor es muy probable que haya entendido que yo sólo me compraré un coche en el caso de que me toque la lotería. El lenguaje usual es rico en matices y las oraciones pueden estar cargadas de significados añadidos y no explicitados; por el contrario en matemáticas el lenguaje ha de ser preciso, unívoco y despejado de significaciones no explicitadas.

Definición 2.1.11 *Dadas dos proposiciones p y q, denominamos doble implicación de p y q, y lo denotamos por $p \longleftrightarrow q$, a la proposición que es verdadera cuando ambas tienen el mismo valor lógico y sólo en ese caso. Se lee "p doble implicación q", o "p si y sólo si q" o "p equivalente a q".*

La correspondiente tabla de verdad es:

p	q	$p \longleftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Ejemplo 2.1.12 Sean p y q, respectivamente, "24 es par" y "13 es primo". La proposición "24 es par si y sólo si 13 es primo" es verdadera. También lo es $p \longleftrightarrow q$, si p y q son, respectivamente, "12 es múltiplo de 8" y "35 es par". Si p y q son, respectivamente, "11 es primo" y "4 es impar", la doble implicación de p y q es falsa. □

Definición 2.1.13 *Dadas dos proposiciones p y q, se llama disyunción excluyente de p y q, o bien diferencia simétrica de p y q, lo que denotamos por $p \underline{\vee} q$,*

a la proposición que es verdadera sólo cuando p y q no tienen simultáneamente el mismo valor de verdad.

Su correspondiente tabla de verdad es:

p	q	$p \underline{\vee} q$
V	V	F
V	F	V
F	V	V
F	F	F

Esta es la o excluyente a la que anteriormente hicimos referencia "o bien es culpable, o bien es inocente", pero no puede ser ambas cosas a la vez.

Ejemplo 2.1.14 Si p y q, son respectivamente, "24 es par" y "13 es primo", entonces $p \underline{\vee} q$ se lee "o bien 24 es par, o bien 13 es primo, pero no ambos", que es falsa. □

Como hemos visto las tablas de verdad nos permiten conocer el valor de verdad de una proposición compuesta, conociendo los valores lógicos de las proposiciones simples que la forman. Por ello, para hacer una tabla de verdad se necesita:

1. Distinguir cuántas proposiciones simples existen.
2. Si n es el número de proposiciones simples, encontrar las 2^n variaciones posibles de valores de verdad.
3. Descomponer la proposición compuesta en las proposiciones simples que la integran.

Ejemplo 2.1.15 Veamos la tabla de verdad de la proposición $\neg(p \wedge \neg q)$.

p	q	$\neg q$	$p \wedge \neg q$	$\neg(p \wedge \neg q)$
V	V	F	F	V
V	F	V	V	F
F	V	F	F	V
F	F	V	F	V

En la última columna obtenemos los posibles valores lógicos de la proposición $\neg(p \wedge \neg q)$. Obsérvese que coinciden con los de $p \longrightarrow q$. □

Ejemplo 2.1.16 La tabla de verdad de la proposición $(p \longrightarrow q) \wedge (q \longrightarrow p)$ es:

p	q	$p \longrightarrow q$	$q \longrightarrow p$	$(p \longrightarrow q) \wedge (q \longrightarrow p)$
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

obteniéndose la tabla de verdad de $p \longleftrightarrow q$. Por ello, en la doble implicación p y q son condiciones necesarias y suficientes para que la otra proposición se verifique. □

Ejemplo 2.1.17 Si realizamos la tabla de verdad de $\neg(p \longleftrightarrow q)$:

p	q	$p \longleftrightarrow q$	$\neg(p \longleftrightarrow q)$
V	V	V	F
V	F	F	V
F	V	F	V
F	F	V	F

la última columna nos da los posibles valores lógicos de $\neg(p \longleftrightarrow q)$, que no son otros que los de $p \veebar q$. □

Ejercicios

1. ¿Cuáles de los siguientes enunciados son proposiciones? En su caso ¿cuáles son sus valores de verdad?
   (a) Sevilla es la capital de Andalucía.
   (b) París es la capital de Francia.
   (c) $7 + 8 = 12$.
   (d) $x + 3 = 8$.
   (e) No sigas hablando.
   (f) $x \cdot y = y \cdot x$, cualesquiera que sean los números reales x e y.
2. ¿Cuál es la negación de las siguientes proposiciones?
   (a) $10 = 23$.
   (b) $7 > 21$.
   (c) Un cuadrilátero no tiene 5 lados.
   (d) 363 no es divisible por 11.
3. Construir una tabla de verdad para cada una de las siguientes proposiciones:

(a) $(p \vee \neg q) \longrightarrow q$.

(b) $(p \vee q) \longrightarrow (p \wedge q)$.

(c) $(p \longrightarrow q) \longrightarrow (q \longrightarrow p)$.

(d) $p \longrightarrow \neg q$.

(e) $\neg p \longleftrightarrow q$.

(f) $(p \longrightarrow q) \vee (\neg p \longrightarrow q)$.

(g) $(p \wedge \neg q) \wedge (\neg p \wedge q)$

(h) $(p \longrightarrow q) \wedge (\neg p \longrightarrow q)$.

(i) $(p \longleftrightarrow q) \wedge (\neg p \longleftrightarrow q)$.

(j) $(\neg p \longleftrightarrow \neg q) \longleftrightarrow (p \longleftrightarrow q)$.

4. Simbolizar las siguientes expresiones:

   (a) Nunca admitiré que nos cobren a ti y a mí.

   (b) Nunca admitiré que nos cobren ni a ti ni a mí.

   (c) No es cierto que María o Juan fueran a su casa.

   (d) No te compro la moto y la cadena.

5. "Como llueva, seguro que no voy al campo". No fue al campo, ¿qué puede afirmarse? Fue al campo, ¿qué puede decirse?

6. "Si me voy de vacaciones, en octubre estaré totalmente relajado".

   (a) En octubre estaba relajado, ¿qué podemos deducir?

   (b) No me fui de vacaciones, ¿qué podemos deducir?

   (c) En octubre no estaba relajado, ¿qué podemos deducir?

   (d) Me fui de vacaciones, ¿qué deducimos?

7. "Iré a Francia sólo si apruebo en junio". ¿Qué ocurrirá en los siguientes casos?:

   (a) No aprobé en junio.

   (b) Fui a Francia.

   (c) No fui a Francia.

   (d) Aprobé en junio.

8. "Volveré a ese bar sólo si no sigue el mismo camarero". Analizar las siguientes expresiones en relación con la anterior:

   (a) He vuelto al bar, luego no sigue ese camarero.

   (b) No es cierto que no siga el camarero y yo haya vuelto al bar.

   (c) Sigue el camarero o vuelvo al bar y a la vez no vuelvo al bar o no sigue ese camarero.

(d) No vuelvo al bar y no sigue el camarero.

(e) No vuelvo al bar y sigue el camarero.

9. Juan, Pedro, Marta y Luisa fueron al extranjero en vacaciones, cada uno a un país distinto. La vecina del quinto, de Luisa, (muy cotilla ella) les preguntó donde estuvieron. Estas fueron sus respuestas:

- Pedro: "Luisa fue a Londres y Marta a Roma".
- Marta: "Juan fue a Roma y Luisa se marchó a Oslo".
- Juan: "Marta se fue a París y Pedro a Roma".

Si cada uno de ellos realizó exclusivamente una afirmación verdadera, ¿a qué ciudad fue cada uno de ellos?

2.2 Proposiciones equivalentes

Un tipo importante de paso que a veces se usa en un razonamiento matemático es reemplazar una afirmación por otra "equivalente" en el sentido que ahora analizaremos.

Definición 2.2.1 *Decimos que una proposición compuesta es una tautología si siempre es verdadera, independientemente de la combinación elegida de valores lógicos de las proposiciones simples que la integran. Si, por el contrario, el valor lógico de una proposición compuesta es siempre falso, decimos que ésta es una contradicción. Cuando una proposición compuesta no es una tautología y tampoco es una contradicción (es decir, puede ser verdadera o falsa, dependiendo de la combinación de los valores lógicos de las proposiciones simples) se dice que es una contingencia o que es indeterminada.*

Definición 2.2.2 *Decimos que dos proposiciones compuestas p y q son lógicamente equivalentes si la proposición doble implicación de ambas, $p \longleftrightarrow q$, es una tautología.*

Ejemplo 2.2.3 Un claro ejemplo de contradicción es $p \wedge \neg p$. Algunos ejemplos de tautologías son:

1. La *ley del tercio excluso*: $p \vee \neg p$.

2. La *ley de no contradicción*: $\neg(p \wedge \neg p)$.

3. El *método de demostración por reducción al absurdo*:

$$(p \longrightarrow q) \longleftrightarrow [(p \wedge \neg q) \longrightarrow (t \wedge \neg t)]. \tag{2.1}$$

Puesto que $t \wedge \neg t$ es siempre falsa, para conocer cómo resultan los valores lógicos de $p \wedge \neg q \longrightarrow t \wedge \neg t$ no es necesario considerar las ocho posibles combinaciones de los valores de verdad de las proposiciones simples p, q y t, bastando tener en cuenta las cuatro formas en que se pueden combinar los valores lógicos de p y q.

p	q	$\neg p$	$\neg q$	$p \longrightarrow q$	$p \wedge \neg q$	$t \wedge \neg t$	$p \wedge \neg q \longrightarrow t \wedge \neg t$	$(\star)$
V	V	F	F	V	F	F	V	V
V	F	F	V	F	V	F	F	V
F	V	V	F	V	F	F	V	V
F	F	V	V	V	F	F	V	V

Observemos, tal y como se indica en la columna $(\star)$, que las proposiciones $p \longrightarrow q$ y $(p \wedge \neg q) \longrightarrow (t \wedge \neg t)$ son lógicamente equivalentes, por lo que una puede ser sustituida por otra y se tiene que la proposición (2.1) es una tautología. Ahora bien, observemos que la segunda proposición es una implicación, cuya premisa es el antecedente p y la negación $\neg q$ del consecuente de la primera; observemos del mismo modo que la conclusión de la segunda proposición es una contradicción: $t \wedge \neg t$.

4. Son lógicamente equivalentes $p \longrightarrow q$ y $\neg p \vee q$.

p	$\neg p$	q	$p \longrightarrow q$	$\neg p \vee q$
V	F	V	V	V
V	F	F	F	F
F	V	F	V	V
F	V	F	V	V

Un ejemplo de una proposición indeterminada es $p \longrightarrow p \wedge q$.

p	q	$p \wedge q$	$p \longrightarrow p \wedge q$
V	V	V	V
V	F	F	F
F	V	F	V
F	F	F	V

□

Las equivalencias lógicas también reciben el nombre de leyes lógicas . Algunas importantes leyes lógicas son las siguientes:

1. Asociativas: $[(p \vee q) \vee r] \longleftrightarrow [p \vee (q \vee r)]$ y $[(p \wedge q) \wedge r] \longleftrightarrow [p \wedge (q \wedge r)]$.
2. Distributivas: $[p \vee (q \wedge r)] \longleftrightarrow [(p \vee q) \wedge (p \vee r)]$ y $[p \wedge (q \vee r)] \longleftrightarrow [(p \wedge q) \vee (p \wedge r)]$.

3. Conmutativas: $(p \vee q) \longleftrightarrow (q \vee p)$, $(p \wedge q) \longleftrightarrow (q \wedge p)$.

4. De identidad: $(p \wedge V) \longleftrightarrow p$, $(p \vee F) \longleftrightarrow p$. Donde mediante V representamos una proposición que es una tautología y con F representamos una proposición que es una contradicción.

5. De complemento: $(p \vee \neg p) \longleftrightarrow V$, $(p \wedge \neg p) \longleftrightarrow F$. Al igual que antes, V y F representan, respectivamente, una tautología y una contradicción.

6. Idempotentes: $(p \vee p) \longleftrightarrow p$, $(p \wedge p) \longleftrightarrow p$.

7. De dominación: $(p \vee V) \longleftrightarrow V$, $(p \wedge F) \longleftrightarrow F$. Como antes, V y F representan, respectivamente, una tautología y una contradicción.

8. De absorción o cancelativas: $[(p \wedge q) \vee q] \longleftrightarrow q$, $[(p \vee q) \wedge q] \longleftrightarrow q$.

9. de De Morgan: $\neg(p \wedge q) \longleftrightarrow (\neg p \vee \neg q)$, $\neg(p \vee q) \longleftrightarrow (\neg p \wedge \neg q)$.

10. Doble negación: $\neg(\neg p) \longleftrightarrow p$

La demostración de estas leyes se hace mediante una tabla de verdad. Probaremos una de las leyes distributivas y dejamos la oportuna prueba de las restantes al lector: $[p \wedge (q \vee r)] \longleftrightarrow [(p \wedge q) \vee (p \wedge r)]$.

p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$
V	V	V	V	V	V	V	V
V	V	F	V	V	V	F	V
V	F	V	V	V	F	V	V
V	F	F	F	F	F	F	F
F	V	V	V	F	F	F	F
F	V	F	V	F	F	F	F
F	F	V	V	F	F	F	F
F	F	F	F	F	F	F	F

Las columnas quinta y octava nos dicen que efectivamente la proposición es tautológica. Como puede observar el lector el procedimiento no es complicado, en todo caso engorroso; si no desea olvidar ninguna posible combinación una buena forma es hacerse un diagrama de árbol, tal y como se indica en la Figura 2.1 y que es suficientemente explícito, por lo que no parece necesario ninguna aclaración adicional.

Aunque cualquier equivalencia lógica puede probarse a partir de las tablas de verdad, dado el engorro de las mismas, sobre todo cuando el número de proposiciones simples es muy elevado, es un método alternativo aconsejable partir de un lado de la equivalencia lógica que se quiere establecer y haciendo

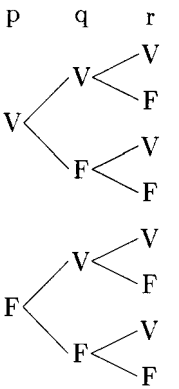


Figura 2.1: Diagrama de árbol

uso de otras equivalencias lógicas conocidas llegar al otro lado.

Ejemplo 2.2.4 Probaremos que $\neg[p \vee (\neg p \vee q)]$ y $\neg p \wedge \neg q$ son lógicamente equivalentes.

$$
\begin{array}{lll}
\neg[p \vee (\neg p \wedge q)] & \longleftrightarrow & \neg p \wedge \neg(\neg p \wedge q) \quad \text{De Morgan} \\
& \longleftrightarrow & \neg p \wedge [\neg(\neg p) \vee \neg q] \quad \text{De Morgan} \\
& \longleftrightarrow & \neg p \wedge [p \vee \neg q] \quad \text{Doble negación} \\
& \longleftrightarrow & (\neg p \wedge p) \vee (\neg p \wedge \neg q) \quad \text{Distributiva} \\
& \longleftrightarrow & F \vee (\neg p \wedge \neg q) \quad \text{Contradicción} \\
& \longleftrightarrow & (\neg p \wedge \neg q) \vee F \quad \text{Conmutativa} \\
& \longleftrightarrow & (\neg p \wedge \neg q) \quad \text{Identidad}
\end{array}
$$

□

Entre las equivalencias lógicas, un caso de especial interés lo constituyen las que relacionan una implicación $p \longrightarrow q$ con otras implicaciones en las que aparecen las negaciones de las proposiciones p y q.

Se tiene que:

p	q	$\neg p$	$\neg q$	$p \longrightarrow q$	$q \longrightarrow p$	$\neg p \longrightarrow \neg q$	$\neg q \longrightarrow \neg p$
V	V	F	F	V	V	V	V
V	F	F	V	F	V	V	F
F	V	V	F	V	F	F	V
F	F	V	V	V	V	V	V

Las columnas quinta y octava y la sexta y séptima nos indican que se tienen las siguientes leyes lógicas:

1. $(p \longrightarrow q) \longleftrightarrow (\neg q \longrightarrow \neg p)$.

   La implicación $p \longrightarrow q$ recibe el nombre de *implicación directa* y el condicional $(\neg q \longrightarrow \neg p)$ la *implicación contrarrecíproca* de la anterior. Obviamente cualquiera de las dos implicaciones podría tomarse como implicación directa, siendo la otra su contrarrecíproca.

2. $(q \longrightarrow p) \longleftrightarrow (\neg p \longrightarrow \neg q)$.

   Obviamente una es contrarrecíproca de la otra, pero en relación a la implicación $p \longrightarrow q$, si la tomamos como implicación directa, reciben los nombres siguientes: $q \longrightarrow p$ *implicación recíproca* del condicional $p \longrightarrow q$. y $\neg p \longrightarrow \neg q$ *implicación contraria* de $p \longrightarrow q$.

Si consideramos como implicación directa a $p \longrightarrow q$, entonces: $q \longrightarrow p$ es la recíproca, $\neg q \longrightarrow \neg p$ es la contrarrecíproca y $\neg p \longrightarrow \neg q$ es la contraria.

Ejercicios

1. Usar las tablas de verdad para verificar las siguientes equivalencias:

   (a) $(p \wedge V) \longleftrightarrow p$.

   (b) $(p \wedge F) \longleftrightarrow F$.

   (c) $(p \vee p) \longleftrightarrow p$.

   (d) $(p \vee V) \longleftrightarrow V$.

2. Utilizar las tablas de verdad para verificar las leyes conmutativas y asociativas de la conjunción y de la disyunción.

3. Utilizar las tablas de verdad para verificar la ley distributiva de la disyunción respecto de la conjunción.

4. Utilizar las tablas de verdad para verificar las leyes de *De Morgan*.

5. Demostrar que las siguientes proposiciones son tautologías:

   (a) $(p \wedge q) \longrightarrow p$.

   (b) $p \longrightarrow (p \vee q)$.

   (c) $\neg p \longrightarrow (p \longrightarrow q)$.

   (d) $\neg(p \longrightarrow q) \longrightarrow \neg q$.

   (e) $(p \wedge q) \longrightarrow (p \vee q)$.

   (f) $[(p \longrightarrow q) \wedge (q \longrightarrow r)] \longrightarrow (p \longrightarrow r)$.

6. Demostrar las leyes cancelativas.

7. Determinar cuándo la proposición $(\neg q \wedge (p \longrightarrow q)) \longrightarrow \neg p$ es una tautología.

8. Utilizando las leyes lógicas simplificar las siguientes fórmulas:

   (a) $\neg(q \vee \neg p) \vee p$.

   (b) $p \vee (q \wedge \neg p)$.

   (c) $\neg(p \vee (q \wedge \neg r)) \wedge q$.

9. Demostrar que $p \longleftrightarrow q$ y $(p \wedge q) \vee (\neg p \wedge \neg q)$ son equivalentes.

10. Demostrar que $(p \longrightarrow q) \longrightarrow r$ y $p \longrightarrow (q \longrightarrow r)$ no son equivalentes.

11. Demostrar que son lógicamente equivalentes $p \longrightarrow (q \longrightarrow r)$ y $(p \wedge q) \longrightarrow r$.

12. Formar una proposición compuesta por otras tres p, q y r que sea verdadera cuando lo sean dos de las proposiciones p, q, r y falsa en cualquier otro caso.

13. Una colección de conectivos lógicos se dice que es *funcionalmente completo* si cualquier proposición compuesta es lógicamente equivalente a una proposición compuesta en la que sólo figuran operadores lógicos de esa colección.

    Demostrar que $\neg$, $\wedge$ y $\vee$ forman una colección de conectivos lógicos funcionalmente completo. ¿Constituirá $\neg$ y $\wedge$ también una colección de conectivos lógicos funcionalmente completo?, ¿Y $\neg$ y $\vee$?

14. La expresión $\neg(p \longrightarrow q) \longrightarrow \neg q$, ¿es una tautología, una contradicción o una contingencia?

15. Probar que las siguientes proposiciones son tautologías:

    (a) $[(p \longrightarrow q) \wedge p] \longrightarrow q$.

    (b) $[(p \longrightarrow q) \wedge \neg q] \longrightarrow \neg p$.

    (c) $[(p \longrightarrow q) \wedge (p \longrightarrow r)] \longrightarrow [p \longrightarrow (q \wedge r)]$.

    (d) $[(p \longrightarrow q) \wedge (r \longrightarrow q)] \longrightarrow [(p \vee r)] \longrightarrow q$.

2.3 Predicados y cuantificadores

Es usual encontrar en matemáticas afirmaciones que involucren a variables, como por ejemplo: "$x > 31$", "$x = y - 23$" o "$x^2 + y^2 = z^2$". Estas afirmaciones no son ni verdaderas ni falsas, si los valores de las variables no se especifican.

La afirmación "$x > 31$" consta de un *sujeto* de la afirmación, que es x, y de un *predicado*, "es mayor que 31". Este último se refiere a una propiedad que el sujeto de la afirmación puede tener o no, dependiendo del valor del mismo. Si denotamos la oración "$x > 31$" por $P(x)$, entonces $P(12)$ es "$12 > 31$" que es

una proposición falsa, mientras que $P(32)$ es la proposición "$32 > 31$" que es verdadera. Estas oraciones $P(x)$ tales que para cada valor de la variable x se tiene que $P(x)$ es una proposición, reciben el nombre de *predicados* o *funciones proposicionales.*

Como hemos indicado, las oraciones en cuestión pueden contemplar más de una variable. Por ejemplo "$x = y - 23$" que podemos denotarla como $Q(x, y)$, resultando que $Q(-23, 0)$ o $Q(7, 30)$, entre otras, son verdaderas y, en particular, $Q(1, 2)$ es falsa. En general una afirmación que involucra n variables la denotaremos por $P(x_1, \ldots, x_n)$.

Los valores de las variables se toman de un cierto "universo de discurso". En los ejemplos vistos, los valores de la variable son números reales.

Definición 2.3.1 *Un enunciado $P(x)$ diremos que es un predicado o una función proposicional si es una expresión en la que aparece una variable, que pertenece a un cierto universo de discurso, tal que para cada valor de la variable x el enunciado $P(x)$ es una proposición.*

De forma análoga se puede definir un predicado con n variables. Puesto que al asignar valores a todas las variables de una función proposicional obtenemos una proposición, es natural considerar los conceptos de negación, disyunción y conjunción de predicados con un mismo "universo de discurso".

Si $P(x)$ es un predicado, llamamos *predicado negación* de $P(x)$ y lo denotamos por $\neg P(x)$, al predicado que asigna a cada valor "a" de la variable x, la proposición $\neg P(a)$.

Si $P(x)$ y $Q(x)$ son dos predicados, con un mismo universo de discurso, llamamos *predicado disyunción* de ambos, y lo denotamos por $(P \vee Q)(x)$, al predicado que asigna a cada valor "a" de la variable x la proposición $P(a) \vee Q(a)$.

Si $P(x)$ y $Q(x)$ son dos predicados, con un mismo universo de discurso, llamamos *predicado conjunción* de ambos, y lo denotamos por $(P \wedge Q)(x)$, al predicado que asigna a cada valor "a" de la variable x la proposición $P(a) \wedge Q(a)$.

Las correspondientes propiedades de las proposiciones vistas en la sección anterior (conmutativas, asociativas, etc.) se verifican también para predicados con un mismo "universo de discurso".

2.3.1 Cuantificadores universal y existencial

Hay dos formas para pasar de una función proposicional a una proposición: dando valores a las variables y mediante *cuantificación* del predicado.

Muchas afirmaciones matemáticas aseguran que una propiedad es verdadera para todos los valores de una variable, por ejemplo "$x \cdot y = y \cdot x$, cualesquiera que sean los números naturales x e y", o también "$x = 0 + x$ cualquiera que sea el número real x". De estas afirmaciones podemos asegurar si son verdaderas o

falsas; es decir, son proposiciones. Ello es así gracias a la partícula "cualquiera que sea", que nos indica la "evaluación" de x en todo el "universo de discurso", efectuándose una cuantificación universal.

Definición 2.3.2 *Si $P(x)$ es un predicado, el cuantificador universal de $P(x)$ es una proposición, que denotaremos por $\forall x\ P(x)$, que es verdadera si $P(a)$ es verdadera, para cada valor "a", en el "universo de discurso", de la variable x y es falsa en otro caso. Se lee "para cada x $P(x)$" o "para todo x $P(x)$", o también "cualquiera que sea x $P(x)$". Al símbolo $\forall$ se le denomina cuantificador universal.*

Ejemplo 2.3.3 "Para cada ángulo x, $\operatorname{sen}^2 x + \cos^2 x = 1$", es una proposición verdadera cuyo "universo de discurso" son los números reales. Podemos simbolizar el enunciado anterior de la siguiente forma: "$\forall x$, $\operatorname{sen}^2 x + \cos^2 x = 1$".

Si el "universo de discurso" donde toma valores la variable son los números reales y tenemos el predicado $P(x)$: "$x < 13$", entonces $\forall x\ P(x)$ es una proposición falsa, pues por ejemplo $P(26)$ es falsa.

Con el mismo "universo de discurso", el predicado $P(x)$: "$x^2 \geq x$" da origen a la proposición "$\forall x\ x^2 \geq x$", que es falsa, pues por ejemplo $P(10^{-1})$ es falsa. Sin embargo, si el universo de discurso son los números enteros positivos, entonces $\forall x\ P(x)$ es verdadera. □

El ejemplo nos indica cómo el valor de verdad del cuantificador universal $\forall x\ P(x)$ depende sólo de quien es el "universo de discurso", en dónde toma valores la variable x, y de la estructura lógica del predicado $P(x)$.

Evidentemente si el "universo de discurso" sólo tiene un número finito de valores $x_1, x_2, \ldots, x_n$, entonces $\forall x\ P(x)$ coincide con la proposición

$$P(x_1) \wedge P(x_2) \wedge \ldots \wedge P(x_n),$$

proposición que es verdadera si y sólo si lo es cada una de las proposiciones $P(x_i)$, con $1 \leq i \leq n$.

Muchas afirmaciones matemáticas afirman que existe un elemento con una cierta propiedad; por ejemplo "existe al menos un ángulo θ tal que $\cos\theta = \theta$". De afirmaciones como ésta también es posible (como antes) asegurar si es verdadera o falsa; es decir se tratan de proposiciones, obtenidas gracias a la partícula "existe al menos".

Definición 2.3.4 *Si $P(x)$ es un predicado, el cuantificador existencial de $P(x)$ es una proposición, que denotaremos por $\exists x\ P(x)$, que es verdadera si para algún "a", en el "universo de discurso" de la variable x, se tiene que $P(a)$ es verdadera y es falsa si para cada "a" $P(a)$ es falsa. Se lee "existe al menos un x tal que $P(x)$" o "para algún x $P(x)$". Al símbolo $\exists$ se le denomina cuantificador existencial.*

Ejemplo 2.3.5 Si el "universo de discurso" donde toma valores la variable son los números reales y tenemos el predicado $P(x)$: "$x < 13$", entonces $\exists x P(x)$ es una proposición verdadera, pues por ejemplo $P(2)$ es verdadera.

También para los números reales, si tenemos el predicado $P(x)$: "$x = x+3$", entonces $\exists x\ P(x)$ es claramente una proposición falsa.

También para los números reales el cuantificador existencial "existe al menos un x tal que $x^2 + x + 1 = 0$" es una proposición falsa. Sin embargo si el "universo de discurso" son ahora los números complejos, entonces se trata de una proposición verdadera. □

Como en el caso del cuantificador universal, el valor de verdad del cuantificador existencial depende del "universo de discurso" y de la estructura lógica del predicado.

Cuando el universo de discurso lo integran un número finito de valores $x_1, x_2, \ldots, x_n$, entonces el cuantificador existencial $\exists x\ P(x)$ coincide con la proposición $P(x_1) \vee P(x_2) \vee \ldots \vee P(x_n)$, que es verdadera si y sólo si para alguno de los valores x_i, con $1 \leq i \leq n$, $P(x_i)$ es verdadera.

En la siguiente tabla resumimos lo dicho sobre los valores de verdad de los cuantificadores universal y existencial:

Proposición	**Es verdad cuando**	**Es falsa cuando**
$\forall x P(x)$	$P(x)$ es verdad para cada x.	Al menos para un x $P(x)$ es falso.
$\exists x P(x)$	Al menos para un x $P(x)$ es verdadero.	$P(x)$ es falso cualquiera que sea el valor de x.

2.3.2 Negación de cuantificadores

La negación de cuantificadores es usual en matemáticas y aún en el lenguaje usual.

Sea la proposición "cualquier español sabe hablar inglés", que podemos simbolizarlo como: $\forall x\ P(x)$, siendo $P(x)$ el predicado "x sabe hablar inglés", y x toma valores en el universo de "los españoles". Su negación será $\neg\forall x\ P(x)$, que se corresponde con "no es cierto que todos los españoles sepan hablar inglés", o equivalentemente "existe al menos un español que no sabe hablar inglés", que simbolizamos como $\exists x\ \neg P(x)$.

Supongamos ahora que decimos "hay al menos un español que ha estado en la Luna", que podemos simbolizar como $\exists x\ P(x)$, siendo el "universo" donde x toma valores "los españoles" y el predicado $P(x)$: "x ha estado en la Luna". Su negación, $\neg\exists x\ P(x)$, es "no hay español alguno que haya estado en la Luna",

o equivalentemente "cualquiera que sea el español considerado, no ha estado en la Luna", que simbolizamos por $\forall x\ \neg P(x)$.

De forma general podemos afirmar que las proposiciones $\neg\forall x\ P(x)$ y $\exists x\ \neg P(x)$, así como las proposiciones $\neg\exists x\ P(x)$ y $\forall x\ \neg P(x)$, son, respectivamente, lógicamente equivalentes si los cuantificadores están extendidos al mismo "universo de discurso". La tabla anterior evidencia la validez de esta afirmación; pero si quisiésemos ser más formalistas podemos, por ejemplo para probar la equivalencia $\forall x\ \neg P(x) \longleftrightarrow \neg\exists x\ P(x)$, proceder así:

> Supongamos $\forall x\ \neg P(x)$ y supongamos que $\exists x\ P(x)$, así podremos tener un valor "a" tal que $P(a)$ es verdadero. Como $\forall x\ \neg P(x)$, para $x = a$ se tendrá $\neg P(a)$. Tenemos entonces $P(a) \wedge \neg P(a)$. La tautología *método de reducción al absurdo*, véase (2.1), nos asegura que $\forall x\ \neg P(x) \longrightarrow \neg\exists x\ P(x)$.
>
> Supongamos ahora que $\neg\exists x\ P(x)$. Sea a arbitrario verificando $P(a)$, por tanto $\exists x\ P(x)$. Pero entonces tenemos que $\neg\exists x\ P(x) \wedge \exists x\ P(x)$, luego $\neg P(a)$ y como a es arbitrario, concluimos que $\forall x\ \neg P(x)$ y de esta forma $\neg\exists x\ P(x) \longrightarrow \forall x \neg P(x)$.

Un razonamiento como el precedente se denomina deductivo. Sobre la deducción volveremos más tarde, dedicándole una atención preferente.

Podemos esquematizar los efectos de la negación de cuantificadores como sigue:

Negación	**Afirmación equivalente**	**La negación es verdad cuando**	**La negación es falsa cuando**
$\neg\forall x P(x)$	$\exists x \neg P(x)$	Al menos para un x $P(x)$ es falso.	$P(x)$ es verdad cualquiera que sea el valor de x.
$\neg\exists x P(x)$	$\forall x \neg P(x)$	$P(x)$ es falsa para cada x.	Al menos para un x $P(x)$ es verdad.

Hemos de observar que la actuación de cuantificadores sobre la negación, disyunción o conjunción de predicados con un mismo "universo de discurso", permite establecer cierto tipo de tautologías que son de interés. Por ejemplo, si $P(x)$ y $Q(x)$ son predicados con un mismo "universo de discurso", entonces se tienen las siguientes tautologías:

1. $\forall x P(x) \longleftrightarrow \neg[\exists x \neg P(x)]$.
2. $\forall x(P \wedge Q)(x) \longleftrightarrow (\forall x P(x)) \wedge (\forall x Q(x))$.
3. $\exists x(P \vee Q)(x) \longleftrightarrow (\exists x P(x)) \vee (\exists x Q(x))$.
4. $\forall x(p \wedge P(x)) \longleftrightarrow p \wedge (\forall x P(x))$, donde p es una proposición.

5. $\exists x(p \vee P(x)) \longleftrightarrow p \vee (\exists x P(x))$, donde p es una proposición.
6. $[\forall x P(x) \vee \forall x Q(x)] \longrightarrow [\forall x((P \vee Q)(x))]$.
7. $[\exists x((P \wedge Q)(x)] \longrightarrow [(\exists x P(x)) \wedge (\exists x Q(x))]$.

Veamos algunas de ellas, dejando las restantes para realizarlas como ejercicios, una vez se haya visto la sección 2.4.2 sobre "argumentos y reglas de inferencia.

1

$$\begin{array}{lll} \neg[\exists x \neg P(x)] & \longleftrightarrow & \neg[\neg \forall x \neg \neg P(x)] \quad \text{Negación del cuant. univ.} \\ & \longleftrightarrow & \forall x P(x) \quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \text{Doble negación} \end{array}$$

2 Veamos que $(\forall x P(x)) \wedge (\forall x Q(x)) \longrightarrow \forall x(P \wedge Q)(x)$ es una tautología.

Al ser una implicación sólo hemos de ver que de la verdad del antecedente se sigue la verdad del consecuente. Sea pues $(\forall x P(x)) \wedge (\forall x Q(x))$ verdadero y "a" un elemento arbitrario del "universo de discurso", entonces $P(a) \wedge Q(a)$ es verdadero, luego $(P \wedge Q)(a)$ es verdadero y "a" es arbitrario, luego $\forall x(P \wedge Q)(x)$ es verdadero. Así la implicación es una tautología. Análogamente se puede probar que la implicación recíproca también es una tautología.

Como antes, al ver las equivalencias lógicas de la negación de los cuantificadores, estamos efectuando una deducción que es "correcta" por apoyarse en ciertas "reglas de inferencia" que son válidas y que hemos utilizado, aunque no se hayan explicitado. Pero éste es un tema en el que, como ya anunciamos, nos detendremos posteriormente. Por el momento, y sin que sirva de precedente, apelamos al "sentido común" del lector para que acepte como válido aquél razonamiento que no repugne a su inteligencia[1].

2.3.3 Cuantificación múltiple

Ya hemos indicado con anterioridad que con frecuencia, en matemáticas, aparecen enunciados con varias variables. Si $x_1, x_2, \ldots, x_n$ son variables que toman valores en un cierto universo de discurso, un predicado de estas n variables, que denotamos por $P(x_1, x_2, \ldots, x_n)$, es un enunciado que para cada sistema de valores concretos, $a_1, a_2, \ldots, a_n$, de las variables, la expresión $P(a_1, a_2, \ldots, a_n)$ es una proposición.

Si fijamos $n - 1$ valores, por ejemplo para $2 \leq i \leq n$, obtenemos un predicado $P(x_1, a_2, \ldots, a_n)$ de una variable x_1. Resulta de este modo que

[1] Tras la sección que dedicamos a la *deducción* podrá probarse rigurosamente la validez de los anteriores razonamientos. Esperamos que el lector no entienda que es válido todo aquello que no es contrario a nuestro subjetivo sentido común.

$\exists x_1 P(x_1, a_2, \ldots, a_n)$ y $\forall x_1 P(x_1, a_2, \ldots, a_n)$ son proposiciones. De este modo los enunciados $\exists x_1 P(x_1, x_2, \ldots, x_n)$ y $\forall x_1 P(x_1, x_2, \ldots, x_n)$ pueden interpretarse como predicados de $n-1$ variables.

Con frecuencia nos encontramos con expresiones matemáticas que involucran múltiples cuantificadores de funciones proposicionales de más de una variable, por lo que resulta importante saber si el orden de los mismos tiene importancia.

Ejemplo 2.3.6 Sea $P(x, y)$ el predicado "$x + y = 2$", con x e y números reales. Consideremos ahora las proposiciones "$\exists y \forall x P(x, y)$" y "$\forall x \exists y P(x, y)$". La primera nos dice que "existe al menos un número real y tal que cualquiera que sea el número real x considerado se tiene que $x+y = 2$", lo que es claramente falso. La segunda nos dice que "cualquiera que sea el número real x considerado, existe un número real y tal que $x + y = 2$", lo que es verdadero ($y = 2 - x$). Consecuentemente ambas proposiciones no son lógicamente equivalentes y así el orden de los cuantificadores es de gran importancia. □

Puede probarse, y lo dejamos como ejercicio para el lector, que los cuantificadores universales sí conmutan entre sí, al igual que lo hacen los existenciales. Así, por ejemplo, para predicados con dos variables, son tautologías:

1. $\forall x \forall y P(x, y) \longleftrightarrow \forall y \forall x P(x, y)$.
2. $\exists x \exists y P(x, y) \longleftrightarrow \exists y \exists x P(x, y)$.

Para predicados con dos variables, podemos resumir la actuación de los cuantificadores en la siguiente tabla:

Afirmación	**Es verdad cuando**	**Es falsa cuando**
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x, y)$ es verdadera cualesquiera que sean x e y.	Al menos para un par de valores x, y $P(x, y)$ es falsa.
$\exists x \forall y P(x, y)$	Existe un x tal que $P(x, y)$ es verdadera cualquiera que sea y.	Para cada x al menos hay un y para el que $P(x, y)$ es falsa.
$\forall x \exists y P(x, y)$	Para cada x al menos hay un y de forma que $P(x, y)$ es verdadera.	Existe un x tal que $P(x, y)$ es falsa para cualquier y.
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$	Existe un par x, y para el que $P(x, y)$ es verdad.	$P(x, y)$ es falsa cualesquiera que sean x e y.

Ejercicios

1. Sea $P(x)$ el predicado "$x \leq 4$". ¿Cuáles son los valores de verdad de las siguientes proposiciones?:

(a) $P(0)$.

(b) $P(4)$.

(c) $P(6)$.

2. ¿Qué quieren decir las siguientes fórmulas?, ¿son verdaderas o falsas?

   (a) $\forall x\ (x^2 \geq 0)$, donde el universo de discurso es el conjunto de los números reales.

   (b) $\exists x\ (x^2 - 2x + 3 = 0)$, con universo nuevamente los reales.

   (c) $\exists x\ (H(x) \wedge M(x))$, donde el universo de discurso lo forman todos los humanos, $H(x)$ es la afirmación "x es un hombre" y $M(x)$ es "x es moreno".

   (d) $\forall x\ (H(x) \longrightarrow M(x))$, en las mismas condiciones del caso anterior.

   (e) $\forall x\ G(x, y)$, donde el universo es el mismo del caso anterior y $G(x, y)$ es el predicado "a x le gusta y".

3. ¿Qué significan las siguientes fórmulas?, ¿son verdaderas o falsas? El universo de discurso en cada caso es $\mathbb{N}$, conjunto de todos los números naturales.

   (a) $\forall x \exists y (x < y)$.

   (b) $\exists y \forall x (x < y)$.

   (c) $\exists x \forall y (x < y)$.

   (d) $\forall y \exists x (x < y)$.

   (e) $\exists x \exists y (x < y)$.

   (f) $\forall x \forall y (x < y)$.

4. Analizar la forma lógica de las siguientes afirmaciones y expresarlas simbólicamente, siendo el universo de discurso los números naturales:

   (a) x es un cuadrado perfecto.

   (b) x es múltiplo de y.

   (c) x es primo.

   (d) x es el menor número que es a la vez múltiplo de y y de z.

5. Analizar la forma lógica de las siguientes afirmaciones y expresarlas simbólicamente, siendo el universo de discurso los números reales:

   (a) El elemento neutro para la suma es el 0.

   (b) Cualquier número real tiene un inverso respecto de la adición.

   (c) Los números negativos no tienen raíz cuadrada.

   (d) Cualquier número positivo tiene exactamente dos raíces cuadradas.

6. Supongamos que el universo de discurso de la función proposicional $P(x, y)$ consiste en pares (x, y) donde tanto x como y pueden tomar sólo los valores 1, 2 y 3. Escribir las siguientes proposiciones usando la conjunción y la disyunción:

   (a) $\exists x\ P(x, 3)$.

   (b) $\forall x\ \forall y\ P(x, y)$.

   (c) $\exists x\ \forall y\ P(x, y)$.

   (d) $\forall y\ P(1, y)$.

   (e) $\exists x\ \exists y\ P(x, y)$.

   (f) $\forall y\ \exists x\ P(x, y)$.

7. Demostrar que las proposiciones siguientes tienen los mismos valores de verdad:

   (a) $\neg\exists x\ \forall y P(x, y)$ y $\forall x\ \exists y\ \neg P(x, y)$.

   (b) $\forall x\ (P(x) \wedge Q(X))$ y $\forall x P(x)\ \wedge\ \forall x Q(x)$.

   (c) $\exists x\ (P(x) \vee Q(x))$ y $\exists x P(x) \vee \exists x Q(x)$.

8. Establecer las siguientes equivalencias lógicas, donde A es una proposición que no tiene cuantificadores:

   (a) $(\forall x P(x)) \wedge A$ y $\forall x(P(x) \wedge A)$.

   (b) $(\exists P(x)) \wedge a$ y $\exists x(P(x) \wedge A)$.

   (c) $\forall x(A \vee P(x)) \longleftrightarrow A \vee (\forall x P(x))$.

   (d) $A \vee (\exists x P(x)) \longleftrightarrow \exists x(A \vee P(x))$.

9. Probar que las siguientes implicaciones son falsas:

   (a) $[\forall x(P \vee Q)(x)] \longrightarrow [\forall x P(x) \vee \forall x Q(x)]$.

   (b) $[\exists x P(x) \wedge \exists x Q(x)] \longrightarrow [\exists x(P \wedge Q)(x)]$.

10. Demostrar que $\exists x P(x) \wedge \exists x Q(x)$ y $\exists x(P(x) \wedge Q(x))$ no son lógicamente equivalentes.

11. Demostrar que $\forall x P(x) \wedge \exists x Q(x)$ y $\forall x \exists y(P(x) \wedge Q(y))$ son equivalentes, donde la nueva variable y se usa para combinar de forma adecuada los cuantificadores.

12. Si denotamos mediante $\exists! x$ la proposición *existe un único x tal que $P(x)$ es verdadero*, ¿cuáles son los valores de verdad de las siguientes afirmaciones?:

   (a) $\exists! x P(x) \longrightarrow \exists x P(x)$.

   (b) $\forall x P(x) \longrightarrow \exists! x P(x)$.

   (c) $\exists! x \neg P(x) \longrightarrow \neg\forall x P(x)$.

13. Expresar el cuantificador $\exists! x P(x)$ usando los cuantificadores universal y existencial y los *juntores* (conectivos lógicos).

14. Sea $f : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $\lim_{x \longrightarrow a} f(x) = b$. Recordemos que ello significa que para cualquier número real $\epsilon > 0$ existe un número real $\delta > 0$ tal que $|f(x) - b| < \epsilon$, cuando $0 < |x - a| < \delta$.

    (a) Expresar simbólicamente esta definición.

    (b) Expresar simbólicamente que $\lim_{x \longrightarrow a} f(x) \neq b$ y explicar qué significa.

    (c) ¿Es cierto que si no existe $\lim_{x \longrightarrow a} f(x)$, entonces cualquiera que sea $b \in \mathbb{R}$ existe un número real $\epsilon > 0$ tal que cualquiera que sea el número real $\delta > 0$, si $|x - a| > \delta > 0$, entonces $|f(x) - b| > \epsilon$? Contestar razonadamente.

15. Sea $(a_n)_n$ una sucesión de números reales que es de Cauchy. Ello significa que para cualquier número real $\epsilon > 0$ existe $n_0 \in \mathbb{N}$ tal que $|a_p - a_q| < \epsilon$, cualesquiera que sean $p, q \in \mathbb{N}$ con $p \geq q \geq n_0$.

    (a) Expresar simbólicamente esta definición.

    (b) Explicar qué significa y expresar simbólicamente que la sucesión $(a_n)_n$ no es de Cauchy.

    (c) ¿Es cierto que si $(a_n)_n$ no es de Cauchy, existe un número real $\epsilon > 0$ tal que es posible construir una sucesión $(n_k)_k$ de índices no decreciente $(1 \leq n_1 \leq n_2 \leq \ldots \leq n_k \ldots)$ tal que $|a_{n_{i+1}} - a_{n_i}| > \epsilon$ para cada $i \in \mathbb{N}$? Contestar razonadamente.

16. Sea $\sum_{n=1}^{\infty} a_n$ una serie de números reales convergente y sea $(s_n)_n$, con $s_n = \sum_{i=1}^{n} a_i$ la sucesión de sus sumas parciales. Ello significa que para cualquier número real $\epsilon > 0$ existe $n_0 \in \mathbb{N}$ tal que $|s_p - s_q| < \epsilon$, cualesquiera que sean $p, q \in \mathbb{N}$ con $p \geq q \geq n_0$ (*criterio de Cauchy*).

    (a) Expresar simbólicamente esta definición.

    (b) Explicar qué significa y expresar simbólicamente que la serie anterior no es convergente (partiendo de la caracterización de una serie convergente por el *criterio de Cauchy*).

    (c) ¿Es cierto que si $\sum_{n=1}^{\infty} a_n$ no es convergente, existe un número real $\epsilon > 0$ tal que es posible construir una sucesión $(n_k)_k$ de índices no decreciente $(1 \leq n_1 \leq n_2 \leq \ldots \leq n_k \ldots)$ tal que $|\sum_{j=n_i+1}^{n_{i+1}} a_j| > \epsilon$ para cada $i \in \mathbb{N}$? Contestar razonadamente.

17. Un punto $x \in \mathbb{R}$ se dice de adherencia de un conjunto $A \subseteq \mathbb{R}$ y se denota mediante $x \in \overline{A}$ si cualquiera que sea $\varepsilon > 0$ existe un punto $a \in A$ tal que $|x - a| < \varepsilon$. Expresar simbólicamente esta definición. Expresar simbólicamente y explicar que $x \notin \overline{A}$.

2.4 Deducción. Terminología matemática

2.4.1 Definiciones

Desde los estudios de bachillerato los alumnos están habituados a ver *definiciones* y *teoremas*, éstos y otros términos matemáticos los encontrará continuamente el lector que quiera asomarse al mundo de las matemáticas. Vamos pues a precisar el significado de los mismos.

Una definición no es más que una declaración sobre objetos o propiedades de objetos matemáticos que es aceptada por la comunidad de matemáticos. Ya hemos topado con algunas definiciones, por ejemplo, lo que significa que p *implica* q sea verdadero; concretamente se dijo que la *implicación* sólo es falsa cuando el antecedente es verdadero y el consecuente es falso. Cualquiera es libre de aceptar o no esta definición, pero si no la acepta y define como *implicación* otra cosa, puede que nadie le entienda.

No obstante hemos de advertir que una definición no es una declaración caprichosa, por el contrario recoge usualmente un concepto matemático que se reiterará con frecuencia y permite referirnos a él con mayor comodidad. Por ejemplo, "se dice que un número entero es *primo* si es un entero positivo mayor que uno y no es divisible por otro entero positivo mayor que uno y menor que él mismo"; evidentemente es más económico, más sencillo y más claro hablar de que el número p es primo que decir que "p es un entero positivo ..."

2.4.2 Argumentos y reglas de inferencia

En matemáticas se hace uso continuo del *razonamiento deductivo* o *argumento deductivo* o *demostración*, consistente en un conjunto finito de enunciados o proposiciones, una de ellas llamada *conclusión*, que se sigue de las otras llamadas *premisas*. La forma de derivar de las *premisas* a la *conclusión* se hace mediante las *reglas de inferencia*.

Si bien los argumentos deductivos constan de proposiciones no son como éstas verdaderos o falsos, sino bien construidos o mal construidos, *correctos* o *incorrectos*, *válidos* o *no válidos*.

No obstante, utilizando el concepto de verdad o falsedad cabe definir un argumento válido como un conjunto de enunciados tal que no es posible que las premisas sean verdaderas y la conclusión sea falsa, de modo que escrita como fórmula lógica resulta una tautología; o lo que es lo mismo, en un argumento bien construido la verdad de las premisas es incompatible con la falsedad de la conclusión.

Observemos que no estamos excluyendo la posibilidad de argumentos que

tengan una o más premisas falsas y conclusión falsa y no obstante sean correctos.

Ejemplo 2.4.1

- España tiene más población que Estados Unidos
- Estados Unidos tiene más población que Alemania

luego

- España tiene más población que Alemania

□

Tampoco estamos excluyendo argumentos cuyas premisas contengan alguna falsedad, pero cuya conclusión sea verdadera y sin embargo sean correctos.

Ejemplo 2.4.2

- España tiene menos población que Estados Unidos
- Estados Unidos tiene menos población que Alemania

luego

- España tiene menos población que Alemania

□

Cuando todas las proposiciones usadas en un argumento válido son verdaderas, se llega a una proposición verdadera (si se han usado correctamente las reglas de inferencia). No obstante un argumento válido puede conducir a una proposición falsa si una o más aserciones falsas son utilizadas en el argumento.

Ejemplo 2.4.3

- Si 101 es divisible por 3, entonces 101^2 es divisible por 9
- 101 es divisible por 3

luego

- 101^2 es divisible por 9.

Sea p la proposición "101 es divisible por 3" y q la proposición "101^2 es divisible por 9". El argumento que tenemos responde esquemáticamente a:

$$\begin{array}{l} p \longrightarrow q \\ p \\ \hline q \end{array}$$

la proposición $p \longrightarrow q$ es verdadera, pero p es falsa. El argumento está basado correctamente en la regla de inferencia *Modus Ponens*, que inmediatamente veremos, pero la conclusión es falsa. □

Como ya hemos indicado las reglas de inferencia son las reglas que gobiernan las operaciones deductivas, son las reglas de transformación de fórmulas y proporcionan los esquemas válidos de razonamiento independientemente de la verdad o falsedad de las proposiciones componentes y se corresponden con tautologías. Las reglas se esquematizan escribiendo una serie de fórmulas separadas por una línea horizontal que señala el tránsito de los antecedentes al resultado

de la deducción.

Ejemplo 2.4.4

– Si llueve, llevo paraguas
– Hoy llueve
luego
– llevo paraguas

Llamando p a la proposición "llueve" y q a "llevo paraguas", el argumento puede esquematizarse como sigue:

$$\frac{\begin{array}{l} p \longrightarrow q \\ p \end{array}}{q}$$

También puede representarse así:

$$p \longrightarrow q,\ p \vdash q$$

donde el símbolo $\vdash$ recibe el nombre de deductor, de forma que a la izquierda del deductor se escriben las premisas separadas unas de otras por comas y a la derecha del deductor se escribe la conclusión. □

Las fórmulas que aparecen encima de la línea horizontal (o delante del deductor) reciben el nombre de *premisas* de la regla de inferencia, y la fórmula que hay debajo de la línea horizontal (o detrás del deductor) recibe el nombre de la *conclusión* de la regla de inferencia. En toda regla el orden de las premisas es indiferente.

A continuación indicamos las reglas básicas del *cálculo proposicional*, dejando como ejercicio al lector que establezca y pruebe las correspondientes tautologías. Por ejemplo, la tautología correspondiente a la regla de "introducción del negador" (IN) es $[p \longrightarrow (q \wedge \neg q)] \longleftrightarrow \neg p$.

Con la notación

$$\begin{array}{|l} A \\ \vdots \\ B \end{array}$$

indicamos que a partir de la fórmula A llegamos, mediante una sucesión finita de pasos, a la fórmula B.

1. Reglas de introducción

   - Implicador (II)

$$\frac{\begin{array}{|l} p \\ \vdots \\ q \end{array}}{p \longrightarrow q}$$

- Conjuntor (IC)

$$\frac{\begin{array}{c}p\\q\end{array}}{p \wedge q}$$

- Disyuntor (ID)

$$\frac{p}{p \vee q} \qquad \frac{q}{p \vee q}$$

- Negador (IN)

$$\frac{\begin{array}{|l}p\\ \vdots\\ q \wedge \neg q\end{array}}{\neg p}$$

2. Reglas de eliminación

- Implicador (EI) o *Modus ponens*

$$\frac{\begin{array}{c}p \longrightarrow q\\p\end{array}}{q}$$

- Conjuntor (EC)

$$\frac{p \wedge q}{p} \qquad \frac{p \wedge q}{q}$$

- Disyuntor (ED)

$$\frac{\begin{array}{l}p \vee q\\ \begin{array}{|l}p\\ \vdots\\ r\end{array}\\ \begin{array}{|l}q\\ \vdots\\ r\end{array}\end{array}}{r}$$

- Negación (EN) $\dfrac{\neg\neg p}{p}$

Algunas otras reglas de inferencia derivadas de éstas, pero muy usuales son:

1. *Modus tollens*

$$\frac{\begin{array}{c}p \longrightarrow q\\ \neg q\end{array}}{\neg p}$$

No es otra que la proposición contrarrecíproca, como ya sabemos, y que se corresponde con la tautología $[\neg q \wedge (p \longrightarrow q)] \longrightarrow \neg p$.

2. *Silogismo hipotético*

$$\frac{\begin{array}{c} p \longrightarrow q \\ q \longrightarrow r \end{array}}{p \longrightarrow r}$$

y se corresponde con la tautología $[(p \longrightarrow q) \wedge (q \longrightarrow r)] \longrightarrow (p \longrightarrow r)$.

3. *Silogismo disyuntivo*

$$\frac{\begin{array}{c} p \vee q \\ \neg p \end{array}}{q}$$

y se corresponde con la tautología $[(p \vee q) \wedge \neg p] \longrightarrow q$

Hay muchos argumentos en los que aparecen cuantificadores, por ejemplo:

– Todo gaditano es andaluz.
– Todo andaluz es español.
luego
– Todo gaditano es español.

El cuantificador universal "todo" interviene en las premisas del razonamiento anterior. A continuación veremos las reglas que gobiernan la deducción cuando intervienen cuantificadores (*cálculo de predicados*). En la sección 2.3.2 ya se puso en evidencia la necesidad de conocer qué reglas de inferencia son válidas cuando aparecen cuantificadores, por ejemplo cuando se vio que

$$\forall x \neg P(x) \longleftrightarrow \neg \exists x P(x).$$

El procedimiento en el cálculo de cuantores se reduce a:

1. Abrir las fórmulas cerradas por cuantificadores, suprimiendo éstos.
2. Aplicar las reglas del cálculo proposicional a las fórmulas anteriormente resultantes.
3. Volver a poner los cuantificadores suprimidos.

Las reglas básicas del *cálculo de predicados o cuantificacional* son las siguientes:

- Introducción del generalizador (IG)

$$\frac{P(a)}{\forall x P(x)}$$

Con la condición de que "a" no puede ocurrir en ningún supuesto previo que no esté cancelado.

- Eliminación del generalizador (EG)

$$\frac{\forall x P(x)}{P(a)}$$

- Introducción del particularizador (IP)

$$\frac{P(a)}{\exists x P(x)}$$

- Eliminación del particularizador (EP)

$$\frac{\begin{array}{l}\exists x P(x) \\ \left[\begin{array}{l} P(a) \\ \vdots \\ Q \end{array}\right.\end{array}}{Q}$$

Con la condición de que "a" no debe ocurrir en $\exists x P(x)$, en Q ni en supuesto alguno previamente no cancelado.

Ejemplo 2.4.5 Deduzcamos formalmente que $\neg\exists P(x) \longrightarrow \forall x \neg P(x)$. Para ello procedemos como se indica en el esquema siguiente:

–	1	$\neg\exists x P(x)$	
⌐	2	$P(a)$	
|	3	$\exists x P(x)$	IP 2
⌙	4	$\neg\exists x P(x) \wedge \exists x P(x)$	IC 1,3
	5	$\neg P(a)$	IN 2 a 4
	6	$\forall x \neg P(x)$	IG 5

□

Aplicando cuidadosamente las anteriores reglas de inferencia se podrán efectuar deducciones en las que intervengan los cuantificadores. Este es un buen momento para abordar las propuestas realizadas en la sección 2.3.2.

2.4.3 Falacias

Las *falacias* parecen reglas de inferencia pero están basadas en contingencias y no en tautologías. Vemos a continuación algunas muy usuales (tal vez no

en situaciones tan simples como las que se presentan en los ejemplos, pero con idéntica estructura) para mostrar la distinción entre un razonamiento correcto y otro incorrecto:

Falacia de afirmación de la conclusión

La proposición $[(p \longrightarrow q) \wedge q] \longrightarrow p$ no es una tautología, pues no es verdad en todos los casos.

p	q	$p \longrightarrow q$	$(p \longrightarrow q) \wedge q$	$[(p \longrightarrow q) \wedge q] \longrightarrow p$
V	V	V	V	V
V	F	F	F	V
F	V	V	V	F
F	F	V	F	V

No obstante, a veces, se usan argumentos incorrectos que tratan esta proposición como una tautología. Este tipo de razonamiento incorrecto lo denominaremos *falacia de afirmación de la conclusión.*

Ejemplo 2.4.6 ¿Es correcto el siguiente razonamiento?: "Si hago cualquier problema propuesto en clase, entonces aprobaré la asignatura. Apruebo la asignatura, luego hice cualquier problema propuesto en clase".

Si llamamos p a "hago cualquier problema propuesto en clase" y q a "apruebo la asignatura", el argumento anterior tiene la siguiente forma:

$$\begin{array}{l} p \longrightarrow q \\ q \\ \hline p \end{array}$$

que como acabamos de ver no se corresponde con una tautología sino con una contingencia. □

Ejemplo 2.4.7 Sean p y q, respectivamente las proposiciones siguientes: "5 es divisor de $n-1$" y "5 es divisor de n^2-1". La proposición "Si 5 es divisor de $n-1$ entonces 5 es divisor de n^2-1" $(p \longrightarrow q)$ es verdadera. Si q es verdadera, es decir, si "5 es divisor de n^2-1" es verdadera, ¿de aquí se deduce que "5 es divisor de $n-1$" (es decir, que p es verdadera)?

No, ya que de ser 5 divisor de n^2-1 se deduce que 5 es divisor de $n+1$ o de $n-1$, pero no necesariamente de este último. Este tipo de argumento se corresponde exactamente con el mismo esquema que el del ejemplo anterior. □

Falacia de negación de la hipótesis

La proposición $[(p \longrightarrow q) \wedge \neg p] \longrightarrow \neg q$ no es una tautología, ya que es falsa cuando q es verdadera y p es falsa, como puede comprobarse. Muchos argumen-

tos usan incorrectamente esta falsa regla de inferencia, que recibe el nombre de *falacia de negación de la hipótesis.*

Ejemplo 2.4.8 Si consideramos p y q como en el ejemplo 2.4.6, el esquema de razonamiento siguiente:

$$\begin{array}{l} p \longrightarrow q \\ \neg p \\ \hline \neg q \end{array}$$

es una falacia. Es posible aprobar la asignatura sin hacer todos los problemas propuestos en clase. □

Ejemplo 2.4.9 Sean p y q las proposiciones del ejemplo 2.4.7. El siguiente argumento:

– Si 5 es divisor de $n-1$ entonces 5 es divisor de n^2-1
– 5 no es divisor de $n-1$
luego
5 no es divisor de n^2-1

¿es correcto?

Claramente es una falacia, con análogo esquema que la del ejemplo 2.4.7, toda vez que $n-1$ puede no ser múltiplo de 5 y sin embargo $(n-1)(n+1)$ puede serlo, como consecuencia de poder ser $n+1$ múltiplo de 5. □

Falacia del razonamiento circular

Este tipo de argumentación incorrecta sucede cuando uno o más pasos de la demostración están basados en la verdad de las afirmaciones que están siendo probadas; es decir, cuando para demostrar una afirmación se usa la propia afirmación u otra equivalente a ella.

Ejemplo 2.4.10 Tratemos de probar que si n^2 es un número entero impar, entonces n es un entero impar.

El argumento en cuestión sería de la forma siguiente: "supongamos que n^2 es impar, entonces para algún entero m se tendrá que $n^2 = 2m+1$. Sea $n = 2i+1$, para algún entero i, luego n es impar. Este razonamiento es claramente incorrecto pues introduce como premisa aquello que se quiere demostrar. □

Hemos de notar que el razonamiento incorrecto sigue siéndolo aunque la conclusión sea cierta. Por simplicidad en los ejemplos anteriores hemos presentado casos donde reglas de inferencia incorrectas proporcionaban conclusiones falsas. Ahora bien, podría darse que obtuviésemos una conclusión verdadera haciendo uso de una falacia, en este caso el argumento deductivo sigue siendo incorrecto y no se habría demostrado que la conclusión se deriva de las premisas dadas; por así decirlo el teorema aún estaría sin demostrar.

2.4.4 Axiomas y teoremas

Un término que encontramos usualmente en matemáticas es el de *proposición*[2]. Por *proposición* matemática entendemos un enunciado o afirmación matemática que puede demostrarse que es verdadero. Demostrar una *proposición*, como acabamos de indicar, consiste en hacer ver que la misma es consecuencia lógica y necesaria de ciertas proposiciones previamente establecidas, que a su vez deben haber sido probadas y así sucesivamente. El proceso de demostración sería de esta manera una labor de regresión infinita, evidentemente imposible, salvo que haya un punto inicial de partida, del que ya no podamos retroceder. Este punto de partida está formado por una serie de proposiciones llamadas *axiomas* o *postulados*, que son aceptados como verdaderos sin necesidad de demostración. Por tanto, las afirmaciones usadas en una demostración incluyen *axiomas* o *postulados*, las hipótesis del teorema a demostrar y los teoremas previamente demostrados.

Cuando los resultados de un campo científico se secuencian en orden lógico, de suerte que es posible deducirlos de unos cuantos axiomas previamente elegidos con "buen criterio", entonces decimos que la teoría en cuestión se presenta de forma axiomática. La elección de los axiomas no es del todo arbitraria, sino que obedece a la necesidad de sustentar toda la teoría en un número reducido de asertos que en alguna medida son validados por nuestra intuición acerca de los objetos matemáticos de la teoría. Conviene que estos axiomas sean pocos y sencillos, pero sobre todo el sistema de axiomas debiera ser *consistente* (no deben deducirse de ellos dos teoremas mutuamente contradictorios, es decir no debiera deducirse en el sistema p y $\neg p$) y *completo* (en el sentido de que todo teorema de la teoría fuese deducible a partir de ellos)[3]; por último es deseable, aunque no imprescindible, que los axiomas sean *independientes* (es decir, ninguno de ellos debiera deducirse de los restantes).

Ejemplo 2.4.11 El primer ejemplo de sistema axiomático nos lo proporciona *Euclides* en su obra maestra los *Elementos*. Allí establece los cinco *postulados* siguientes:

1. Desde cualquier punto a cualquier otro se puede trazar una recta.
2. Toda recta limitada puede prolongarse indefinidamente en la misma dirección.
3. Con cualquier centro y cualquier radio se puede trazar una circunferencia.
4. Todos los ángulos rectos son iguales entre sí.
5. Si una recta, al cortar a otras dos, forma de un mismo lado ángulos internos menores que dos rectos, esas dos rectas prolongadas indefinidamente se

[2] Hay que distinguir entre el concepto de proposición matemática y el de proposición lógica.

[3] Estas cuestiones son bastante más complejas de lo que aparentemente pueden parecer y a ellas dedicaremos unas líneas en el Epílogo.

cortan del lado en que están los ángulos menores que dos rectos.

éste último se conoce con el nombre de *postulado de las paralelas* y ha sido origen de apasionantes trabajos y desarrollo de nuevas teorías en matemáticas. □

Algunas *proposiciones* matemáticas son consideradas especialmente importantes y se denominan *teoremas*.

Ejemplo 2.4.12 "Cualquier número entero positivo n se puede descomponer en producto de factores primos, siendo esta descomposición única salvo en el orden de los factores".

Este es el conocido *Teorema Fundamental de la Aritmética* □

Las demostraciones de ciertos *teoremas* y de ciertas *proposiciones* pueden ser muy largas y su lectura puede resultar farragosa, conviniendo separar la demostración de ciertas partes utilizadas en la deducción como *proposiciones* independientes, de carácter técnico, que serán usadas en la demostración del *teorema* en cuestión. Este tipo de *proposición* simple usada en la demostración de otra *proposición* o *teorema* recibe el nombre de *lema*.

Ejemplo 2.4.13 **Lema:** Sea $a = bq + r$ con a, b q y r números enteros, entonces el máximo común divisor de a y b y el máximo común divisor de b y r coinciden.

Este *lema* se utiliza para demostrar que el *Algoritmo de Euclides* proporciona el máximo común divisor de dos números. □

Una vez establecido un *teorema* ciertas *proposiciones* pueden establecerse directamente a partir de aquél, recibiendo el nombre de *corolarios*.

Ejemplo 2.4.14 **Teorema:** Si $P(x)$ es un polinomio y a es un número real, entonces $\lim_{x\to a} P(x) = P(a)$.

Corolario: Si $R(x)$ es una función racional y a es un número real que pertenece al dominio de $R(x)$, entonces

$$\lim_{x\to a} R(x) = R(a).$$

En efecto sea $R(x) = \dfrac{P(x)}{Q(x)}$, donde $P(x)$ y $Q(x)$ son polinomios, como a pertenece al dominio de la función, entonces $Q(a) \neq 0$. Dado que estamos ante el límite de un cociente y en virtud del teorema anterior, concluimos que

$$\lim_{x\to a} R(x) = \frac{\lim_{x\to a} P(x)}{\lim_{x\to a} Q(x)} = \frac{P(a)}{Q(a)} = R(a).$$

□

Así como existen proposiciones matemáticas que se aceptan sin una demostración formal (los axiomas), también existen conceptos matemáticos que no

son definidos, son los *conceptos primitivos* de la teoría. Así, por ejemplo, en la axiomática moderna de la geometría, los conceptos de *punto* y *recta* son conceptos primitivos. En la teoría axiomática de conjuntos, a la que se hará referencia en el próximo capítulo, el concepto de *conjunto* y el de *pertenencia* son conceptos primitivos de esta teoría.

Los conceptos primitivos de una teoría aparecen como elementos que satisfacen ciertos axiomas; es decir, se definen por sus propiedades, por las relaciones que entre ellos establece la axiomática.

2.4.5 Métodos de demostración de teoremas

Muchos teoremas son implicaciones. Las técnicas para demostrar una implicación son importantes y a ello dedicaremos unas cuantas consideraciones a continuación.

Recordemos que $p \longrightarrow q$ es falso únicamente si p es verdadero y q es falso. Por tanto para demostrar que $p \longrightarrow q$ sólo se necesita demostrar que q es verdadero si p es verdadero.

Demostración vacía

Si la hipótesis p es falsa, entonces $p \longrightarrow q$ es verdadera siempre, pues $F \longrightarrow V$ y $F \longrightarrow F$, son verdaderas siempre, donde V y F indican, respectivamente, proposiciones que son verdaderas y falsas. Por tanto, si podemos demostrar que p es falsa ya estará demostrado que $p \longrightarrow q$, lo que denominaremos *demostración vacía*. Esta situación puede presentarse al establecer casos particulares de teoremas que afirman que una implicación es verdadera para cualquier entero positivo: "$\forall n\ P(n)$", siendo $P(n)$ una función proposicional.

Ejemplo 2.4.15 Sea n un número natural y $P(n)$: "si n es primo mayor que 2, entonces $n+1$ es compuesto". Demostrar que $P(4)$ es verdadera: "si 4 es primo y $4 > 2$ entonces 5 es compuesto".

$4 > 2$ y 4 es primo es falsa, luego $P(4)$ es verdadera. □

Demostración trivial

Si q es verdadera, entonces $p \longrightarrow q$ es verdadera. Luego demostrando que q es verdadera se habrá demostrado $p \longrightarrow q$.

Ejemplo 2.4.16 Sea $P(n)$ "si a es un número real positivo tal que $0 < a < 1$, entonces $(1+a)^n \geq 1 + na$". Demostremos que $P(0)$ es verdadera.

$P(0)$ es "si $0 < a < 1$, entonces $(1+a)^0 \geq 1 + 0 \cdot a$". Ya que $(1+a)^0 = 1 + 0 \cdot a = 1$, la conclusión de $P(0)$ es verdadera y por tanto $P(0)$ es verdadera

trivialmente. Hemos de observar que la hipótesis de la implicación $(0 < a < 1)$ no se ha usado en la demostración. □

Este tipo de demostración suele presentarse en una demostración por casos (que veremos posteriormente en este mismo epígrafe) y en el proceso de demostración denominado *inducción matemática* que se estudiará en el capítulo 7.

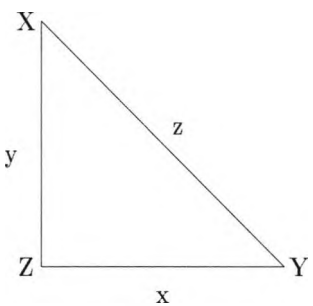
Demostración directa

Si p es verdadera entonces q también es verdadera. Se asume que p es verdadera y se usan las reglas de inferencia y teoremas ya demostrados para probar que q también es verdadera.

Ejemplo 2.4.17 Demostremos que si n es un entero par, entonces n^2 es un entero par.

La hipótesis es "n es un entero par". Por tanto $n = 2m$ para algún entero m, de donde $n^2 = (2m)^2 = 4m^2$, luego n^2 es entero par. □

Ejemplo 2.4.18 Demostremos que si el triángulo rectángulo $\overset{\frown}{XYZ}$ de la figura



tiene de área $\frac{z^2}{4}$, entonces el triángulo es isósceles. La hipótesis es "el área es $\frac{z^2}{4}$". Coloquemos ordenadamente las premisas

$$\frac{xy}{2} = \frac{z^2}{4}. \tag{2.2}$$

Por el teorema de Pitágoras se tiene que:

$$x^2 + y^2 = z^2. \tag{2.3}$$

Sustituyendo (2.3) en (2.2), obtenemos

$$\frac{xy}{2} = \frac{x^2 + y^2}{4}, \tag{2.4}$$

de donde, mediante transformaciones algebraicas tenemos:

$$\begin{gathered} x^2 + y^2 - 2xy = 0, \\ (x-y)^2 = 0, \\ x - y = 0, \\ x = y, \end{gathered}$$

por tanto el triángulo es isósceles. □

Demostración por casos

Si deseamos demostrar una implicación de la forma $(p_1 \vee p_2 \vee \ldots \vee p_n) \longrightarrow q$, podemos tener en cuenta la tautología

$$[(p_1 \vee p_2 \vee \ldots \vee p_n) \longrightarrow q] \longleftrightarrow [(p_1 \longrightarrow q) \wedge (p_2 \longrightarrow q) \wedge \ldots \wedge (p_n \longrightarrow q)]$$

que no es otra que la generalización de la regla de inferencia de eliminación del disyuntor, por lo que la implicación original puede ser demostrada probando cada una de las n implicaciones $p_i \longrightarrow q$ individualmente. De esta forma ante una implicación $p \longrightarrow q$, si podemos obtener n proposiciones p_i tales que p y $p_1 \vee \ldots \vee p_n$ sean equivalentes, podemos demostrar la implicación mediante el procedimiento indicado de descomposición en casos.

Ejemplo 2.4.19 Demostremos que si n es un número entero positivo cualquiera y $N = n(n+2)(5n-1)(5n+1)$, entonces N es múltiplo de 8.

Sean las proposiciones:

- p: "$N = n(n+2)(5n-1)(5n+1)$ y n es entero positivo",
- q :"N es múltiplo de 8",
- p_1: "$N = n(n+2)(5n-1)(5n+1)$ y n es par",
- p_2: "$N = n(n+2)(5n-1)(5n+1)$ y n es impar".

Desde luego $p \longleftrightarrow (p_1 \vee p_2)$, ya que n es par o impar. Demostrar que $p \longrightarrow q$ se puede hacer probando que $p_1 \longrightarrow q$ y que $p_2 \longrightarrow q$. En efecto:

- $p_1 \longrightarrow q$
  Si n es par entonces n y $n+2$ son pares consecutivos, por lo que uno ha de ser múltiplo de 2 y el otro múltiplo de 4, de donde se deduce que su producto es múltiplo de 8 y, de este modo, N también es múltiplo de 8.

- $p_2 \longrightarrow q$
  Si n es impar, entonces $5n-1$ y $5n+1$ son pares consecutivos, por lo que uno es múltiplo de 2 y el otro lo es de 4, así su producto es múltiplo de 8, resultando que N también es múltiplo de 8.

Como los casos $p_1 \longrightarrow q$ y $p_2 \longrightarrow q$ son verdaderos, tenemos que también lo es $(p_1 \vee p_2) \longrightarrow q$, y toda vez que $(p_1 \vee p_2)$ equivale a p, concluimos que $p \longrightarrow q$ es verdadero. □

Demostración mediante el contrarrecíproco

Dado que $(p \longrightarrow q) \longleftrightarrow (\neg q \longrightarrow \neg p)$ es una tautología podemos utilizar el contrarrecíproco para demostrar la implicación. La demostración del contrarrecíproco podrá hacerse directamente o mediante cualquier otra técnica.

Ejemplo 2.4.20 Demostremos mediante el contrarrecíproco que "si $5n + 3$ es par entonces n es impar".

Si n es par, n=2k para algún entero k, por lo que $5n + 3 = 10k + 3 = 2(5k + 1) + 1$; de donde $5n + 3$ es impar. Así pues la implicación original es verdadera. □

Ejemplo 2.4.21 Demostremos que si n es un número entero y n^2 es par, entonces n es par.

Supongamos que n es impar, entonces $n = 2k + 1$ para algún entero k, de donde $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ y consecuentemente n^2 es impar. □

Reducción al absurdo

A veces los intentos directos de obtener una conclusión no dan resultados, entonces podemos recurrir a una demostración mediante una especie de rodeo. Consiste en:

1. Dar por supuesta la falsedad de la tesis.
2. Obtener a partir de esta suposición una contradicción: $t \wedge \neg t$.
3. Rechazar dicha suposición y por tanto afirmar la tesis.

Este método recibe el nombre de *reducción al absurdo (reductio ad absurdum)* y se fundamenta en el hecho de que una contradicción es inadmisible, correspondiéndose con la tautología $[(p \wedge \neg q) \longrightarrow (t \wedge \neg t)] \longleftrightarrow (p \longrightarrow q)$, que se vio en la sección 2.2., que no es otra cosa que la regla de inferencia de introducción del negador. Como en el caso anterior, éste es también un procedimiento de demostración indirecta de una proposición, pero con una singularidad especial: se suponen p y $\neg q$ y se llega a una contradicción $t \wedge \neg t$, mientras que en el contrarrecíproco se supone $\neg q$ y se concluye $\neg p$.

Ejemplo 2.4.22 La demostración, dada en el Capítulo 1, del Teorema 1.1.2. □

Ejemplo 2.4.23 Demostremos que $\sqrt{2}$ es un número irracional. Equivalentemente se trata de demostrar que si r es un número real tal que $r^2 = 2$, entonces r es irracional.

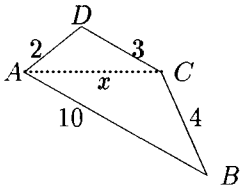


Figura 2.2: Cuadrilátero

Supongamos por el contrario que $r = \frac{p}{q}$ es un número racional, siendo $\frac{p}{q}$ irreducible. Se tiene que $r^2 = \frac{p^2}{q^2}$ y de aquí que $2q^2 = p^2$, por lo que p^2 será par. Así pues [4] $p = 2k$ para algún entero k y de aquí $2q^2 = p^2 = 4k^2$, luego $q^2 = 2k^2$, obteniéndose que q también es par; pero entonces $\frac{p}{q}$ no es irreducible, lo que conlleva una contradicción originada en nuestra suposición de que $\sqrt{2}$ era racional, concluyendo, como se pretendía, que $\sqrt{2}$ es irracional. □

Ejemplo 2.4.24 Demostremos que no existe cuadrilátero alguno cuyos lados tengan de longitud $2, 3, 4$ y 10.

Supongamos que existe un tal cuadrilátero, como se indica en la figura 2.2.

Ya Euclides demostró que cualquier lado de un triángulo es menor que la suma de los otros dos. Por tanto, en el triángulo $\widehat{ABC}$ se tiene que $10 < 4 + x$ y en el $\widehat{ADC}$ $x < 2 + 3$, de donde $10 < 4 + x < 9$, lo que es absurdo; por tanto tal cuadrilátero no existe.

Hay otras formas posibles de configurar un cuadrilátero, pero con razonamientos similares llegaremos siempre a contradicción. □

Hay que recalcar que la deducción por reducción al absurdo no es lo mismo que la demostración de la proposición contrarrecíproca, insistimos en ello con un nuevo ejemplo.

Ejemplo 2.4.25 Demostrar que si p y q son números reales positivos tales que $\sqrt{pq} \neq \frac{p+q}{2}$, entonces $p \neq q$.

Demostrar esta implicación se puede hacer equivalentemente demostrando la contrarrecíproca; es decir, "dados dos números reales positivos p y q, si $p = q$, entonces $\sqrt{pq} = \frac{p+q}{2}$".

[4] Ver ejemplo 2.4.21

En efecto, si $p = q$

$$\sqrt{pq} = \sqrt{pp} = p = \frac{p+p}{2} = \frac{p+q}{2}.$$

Aquí no hay una contradicción obtenida de suponer, en $p \longrightarrow q$, simultáneamente $\neg q$ y p, sino que de $\neg q$ se obtiene directamente $\neg p$. □

Demostración de una doble implicación

La tautología $(p \longleftrightarrow q) \longleftrightarrow [(p \longrightarrow q) \wedge (q \longrightarrow p)]$ nos indica que hemos de demostrar una implicación y su recíproca (la condición necesaria y la condición suficiente).

Ejemplo 2.4.26 Demostremos que un número entero n es impar si y sólo si su cuadrado n^2 es impar.

Sean p y q, respectivamente, las proposiciones "n es impar" y "n^2 es impar".

Veamos que $p \longrightarrow q$. Si n es impar, entonces $n = 2k + 1$ para algún entero k, de donde $n^2 = 4(k^2 + k) + 1$ y por tanto es impar. En el ejemplo 2.4.17 se ha probado ya la implicación $q \longrightarrow p$ mediante el contrarrecíproco. □

Demostración de equivalencias múltiples

Si se trata de demostrar que n proposiciones $p_1, p_2, \ldots, p_n$ tienen los mismos valores de verdad $(p_1 \longleftrightarrow p_2 \longleftrightarrow \ldots \longleftrightarrow p_n)$ podemos hacer uso de la siguiente tautología, cuya comprobación dejamos como ejercicio:

$$[p_1 \longleftrightarrow p_2 \longleftrightarrow \ldots \longleftrightarrow p_n] \longleftrightarrow$$

$$(p_1 \longrightarrow p_2) \wedge (p_2 \longrightarrow p_3) \wedge \ldots \wedge (p_{n-1} \longrightarrow p_n) \wedge (p_n \longrightarrow p_1).$$

Ejemplo 2.4.27 Demostremos que si n es un entero, entonces las siguientes afirmaciones son equivalentes:

- 5 es divisor de n.
- 5 es divisor de n^2.
- 5 no es divisor de $n^2 - 1$ ni de $n^2 + 1$.

Llamemos, respectivamente, p_1, p_2, p_3 a las proposiciones primera, segunda y tercera del enunciado.

1. $p_1 \longrightarrow p_2$
   Supongamos que 5 es divisor de n entonces $n = 5k$ para algún entero k, por lo que $n^2 = 5(5k^2)$ y, por tanto, 5 es divisor de n^2.

2. $p_2 \longrightarrow p_3$
   Si 5 es divisor de n^2, es evidente que 5 no puede dividir ni a $n^2 - 1$ ni a $n^2 + 1$.

3. $p_3 \longrightarrow p_1$
   Es obvio que entre los cinco números consecutivos $n-2$, $n-1$, n, $n+1$ y $n+2$ uno ha de ser múltiplo de 5. Ya que 5 no es divisor de $n^2 - 1$, se tiene que 5 no es divisor ni de $n-1$ ni de $n+1$. Si fuese 5 divisor de $n-2$, entonces $n = 5m+2$ para algún entero m, de donde $n^2 = 25m^2+20m+4$, resultando entonces que $n^2 + 1$ es múltiplo de 5, lo que es imposible por hipótesis. Si fuese 5 divisor de $n+2$, entonces $n = 5r - 2$ para algún entero r, por lo que $n^2 = 25r^2 - 20r + 4$, de donde $n^2 + 1$ sería múltiplo de 5, lo que nuevamente es imposible. Ya que $n-2$, $n-1$, $n+1$ y $n+2$ no son múltiplos de 5, se deduce que n sí lo es.

□

Teoremas y cuantificadores

En los enunciados de muchos teoremas aparecen cuantificadores. A continuación describimos algunos de los métodos más usuales para demostrar teoremas de esta naturaleza.

Demostración de existencia

Los teoremas que son afirmaciones sobre la existencia de un tipo particular de objetos, son proposiciones de la forma $\exists x\ P(x)$, donde $P(x)$ es un predicado. Una demostración de esta clase se denomina una *demostración de existencia.*

Existen varios caminos para tales demostraciones, una de ellas encontrando un elemento a tal que $P(a)$ sea verdadero. Tal demostración de existencia se dice *constructiva.* Pero también es posible dar una demostración *no constructiva*, demostrando la existencia de algún a tal que $P(a)$ es verdadero de alguna forma, aunque no se sepa cuál es ese a. Una forma común de dar una demostración de existencia no constructiva es por *reducción al absurdo* y demostrar que la negación del cuantificador existencial implica una contradicción.

Ejemplo 2.4.28 Veamos un ejemplo de demostración constructiva. Demostremos que, cualquiera que sea el número natural n, existen n enteros compuestos consecutivos.

Demostrar que existen n enteros compuestos consecutivos, cualquiera que sea n, puede simbolizarse mediante el siguiente predicado: $\forall n\ \exists m\ (m+i$ es compuesto para $i = 1, \ldots, n)$, donde el *universo de discurso* son los números naturales.

Sea $m = n + 1$ y consideremos los enteros $m! + 2, \ldots, m! + (n + 1)$. Ninguno de ellos es primo ya que para cada $m! + i$, con $i = 2, \ldots, n + 1$, se tiene que $m! + i = (n + 1)! + i$. Sacando i factor común en el segundo miembro de la última igualdad vemos que i es divisor de $m! + 1$ para cada $i = 2, \ldots, n + 1$, de donde $m! + 2, \ldots, m! + (n + 1)$ son n números compuestos consecutivos.

No sólo hemos demostrado la existencia, sino que tenemos un procedimiento para construir esos números. □

Ejemplo 2.4.29 Demostremos que, cualquiera que sea el número real a, existe otro número real b tal que $a^2 b = a - b$.

Simbólicamente se trata de probar que $\forall a\ \exists b\ (a^2 b = a - b)$, siendo el *universo de discurso* los números reales.

En efecto, para cada número real a dado consideremos el número real $b = \frac{a}{1+a^2}$. Entonces

$$a^2 \frac{a}{1 + a^2} = \frac{a + a^3 - a}{1 + a^2} = a - \frac{a}{1 + a^2}.$$

□

Ejemplo 2.4.30 Veamos ahora un ejemplo de demostración de existencia no constructiva. Demostremos que cualquiera que sea el número entero positivo n existe un primo mayor que n.

De hecho este enunciado es equivalente al del ejemplo 2.4.22. Aquí veremos una demostración directa.

Simbólicamente se trata de demostrar que $\exists x\ P(x)$, donde $P(x)$ es el predicado "x es primo y x es mayor que n", siendo el *universo de discurso* los números enteros positivos.

Sea n un número entero positivo y consideremos $n! + 1$. Si $n! + 1$ es primo ya está. En caso contrario tendrá un factor primo. Ahora bien, cualquiera que sea el entero $k \leq n$ ($\forall\ k \leq n$) se tiene que k es un factor de $n!$, por lo que k no puede ser divisor de $n! + 1$, toda vez que el resto será siempre 1. Por tanto, cualquiera que sea el factor primo de $n! + 1$, será un entero mayor que n; es decir existe un primo mayor que n.

Notemos que no se ha encontrado quién es el número primo, pero se asegura su existencia. □

Contraejemplos

Relacionado con el cuantificador universal existe un tipo de demostración muy usual: demostrar que $\forall x\ P(x)$ es falso. Teniendo en cuenta que

$$\neg\ \forall x\ P(x) \longleftrightarrow \exists x\ \neg P(x),$$

si encontramos un elemento a tal que $P(a)$ es falso entonces habremos demostrado que $\exists x\ \neg P(x)$ es verdadero, que equivale a decir que $\forall x\ P(x)$ es falso.

Un elemento a tal que $P(a)$ es falso se llama un *contraejemplo*. Basta encontrar un contraejemplo para demostrar $\forall x\ P(x)$ es falso.

Ejemplo 2.4.31 Demostremos que es falso que cualquiera que sea el número primo x, se tiene que $x + 2$ es primo también.

Sea $P(x)$ el predicado "$x + 2$ es primo", siendo el *universo de discurso* los números primos. Se trata de ver que $\forall x\ P(x)$ es falso. Como $x = 7$ es primo, pero $x + 2 = 9$ no lo es, tenemos un contraejemplo. □

Ejemplo 2.4.32 Demostremos que es falso que cualquiera que sea el número natural n, $2^{2^n} + 1$ es primo.

Sea $P(n)$ el predicado "$2^{2^n} + 1$" es primo, siendo el *universo de discurso* los números naturales. Se trata de ver la falsedad de $\forall x\ P(x)$. Como $2^{2^5} + 1 = 641 \cdot 6700417$, para $n = 5$ tenemos un contraejemplo. □

Ejercicios

1. ¿Cuál es la regla de inferencia usada en cada uno de los casos siguientes?
   (a) Si hace frío, entonces no voy al campo. Hace frío. Por tanto no voy al campo.
   (b) Si es domingo la biblioteca no abre. La biblioteca está abierta hoy. De esta manera hoy no es domingo.
   (c) Si apruebo el curso, entonces me darán una beca. Si me dan una beca, entonces podré seguir estudiando el año próximo. Por tanto, si apruebo el curso, entonces podré seguir estudiando el año próximo.
   (d) En Navidades me quedaré estudiando. Así pues, en Navidades me quedaré estudiando o me iré de vacaciones.
   (e) En verano trabajo por las tardes y voy de copas por las noches. Por tanto, en verano voy de copas por las noches.

2. Determinar cuál de los siguientes argumentos son válidos, indicando la regla de inferencia usada, así como el tipo de falacia cuando sea el caso.
   (a) Si x es un número real tal que $x > 1$, entonces $x^2 > 1$. Supongamos que $x^2 > 1$. Entonces $x > 1$.
   (b) El número $\sqrt{3}$ es irracional si no se puede expresar como el cociente de dos enteros. De esta manera, ya que $\sqrt{3}$ no puede expresarse como $\frac{a}{b}$, donde a y b son números enteros, es irracional.

(c) Si x es un número real tal que $x > 5$, entonces $x^2 > 25$. Supongamos que $x^2 \leq 25$. Entonces $x \leq 5$.

(d) Un entero positivo o es un cuadrado perfecto o tiene un número par de divisores enteros positivos. Si n es un entero positivo que tiene un número impar de divisores enteros positivos. Entonces n es un cuadrado perfecto.

(e) Si n es tal que $n > 2$, entonces $n^2 > 4$. Supongamos que $n \leq 2$. Entonces $n^2 \leq 4$.

3. El siguiente argumento es una demostración incorrecta del enunciado *si* 3 *no es divisor de* n^2, *entonces* 3 *no es divisor de* n.

"Si 3 *no es divisor de* n^2, *entonces* $n^2 \neq 3k$, *cualquiera que sea el entero* k *considerado. De aquí que* $n \neq 3i$, *cualquiera que sea el entero* i. *Por tanto,* 3 *no es divisor de* n."

¿Qué tipo de falacia se ha cometido?, ¿dónde se encuentra el error en el razonamiento?

4. Sea $P(n)$ el predicado "Si a y b son números reales positivos, entonces $(a+b)^n \geq a^n + b^n$". Demostrar que $P(1)$ es verdadera. ¿Cuál es el tipo de demostración usada?

5. Demostrar, por reducción al absurdo, que la suma de un número irracional y de otro racional es irracional.

6. Demostrar que si a y b son números reales tales que $0 < a < b$, entonces $a^2 < b^2$. ¿Vale también el resultado si b es negativo?

7. Sean a, b, c números reales tales que $a > b$. Probar que si $ac \leq bc$, entonces $c \leq 0$.

8. Sea el siguiente enunciado: *Sea* $n > 2$ *un número natural compuesto. Entonces* $2n + 13$ *es también un número compuesto.*

(a) ¿Cuáles son las hipótesis y la conclusión del mismo?

(b) Demostrar que este enunciado es falso con un contraejemplo.

9. Demostrar que si $x^2 + y = 13$ e $y \neq 4$, entonces $x \neq 3$.

10. Demostrar que si $p \longrightarrow (q \longrightarrow r)$, entonces $\neg r \longrightarrow (p \longrightarrow \neg q)$.

11. Consideremos el siguiente falso enunciado: *Si* x *e* y *son números reales tales que* $x + y = 10$, *entonces* $x \neq 3$ *e* $y \neq 8$.

(a) Del que se ha dado la siguiente demostración:

Supongamos que la conclusión es falsa; es decir que $x = 3$ *e* $y = 8$. *Pero entonces* $x + y = 11$, *lo que contradice la hipótesis de que* $x + y = 10$. *Por tanto, el contrarrecíproco nos confirma que la tesis es verdadera.*

¿Dónde está el error?

(b) Demostrar que el enunciado es falso. ¿Cuál es el tipo de demostración utilizada?

12. Demostrar si es cierto o falso que $n^2 - n + 41$ es primo cuando n es un número entero positivo.

13. Demostrar que $\sqrt{n}$ es irracional si n es un número natural que no es cuadrado perfecto.

14. Demostrar que $\max(x, y) + \min(x, y) = x + y$, donde x e y son números reales.

15. Demostrar por casos que $|x + y| \leq |x| + |y|$, donde x e y son números reales.

16. Demostrar que para cualquier entero n, el resto de dividir n^2 por 4 es 0 o 1.

17. Demostrar que si n es un número entero positivo, entonces n es impar si y sólo si $5n + 6$ es impar.

18. Demostrar si es cierto o falso que *cualquier entero positivo puede escribirse como la suma de los cuadrados de dos números enteros.*

19. Demostrar que si n es un entero, las siguientes afirmaciones son equivalentes:

    (a) 3 es divisor de $n - 1$ o es divisor de $n - 2$.

    (b) n no es divisible por 3.

    (c) 3 es divisor de $n^2 - 1$.

20. Demostrar que es cierto o falso que existen tres números enteros positivos impares tales que son primos de la forma p, $p + 2$, $p + 4$.

21. Dar una demostración de existencia constructiva de la siguiente proposición: *Para cualquier entero positivo n existe un número entero que es divisible por más de n números primos.*

22. Demostrar que existen infinitos números primos que son de la forma "múltiplo de 4 más 1". ¿Cuál es el tipo de demostración usada: constructiva o no constructiva?

23. Consideremos el siguiente enunciado: *Existe x real tal que para cualquier y real se verifica que $xy^2 = y - x$.*
    Del que se ha proporcionado la siguiente demostración:
    Sea $x = \dfrac{y}{y^2 + 1}$. Entonces

$$y - x = y - \frac{y}{y^2 + 1} = \frac{y^3}{y^2 + 1} = \frac{y}{y^2 + 1} \cdot y^2 = xy^2.$$

    ¿Cuál es el error del razonamiento? ¿El enunciado es verdadero?

24. Consideremos el siguiente enunciado:

Cualquiera que sea $x \in \mathbb{R}$ *existe* $y \in \mathbb{R}$ *tal que* $xy^2 \neq y - x$,

del que se ha proporcionado la siguiente demostración:

Sea $x \in \mathbb{R}$ *arbitrario. Consideremos los siguientes casos:*

- $x = 0$. *Sea* $y = 1$, *entonces* $xy^2 = 0$ *e* $y - x = 1 - 0 = 1$, *así* $xy^2 \neq y - x$.
- $x \neq 0$. *Sea* $y = 0$. *Entonces* $xy^2 = 0$ *e* $y - x = -x \neq 0$, *así* $xy^2 \neq y - x$.

Ya que los dos casos contemplan todas las posibilidades, hemos demostrado que existe $y \in \mathbb{R}$ *tal que* $xy^2 \neq y - x$. *Como* x *era arbitrario, ello demuestra el enunciado.*

(a) ¿Es correcta la demostración? Si lo es, indíquese el tipo de demostración utilizada; si no lo es, indíquese el error.

(b) ¿Es el enunciado verdadero? En caso negativo indíquese un contraejemplo.

Capítulo 3

Conjuntos

Con este capítulo se pretende que el lector adquiera cierta familiaridad con los hechos básicos de la teoría de conjuntos. Los conceptos y métodos de ésta son herramientas usuales en las matemáticas y necesitará una aceptable comprensión de los conceptos generales y abstractos que en ella aparecen y una mínima destreza en la manipulación de conjuntos y de las operaciones entre ellos.

Efectuamos una presentación desde una perspectiva descriptiva, pues primamos la comprensión de los hechos básicos sobre la formalización de los mismos; no obstante se efectuarán algunas referencias a los problemas que originaron la necesidad de una axiomatización de esta teoría: así estudiaremos por qué fue necesario introducir *el esquema axiomático de separación*, o por qué es preciso introducir el *axioma de las potencias*, entre otros *axiomas de Zermelo–Fraenkel.*

Pero si este conocimiento básico de conceptos de la teoría de conjuntos y destreza mínima en la manipulación de los mismos es importante, en este capítulo y aunque sea en el transfondo, también estarán presentes diversas técnicas de demostración estudiadas en el capítulo anterior; así buen número de ejercicios requerirá poner en práctica las técnicas para efectuar demostraciones de existencia, contraejemplos ligados al cuantificador universal, la demostración por casos, o aquellas en las que es fundamental la aparición del disyuntor, etc. A medida que se avanza en el estudio de las matemáticas ha de prestarse especial atención a las técnicas de demostración, a reconocer las más adecuadas según el problema, en definitiva a entrenarse en lo sustancial.

3.1 Determinación de conjuntos

Una ciudad, un rebaño o un melonar son ejemplos de conjuntos de objetos. ¿Qué es un conjunto? Según Cantor (1845–1918) *un conjunto es el agrupamiento en un todo de objetos bien definidos y distintos por nuestra percepción o nuestro*

pensamiento, los cuales se denominan elementos del conjunto.

Sin embargo la definición de conjunto es algo que no se contemplará, de forma análoga a como sucede con la geometría clásica, donde no se define lo que es un punto ni lo que es una recta.

Los conjuntos están constituidos por sus elementos y es conveniente tener presente que un conjunto puede ser a su vez elemento de algún otro conjunto. Así una recta (conjunto de puntos) puede ser considerada como elemento del conjunto de todas las rectas de un plano.

El concepto principal de la teoría de conjuntos (que en la teoría axiomática de conjuntos es un concepto primitivo) es el de pertenencia. Cuando un objeto forma parte de un conjunto se dice que ese objeto es un elemento del conjunto o que pertenece a ese conjunto; así si designamos por L el conjunto de las letras del abecedario castellano, f pertenece a L, lo que se denota mediante $f \in L$. Y denotamos que 1 no es un elemento de L mediante $1 \notin L$.

Es bastante usual denotar a los conjuntos mediante letras mayúsculas y a sus elementos mediante letras minúsculas, aunque hay que hacer observar que ello no es imprescindible. Así $x \in A$ indica que x pertenece, o es un elemento del conjunto A.

Para que un conjunto quede bien especificado se puede indicar entre llaves cada uno de sus elementos y en este caso decimos que el conjunto ha sido determinado por *extensión.*

Ejemplo 3.1.1 Sea $A = \{1, 3, 5, 7, 9\}$, que es el conjunto formado por los números naturales impares menores que 10. □

Unos conjuntos especialmente distinguidos en matemáticas son:

- El de los números naturales, que lo denotaremos por $\mathbb{N}$.
- El de los números enteros, que lo denotaremos por $\mathbb{Z}$.
- El de los números racionales, que lo denotaremos por $\mathbb{Q}$.
- El de los números reales, que lo denotaremos por $\mathbb{R}$.
- El de los números complejos, que lo denotaremos por $\mathbb{C}$.

Una importante relación entre conjuntos es la igualdad. Intuitivamente A y B son iguales si los objetos de A y de B son idénticos. De esta forma definimos:

Definición 3.1.2 *Diremos que dos conjuntos A y B son iguales si tienen los mismos elementos.*

Si los conjuntos A y B son iguales se denota mediante $A = B$ y para expresar que no son iguales pondremos $A \neq B$.

Hemos de recalcar que un conjunto está determinado por sus elementos. Y por tanto ello podrá hacerse si podemos indicar si un objeto es o no elemento del mismo.

Definición 3.1.3 *Si A y B son dos conjuntos y todo elemento de A es un elemento de B diremos que A es un subconjunto de B, o que A está contenido o incluido en B y lo denotaremos mediante $A \subseteq B$.*

Cuando A está contenido en B, a veces también se dice que B contiene o incluye a A, lo que también se puede denotar escribiendo $B \supseteq A$. Si A y B son tales que $A \subseteq B$ y $A \neq B$, se dice que A es un subconjunto propio de B, o también que A está estrictamente contenido en B, o que B contiene estrictamente a A y se denotará bien mediante $A \subsetneq B$ o bien mediante $B \supsetneq A$.

A veces para indicar que A está contenido en B se usa $A \subset B$ o también $B \supset A$. Para denotar que A no es subconjunto de B escribimos $A \not\subseteq B$ o también $A \not\subset B$, o también cambiando de orden los conjuntos $B \not\supseteq A$ o bien $B \not\supset A$, lo que se lee usualmente como B *no contiene a* A.

Nosotros, por lo general, utilizaremos las notaciones $A \subseteq B$, para indicar que B contiene a A y $A \subsetneq B$, para indicar que el contenido es estricto.

Ejemplo 3.1.4

1. Dados los conjuntos $A = \{1,2,3,4,5,6,7,8,9,10\}$ y $B = \{1,2,3,4,5\}$, B es un subconjunto de A, lo que denotamos mediante $B \subseteq A$ o $A \supseteq B$. Sin embargo el conjunto $C = \{2,4,6,8,10,12\}$ no es subconjunto ni de A ni de B, ni ellos lo son de C, lo que denotaremos mediante $C \not\subseteq A$, $C \not\subseteq B$, $A \not\subseteq C$ y $B \not\subseteq C$.

2. Si $\mathcal{I}$ es el conjunto de los números impares, se tiene que $\mathcal{I} \subsetneq \mathbb{N}$.

□

De la definición de inclusión se deduce que todo conjunto debe considerarse incluido en sí mismo ($A \subseteq A$); lo que se especifica diciendo que la inclusión de conjuntos tiene la propiedad *reflexiva*. Además si A, B y C son tres conjuntos cualesquiera verificando que $A \subseteq B$ y que $B \subseteq C$, entonces $A \subseteq C$; tal circunstancia se denomina propiedad *transitiva* de la inclusión.

Si dos conjuntos cualesquiera A y B son tales que $A \subseteq B$ y $B \subseteq A$, entonces todo elemento de A lo es de B y recíprocamente, por lo que $A = B$, lo que se conoce como propiedad *antisimétrica*.

La igualdad entre conjuntos puede ser expresada en términos de la inclusión. Así, dos conjuntos cualesquiera A y B son iguales si y sólo si $A \subseteq B$ y $B \subseteq A$. De hecho es bastante usual utilizar en las demostraciones de igualdades de conjuntos este procedimiento de doble contenido.

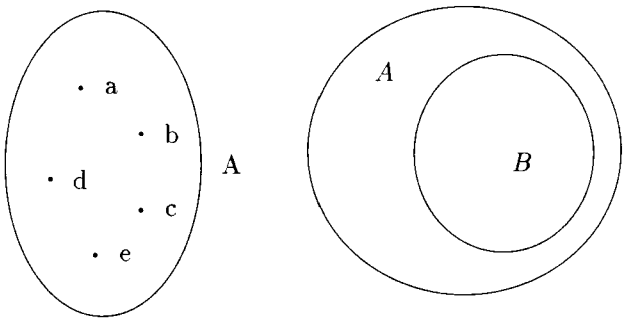


Figura 3.1: Diagramas de Venn

A veces se suelen utilizar representaciones visuales de los conjuntos, mediante recintos cerrados, cada uno de los cuales representa un conjunto, tal y como se señala en la figura 3.1, en la que aparecen representados, por una parte, el conjunto $A = \{a, b, c, d, e\}$ y, por otra, que $B \subseteq A$. Este tipo de representaciones se denominan *diagramas de Venn.*

Desde luego la relación de pertenencia y la de inclusión son conceptualmente muy diferentes. Mientras la segunda es reflexiva ($A \subseteq A$) la primera no, mientras la segunda es transitiva, la primera no.

No siempre es posible la determinación de un conjunto por extensión, es decir enumerando cada uno de sus elementos, ésta es la situación de los conjuntos numéricos anteriores. Así también, si hablamos de los números pares estamos dando una propiedad característica de una parte de los números naturales $\mathbb{N}$ que determina con absoluta precisión cuando un elemento pertenece o no a dicho subconjunto. La determinación de un conjunto a partir de una propiedad que caracteriza a los elementos de ese conjunto se llama determinación de un conjunto por *comprensión.*

Ejemplo 3.1.5 Sea A el conjunto de todos los españoles. Decir que x es un político español será cierto para algunos de los ciudadanos españoles, mientras que será falso para otros. El conjunto en cuestión se denota por

$$\{x \in A : \ x \quad \text{es político}\}.$$

□

En general si $p(x)$ es una proposición que se afirma acerca de los elementos x de un cierto conjunto A, entonces $\{x \in A : \ p(x)\}$ determina un subconjunto de A. Así pues tenemos un principio que permite determinar "*comprensivamente*" conjuntos a partir de otros ya existentes, los subconjuntos formados por aquellos

elementos que verifican una determinada propiedad.

Ejemplo 3.1.6

1. $A = \{y \in \mathbb{R} : \ 2 < y < 5\}$ es el conjunto de los puntos de la recta comprendidos entre 2 y 5.

2. $A = \{(x, y) \in \mathbb{R}^2 : \ x^2 + y^2 = 1\}$ es el conjunto de los puntos del plano que determinan la circunferencia unidad.

3. $A = \{(x, y) \in \mathbb{R}^2 : \ x^2 < y\}$ es el conjunto de los puntos del plano "interiores" (en el sentido de comprendidos entre las dos ramas de la parábola) a la parábola $y = x^2$.

□

Nótese que $p(x)$ ha de poderse evaluar, saber si es verdadera o falsa, para ciertos elementos del conjunto A, a los que se refiere. Así, si A es el conjunto de los españoles y $p(x)$ es "x morirá en accidente de tráfico el mes próximo", es claro que $\{x \in A : \ p(x)\}$ no forma un conjunto, pues $p(x)$ no proporciona un criterio para decidir si un español x pertenece o no al conjunto.

Naturalmente, cuando es posible la determinación de un conjunto por extensión, también puede hacerse por comprensión.

Ejemplo 3.1.7

1. El conjunto $A = \{-6, -2, 2, 3\}$ también se puede determinar como el conjunto de las soluciones de la ecuación $x^4 - 13x^2 + 36 = 0$.

2. El conjunto

   $$A = \{(0,0), (0,1), (0,-1), (1,1), (1,-1), (-1,1), (-1,-1), (1,0), (-1,0)\},$$

   queda también determinado si decimos que A es el "conjunto de los puntos reticulares (con coordenadas enteras) del plano interiores a la circunferencia de ecuación $x^2 + y^2 = 4$".

3. El conjunto $A = \{2, 3, 5, 7, 11, 13, 17, 19\}$, queda también determinado si decimos que A es el "conjunto de los números primos menores que 20".

□

Para conjuntos determinados por comprensión, la relación de inclusión determina cierta relación entre las proposiciones que permiten definir dichos conjuntos. Sea así un cierto conjunto $\mathcal{U}$ y los conjuntos $A = \{x \in \mathcal{U} : \ p(x)\}$ y $B = \{x \in \mathcal{U} : \ q(x)\}$, veamos que relación hay entre las proposiciones p y q si $A \subseteq B$.

Si $x \in A$, entonces $x \in B$, por lo que si $p(x)$ es verdadera entonces $q(x)$ también; de donde se sigue que p implica q ($p \longrightarrow q$). De la misma forma si para $x \in \mathcal{U}$ se tiene que $p(x)$ implica $q(x)$, entonces $A \subseteq B$.

Ejemplo 3.1.8

1. Si consideramos los conjuntos $A = \{n \in \mathbb{N} : \ n$ es potencia de 2 $\}$ y $B = \{n \in \mathbb{N} : \ n$ es par$\}$, tenemos que $A \subseteq B$ y que "ser potencia de 2 implica ser par".

2. Si de los números naturales n se predica $p(n)$: "n es múltiplo de cuatro más tres" y también $q(n)$: "n es impar", es claro que si se verifica $p(n)$, entonces también se verifica $q(n)$; es decir, p implica q y desde luego

$$A = \{n \in \mathbb{N} : \ p(n)\} \subseteq B = \{n \in \mathbb{N} : \ q(n)\}.$$

□

Si $A = B$, entonces se tendrá que $A \subseteq B$ y que $B \subseteq A$ y consecuentemente que p y q son proposiciones equivalentes. Y, desde luego, si dos proposiciones p y q son equivalentes, se tiene que $A = B$, siendo $A = \{x \in \mathcal{U} : \ p(x)\}$ y $B = \{x \in \mathcal{U} : \ q(x)\}$.

Ejemplo 3.1.9 Consideremos los cuadriláteros del plano. Si un cuadrilátero tiene los cuatro lados iguales entonces se trata de un paralelogramo y sus diagonales son perpendiculares. Recíprocamente, si un paralelogramo tiene sus diagonales perpendiculares, entonces sus cuatro lados son iguales. Así, el conjunto de los cuadriláteros con los cuatro lados iguales es igual al conjunto de los paralelogramos con las diagonales perpendiculares. □

Dado un conjunto A, entonces existe otro conjunto

$$\{x \in A : \ x \neq x\},$$

sin más que considerar como proposición, relativa a los elementos de A, a $p(x)$: "$x \neq x$". Este conjunto, que evidentemente no tiene elementos, se denomina *conjunto vacío* y se denota por $\emptyset$.

Es claro que $\emptyset \subseteq A$ cualquiera que sea el conjunto A, lo que resulta inmediato mediante lo que en el capítulo anterior denominamos *demostración vacía*. En efecto, hemos de ver que si $x \in \emptyset$ entonces $x \in A$; como $x \in \emptyset$ no es posible (la hipótesis es falsa) se tiene que la implicación es verdadera. Efectúe el lector una demostración de este mismo hecho por reducción al absurdo.

Naturalmente podríamos haber obtenido el conjunto $\emptyset$ mediante otras proposiciones relativas a los elementos de un cierto conjunto A. Por ejemplo si $A = \mathbb{Z}$, podemos formar el conjunto $\{x \in \mathbb{Z} : \ x^2 - 5 = 0\}$ que obviamente es el conjunto vacío.

Ejercicios

1. Definir por extensión los conjuntos:
   (a) Números primos menores que 23.
   (b) Números naturales comprendidos entre 7 y 15.
   (c) Restos de la división entera por 6 de cualquier número natural.
   (d) El conjunto de los números pares.
2. Definir por comprensión los conjuntos:
   (a) $A = \{-6, -4, -2, 0, 2, 4, 6\}$.
   (b) $B = \{1, 2, 4, 8, 16, \ldots\}$.
3. Se considera el conjunto $\mathbb{N}$, sin el 0. Sea A el conjunto de los pares y B el de las sumas de dos números impares. Probar que $A = B$.

3.2 Operaciones entre conjuntos

Los conjuntos pueden "combinarse" de formas diferentes. Así si consideramos el conjunto de los españoles mayores de dieciocho años y el de los españoles que fuman, podemos también hablar del conjunto de los españoles que son mayores de dieciocho años o fuman (en el que hay que considerar a los mayores de edad, a los que fuman y obviamente a los que cumplen los dos requisitos). También podemos considerar el conjunto de españoles que son fumadores y mayores de dieciocho años.

Definición 3.2.1 *Sean A y B dos conjuntos, llamamos unión de los mismos al conjunto formado por los elementos que pertenecen a A o a B y lo denotamos por $A \cup B$.*

$$A \cup B = \{x : x \in A \text{ o } x \in B\}.$$

Se deduce inmediatamente de la definición que si $x \in A$, entonces $x \in A \cup B$, cualquiera que sea el conjunto B.

La representación de $A \cup B$ mediante diagramas de Venn, la vemos en la figura 3.2

Ejemplo 3.2.2

1. Sean $A = \{1, 3, 5, 7, 9\}$, $B = \{5, 6, 7, 8, 11\}$ y $C = \{2, 5, 6, 9, 10\}$, entonces $A \cup B = \{1, 3, 5, 6, 7, 8, 9, 11\}$, $A \cup C = \{1, 2, 3, 5, 6, 7, 9, 10\}$ y finalmente $B \cup C = \{2, 5, 6, 7, 8, 9, 10, 11\}$.

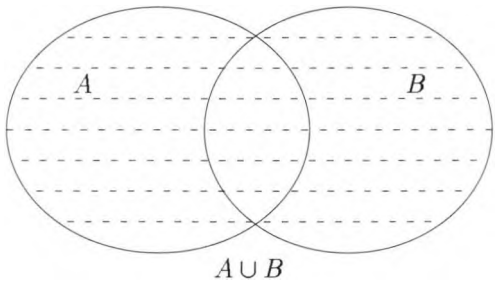
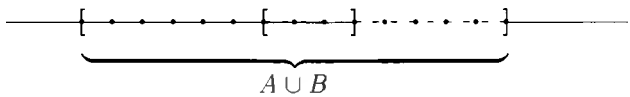


Figura 3.2: $A \cup B$

2. Sean los conjuntos de números reales: $A = \{x \in \mathbb{R} : \ -4 \leq x \leq 5\}$ y $B = \{x \in \mathbb{R} : \ 2 < x \leq 10\}$, entonces $A \cup B = \{x \in \mathbb{R} : \ -4 \leq x \leq 10\}$, que lo podemos representar gráficamente así:



3. Sean los conjuntos $A = \{n \in \mathbb{N} : \ n = \dot{2}\}$, donde $n = \dot{2}$ indica que n es un múltiplo de 2, y $B = \{n \in \mathbb{N} : \ n = 2k + 1\}$, entonces $A \cup B = \mathbb{N}$.

□

Algunos resultados fáciles de demostrar acerca de la unión de dos conjuntos los resumimos en la proposición siguiente.

Proposición 3.2.3 *Cualesquiera que sean los conjuntos A, B y C, se verifican las siguientes afirmaciones:*

1. $A \cup \emptyset = A$.
2. $A \cup A = A$ *(propiedad idempotente).*
3. $(A \cup B) \cup C = A \cup (B \cup C)$ *(propiedad asociativa).*
4. $A \cup B = B \cup A$ *(propiedad conmutativa).*

Demostración. Estas propiedades son demostrables por doble inclusión, haciendo uso de la propiedad antisimétrica de la misma. Las demostraciones están

basadas en las propiedades elementales correspondientes al operador lógico *o* ($\vee$). A continuación vemos la propiedad asociativa, dejando las restantes como ejercicio.

Si $x \in (A \cup B) \cup C$, entonces $x \in (A \cup B)$ o $x \in C$; por consiguiente $x \in A$, o $x \in B$, o $x \in C$ y, de esta forma, $x \in A$ o $x \in (B \cup C)$; de donde $x \in A \cup (B \cup C)$. De aquí que $(A \cup B) \cup C \subseteq A \cup (B \cup C)$.

De otra parte, si $x \in A \cup (B \cup C)$, entonces $x \in A$ o $x \in (B \cup C)$ y de aquí que $x \in A$, o $x \in B$, o $x \in C$. Por tanto $x \in (A \cup B)$ o $x \in C$, de donde $x \in (A \cup B) \cup C$. Tenemos así que $A \cup (B \cup C) \subseteq (A \cup B) \cup C$.

La propiedad antisimétrica de la inclusión garantiza la igualdad buscada.

■

Para dos conjuntos cualesquiera podemos formar un conjunto que contiene a ambos y nada más $\mathcal{C} = \{A, B\}$ y lo denominaremos como la *pareja* no ordenada formada por A y B.

La pareja $\{A, A\}$ se denota mediante $\{A\} = \{x \in \mathcal{C} : x = A\}$ y recibe el nombre de conjunto unitario (tiene un único elemento, el conjunto A). Hay que resaltar que afirmar que $A \in \mathcal{C}$ es equivalente a afirmar que $\{A\} \subseteq \mathcal{C}$.

Hemos de prestar especial atención a que $\{A\}$ y A son cosas bien distintas. El primero es un conjunto cuyo único elemento es el conjunto A y el segundo es el conjunto A integrado por sus elementos. Así, $\emptyset$ y $\{\emptyset\}$ son distintos; el primero es el conjunto que carece de elementos y el segundo es un conjunto unitario, cuyo único elemento es el conjunto $\emptyset$. Este tipo de distinción es importante y así conjuntos como éstos: $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\{\{\emptyset\}\}\}, \ldots \{\emptyset, \{\emptyset\}\}$, son distintos.

Como hemos señalado $\{\emptyset\}$ es un conjunto que contiene un elemento, el $\emptyset$, el segundo es un conjunto también unitario pero cuyo elemento es el conjunto unitario $\{\emptyset\}$, el tercero es un conjunto cuyo elemento es un conjunto cuyo elemento es $\{\{\emptyset\}\}$, etc.

Es fácil comprobar que $\{A\} \cup \{B\} = \{A, B\}$ y ello sugiere la forma de generalizar las parejas: concretamente, escribimos $\{A, B, C\} = \{A\} \cup \{B\} \cup \{C\}$. La definición implícita de la fórmula anterior debería incluir al menos una pareja de paréntesis, pero, en virtud de la propiedad asociativa su omisión no puede conducir a interpretaciones equívocas. Así, pues, para cada tres conjuntos podemos formar un conjunto que los contiene a ellos y nada más. Nos referiremos a este conjunto, determinado de manera única, como la terna (no ordenada) formada por dichos conjuntos. La extensión a un número mayor de conjuntos resulta obvia, obteniéndose cuaternas, etc.

La unión de dos conjuntos es un caso particular de la unión referida a una "colección" dada, $\mathcal{C}$, de conjuntos. Para cada colección $\mathcal{C}$ de conjuntos, existe un conjunto U, tal que $x \in U$ si y sólo si $x \in X$ para algún conjunto X de la colección $\mathcal{C}$. En este caso denotaremos la unión de la siguiente forma:

$$U = \cup\{X : X \in \mathcal{C}\}$$

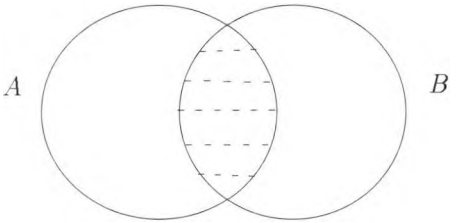


Figura 3.3: Intersección de Conjuntos

o también en la forma $U = \cup_{X \in \mathcal{C}} X$, o simplemente mediante $\cup \mathcal{C}$. Para una colección finita de conjuntos $\{A_1, \ldots, A_n\}$, denotamos la unión por

$$\cup_{i=1}^{n} A_i = A_1 \cup \ldots \cup A_n.$$

Ejemplo 3.2.4

1. $\bigcup_{n \in \mathbb{N}} [n-1, n) = [0, +\infty)$, considerando que $0 \notin \mathbb{N}$.
2. $\bigcup_{n \in \mathbb{N}} (\frac{1}{n}, 1] = (0, 1]$, considerando que $0 \notin \mathbb{N}$.

□

La formación de uniones de conjuntos tiene muchos aspectos similares con otra operación de la teoría de conjuntos, la *intersección*.

Definición 3.2.5 *Dados dos conjuntos A y B llamamos intersección de los mismos al conjunto formado por los elementos que pertenecen a A y a B y lo denotamos por $A \cap B$. $A \cap B = \{x \in A : x \in B\}$.*

Ejemplo 3.2.6

1. Para A, B, y C del apartado 1. del ejemplo 3.2.2, se tiene entonces que $A \cap B = \{5, 7\}$, $A \cap C = \{5, 9\}$ y $B \cap C = \{5, 6\}$.
2. Para A y B del apartado 2. del ejemplo 3.2.2, se tiene que
$$A \cap B = \{x \in \mathbb{R} : 2 < x \leq 5\}.$$
3. Para A y B del apartado 3. del ejemplo 3.2.2, se tiene que $A \cap B = \emptyset$.

□

Cuando dos conjuntos no tienen elementos comunes decimos que son *disjuntos* y en ese caso $A \cap B = \emptyset$.

Al igual que ocurrió con la unión de conjuntos es fácil y conveniente demostrar los resultados que se recogen en la proposición siguiente.

Proposición 3.2.7 *Cualesquiera que sean los conjuntos A, B y C, se verifican las siguientes afirmaciones:*

1. $A \cap \emptyset = \emptyset$
2. $A \cap A = A$, *(propiedad idempotente).*
3. $(A \cap B) \cap C = A \cap (B \cap C)$, *(propiedad asociativa).*
4. $A \cap B = B \cap A$, *(propiedad conmutativa).*

La unión e intersección de conjuntos verifican dos propiedades en la que ambas aparecen involucradas.

Proposición 3.2.8 *Cualesquiera que sean los conjuntos A, B y C, se verifican las siguientes afirmaciones:*

1. *Propiedad distributiva de la unión respecto de la intersección:*

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

2. *Propiedad distributiva de la intersección respecto de la unión:*

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

3. *Propiedades cancelativas:*

$$(A \cup B) \cap A = A \quad \text{y} \quad (A \cap B) \cup A = A.$$

Demostración. Demostramos[1] la primera, dejando las otras tres como ejercicio.

Veamos, en primer lugar, que todo elemento de $A \cup (B \cap C)$ pertenece al conjunto $(A \cup B) \cap (A \cup C)$.

Sea $x \in A \cup (B \cap C)$, entonces $x \in A$ o $x \in B \cap C$. Si $x \in A$ entonces $x \in A \cup B$ y también $x \in A \cup C$, y por tanto $x \in (A \cup B) \cap (A \cup C)$. Por otra parte, si $x \in B \cap C$, entonces $x \in B$ y $x \in C$. Si $x \in B$, entonces $x \in A \cup B$ y si $x \in C$, entonces $x \in A \cup C$. Consecuentemente se tiene que $x \in (A \cup B) \cap (A \cup C)$.

[1] Aunque este tipo de demostración pueda resultar tedioso, es sumamente conveniente estar familiarizados con él.

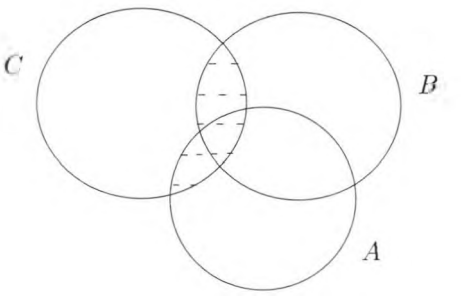


Figura 3.4: Propiedad Distributiva

Veamos ahora la inclusión en el otro sentido. Si $x \in (A \cup B) \cap (A \cup C)$, entonces $x \in A \cup B$ y $x \in A \cup C$. Si $x \in A$, entonces $x \in A \cup (B \cap C)$, y si $x \notin A$ es claro que $x \in B$ y $x \in C$, luego $x \in B \cap C$, de donde $x \in A \cup (B \cap C)$.

La propiedad antisimétrica de la inclusión nos permite concluir que

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

■

La intersección de dos conjuntos es un caso particular de la intersección referida a una colección $\mathcal{C}$ de conjuntos dada, al igual que ocurre con la unión de conjuntos. Para cada colección no vacía $\mathcal{C}$ de conjuntos, existe un conjunto A, tal que $x \in A$ si y sólo si $x \in X$ para cada $X \in \mathcal{C}$.

A recibe el nombre de la intersección de $\mathcal{C}$ y se denota por

$$\cap\{X : X \in \mathcal{C}\},$$

también por $\cap_{X \in \mathcal{C}} X$, o simplemente mediante $\cap\mathcal{C}$.

Para una colección finita de conjuntos $\{A_1, \ldots, A_n\}$ denotaremos la intersección por $\cap_{i=1}^{n} A_i = A_1 \cap \ldots \cap A_n$.

Ejemplo 3.2.9 Considerando que $0 \notin \mathbb{N}$ se tiene que:

$$\bigcap_{n \in \mathbb{N}} \left(-\frac{1}{n}, \frac{1}{n}\right) = \{0\},$$

$$\bigcap_{n \in \mathbb{N}} \left(0, \frac{1}{n}\right) = \emptyset.$$

□

Ejercicios

1. Si A, B y C son conjuntos, demostrar que:
   (a) $A \cup \emptyset = A$ y que $A \cap \emptyset = \emptyset$.
   (b) $A \cup A = A$ y que $A \cap A = A$ (propiedades idempotentes).
   (c) $(A \cap B) \cap C = A \cap (B \cap C)$ (propiedad asociativa).
   (d) $A \cup B = B \cup A$ y que $A \cap B = B \cap A$, (propiedades conmutativas).
   (e) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (propiedad distributiva de la intersección respecto de la unión).
   (f) $(A \cup B) \cap A = A$ y que $(A \cap B) \cup A = A$ (propiedades cancelativas).
   (g) $A \subseteq B$ si y sólo si $A \cup B = B$.
   (h) $A \subseteq B$ si y sólo si $A \cap B = A$.

2. Sean los siguientes subconjuntos de $\mathbb{N}$: A (múltiplos de 3), B (múltiplos de 5, más 1), C (múltiplos de 4, más 1) y D (múltiplos de 7). Determinar:
$$A \cap B,\ C \cup D,\ C \cap D,\ (A \cap B) \cup D.$$

3. Sean $\mathcal{F} = \{A, B, C, D\}$ y $\mathcal{G} = \{E, M, N\}$ dos colecciones de conjuntos ("conjuntos de conjuntos"), donde $A = \{1, 2\}$, $B = \{3, 4\}$, $C = \{1, 5\}$, $D = \{2, 6\}$, $E = \{1, 7\}$, $M = \{2, 8\}$ y $N = \{6, 9\}$. Determinar:
   (a) $\cup\mathcal{F}$, $\cup\mathcal{G}$.
   (b) $\cap\mathcal{F}$, $\cap\mathcal{G}$.
   (c) $(\cup\mathcal{F}) \cap (\cup\mathcal{G})$.
   (d) $(\cup\mathcal{F}) \cup (\cup\mathcal{G})$.
   (e) $(\cap\mathcal{F}) \cup (\cap\mathcal{G})$.
   (f) $\mathcal{F} \cup \mathcal{G}$, $\mathcal{F} \cap \mathcal{G}$.
   (g) $\cup(\mathcal{F} \cap \mathcal{G})$.
   (h) $\cap(\mathcal{F} \cup \mathcal{G})$.

4. Sean A, B y C conjuntos tales que los dos primeros no son disjuntos y el primero con el tercero tampoco y tal que A tiene un único elemento. Probar que $B \cap C \neq \emptyset$ ¿Es su demostración de existencia?, ¿de qué tipo?

5. Demostrar que si $\mathcal{F}$ es una colección de conjuntos y $A \in \mathcal{F}$, entonces: $A \subseteq \cup\mathcal{F}$ y $\cap\mathcal{F} \subseteq A$.

6. Sean $\mathcal{F}$, $\mathcal{G}$ dos colecciones de conjuntos. Probar que si $\mathcal{F} \subseteq \mathcal{G}$, entonces $\cup\mathcal{F} \subseteq \cup\mathcal{G}$.

7. Sean $\mathcal{F}$, $\mathcal{G}$ dos colecciones no vacías de conjuntos. Probar que si $\mathcal{F} \subseteq \mathcal{G}$, entonces $\cap\mathcal{G} \subseteq \cap\mathcal{F}$.

8. Sean $\mathcal{F}$, $\mathcal{G}$ dos colecciones no vacías de conjuntos, tal que cualquier elemento de $\mathcal{F}$ es un subconjunto de todo elemento de $\mathcal{G}$. Probar, entonces, que $\cup\mathcal{F} \subseteq \cap\mathcal{G}$.

9. Sean $\mathcal{F}$, $\mathcal{G}$ dos colecciones de conjuntos, tales que $\mathcal{F} \cap \mathcal{G} \neq \emptyset$. Probar que $\cap\mathcal{F} \subseteq \cup\mathcal{G}$.

10. Sean $\mathcal{F}, \mathcal{G}$ dos colecciones no vacías de conjuntos. Demostrar que

$$\cup(\mathcal{F} \cup \mathcal{G}) = (\cup\mathcal{F}) \cup (\cup\mathcal{G}).$$

11. El siguiente enunciado es falso:

> *Sean $\mathcal{F}$ y $\mathcal{G}$ dos colecciones de conjuntos. Si $\cup\mathcal{F}$ y $\cup\mathcal{G}$ son disjuntos, entonces también lo son $\mathcal{F}$ y $\mathcal{G}$.*

del que se ha dado la siguiente supuesta demostración:

> *Sean $\cup\mathcal{F}$ y $\cup\mathcal{G}$ disjuntos. Supongamos que $\mathcal{F}$ y $\mathcal{G}$ no son disjuntos, entonces existirá un cierto conjunto A que pertenecerá tanto a $\mathcal{F}$ como a $\mathcal{G}$. Como $A \in \mathcal{F}$, entonces $A \subseteq \cup\mathcal{F}$, de donde cualquiera que sea $x \in A$ se tiene que $x \in \cup\mathcal{F}$. Del mismo modo, como $A \in \mathcal{G}$, entonces $A \subseteq \cup\mathcal{G}$, de donde cualquiera que sea $x \in A$ se tiene que $x \in \cup\mathcal{G}$. Por tanto, cualquiera que sea $x \in A$ se tiene que $x \in \cup\mathcal{F}$ y $x \in \cup\mathcal{G}$, pero por hipótesis $(\cup\mathcal{F}) \cap (\cup\mathcal{G}) = \emptyset$, con lo que obtenemos una contradicción. De esta forma $\mathcal{F} \cap \mathcal{G} = \emptyset$.*

   (a) Indicar dónde falla la demostración.

   (b) Encontrar un contraejemplo de esta falsa proposición.

12. Sean $\mathcal{F}$ y $\mathcal{G}$ dos colecciones de conjuntos.

   (a) Probar que $\cup(\mathcal{F} \cap \mathcal{G}) \subseteq (\cup\mathcal{F}) \cap (\cup\mathcal{G})$.

   (b) Se ha formulado la siguiente proposición:

$$(\cup\mathcal{F}) \cap (\cup\mathcal{G}) \subseteq \cup(\mathcal{F} \cap \mathcal{G}),$$

   de la que se ha proporcionado la siguiente demostración:

   > *Supongamos que $x \in (\cup\mathcal{F}) \cap (\cup\mathcal{G})$. Ello quiere decir que $x \in \cup\mathcal{F}$ y $x \in \cup\mathcal{G}$, así que existe $A \in \mathcal{F}$ tal que $x \in A$ y existe $A \in \mathcal{G}$ tal que $x \in A$. De esta forma podemos elegir un conjunto A tal que $A \in \mathcal{F}$, $A \in \mathcal{G}$ y $x \in A$. Ya que $A \in \mathcal{F}$ y $A \in \mathcal{G}$, se tiene que $A \in \mathcal{F} \cap \mathcal{G}$. Por tanto existe $A \in \mathcal{F} \cap \mathcal{G}$ con $x \in A$, de donde $x \in \cup(\mathcal{F} \cap \mathcal{G})$. Ya que x era arbitrario, concluimos que $(\cup\mathcal{F}) \cap (\cup\mathcal{G}) \subseteq \cup(\mathcal{F} \cap \mathcal{G})$.*

i. ¿Es correcta la demostración? En caso afirmativo indicar la estrategia utilizada; por el contrario, si fuese incorrecta, señalar el error.

ii. ¿Es la proposición correcta? En caso negativo indicar un contraejemplo.

13. Consideremos el siguiente enunciado:

Sean B un conjunto y $\mathcal{F}$ una colección no vacía de conjuntos. Entonces $B \cap (\cup_{X \in \mathcal{F}} X) = \cup_{X \in \mathcal{F}} (B \cap X)$.

del que se ha proporcionado la siguiente demostración:

Sea x arbitrario. Supongamos que $x \in B \cap (\cup_{X \in \mathcal{F}} X)$. Entonces $x \in B$ y $x \in \cup_{X \in \mathcal{F}} X$, así que podemos elegir algún $X \in \mathcal{F}$, llamémosle Y, tal que $x \in Y$. Ya que $x \in B$ y $x \in Y$, $x \in B \cap Y$. De esta manera $x \in \cup_{X \in \mathcal{F}} (B \cap X)$.
Supongamos ahora que $x \in \cup_{X \in \mathcal{F}} (B \cap X)$. Entonces podemos elegir algún $X \in \mathcal{F}$, llamémosle Y, tal que $x \in B \cap Y$. Por tanto $x \in B$ y $x \in Y$. Ya que $x \in Y$, $x \in \cup_{X \in \mathcal{F}} X$. Puesto que $x \in B$ y $x \in \cup_{X \in \mathcal{F}} X$, entonces $x \in B \cap (\cup_{X \in \mathcal{F}} X)$.
Como x era arbitrario, queda demostrada nuestra proposición.

(a) ¿Es correcta la demostración? En caso afirmativo indicar la estrategia utilizada; por el contrario, si fuese incorrecta, señalar el error.

(b) ¿Es la proposición correcta? En caso negativo indicar un contraejemplo.

14. Sean $\mathcal{F}$ y $\mathcal{G}$ dos colecciones no vacías de conjuntos tal que cualquier elemento de $\mathcal{F}$ es disjunto con algún elemento de $\mathcal{G}$. Probar que $\cup\mathcal{F}$ y $\cap\mathcal{G}$ son disjuntos.

3.3 Potencia de un conjunto. Conjunto complementario

3.3.1 Potencia de un conjunto

Hemos considerado con anterioridad subconjuntos de un conjunto dado A. Ahora deseamos formar un nuevo conjunto a partir de los subconjuntos del mismo.

Definición 3.3.1 *Dado un conjunto A se denomina conjunto de las partes de A o conjunto potencia de A, y se denota por $\mathcal{P}(A)$, al conjunto cuyos elementos son los subconjuntos de A.*

Ya que $X \in \mathcal{P}(A)$ si y sólo si $X \subseteq A$, es claro que $\emptyset \in \mathcal{P}(A)$ y que $A \in \mathcal{P}(A)$.

Ejemplo 3.3.2

1. Si el conjunto en cuestión es $\emptyset$, entonces $\mathrm{P}(A) = \{\emptyset\}$.
2. Si $A = \{2\}$, entonces $\mathrm{P}(A) = \{\emptyset, \{2\}\}$.
3. Si $A = \{2, 4\}$, entonces $\mathrm{P}(A) = \{\emptyset, \{2\}, \{4\}, \{2, 4\}\}$.
4. Si $A = \{2, 4, 6\}$, entonces $\mathrm{P}(A) = \{\emptyset, \{2\}, \{4\}, \{6\}, \{2, 4\}, \{2, 6\}, \{4, 6\}, A\}$. Hemos de recordar que tanto $\emptyset$ como el propio A son subconjuntos de A y recalcar que el elemento 2 y el conjunto $\{2\}$, cuyo único elemento es el 2, son dos cosas muy distintas.

□

Observemos, en nuestro ejemplo, que cuando el número de elementos del conjunto A es 0, entonces $\mathcal{P}(A)$ tiene un elemento; si A tiene 1 elemento, entonces $\mathcal{P}(A)$ tiene dos; si A tiene 2, entonces $\mathcal{P}(A)$ tiene cuatro; si A tiene 3, entonces $\mathcal{P}(A)$ tiene ocho.

En general, si A es un conjunto que tiene n elementos, entonces $\mathcal{P}(A)$ tiene 2^n elementos.

Esta es la razón por la que $\mathcal{P}(A)$ recibe el nombre de *conjunto potencia*. Veamos que efectivamente el número de elementos de $\mathcal{P}(A)$ es 2^n, si el de A es n:

El número de subconjuntos unitarios de A es obviamente n, tantos como elementos tiene A. El número de subconjuntos con dos elementos es $\binom{n}{2}$, el de i elementos, con $i \leq n-1$ es $\binom{n}{i}$. Finalmente hay un subconjunto con n elementos, el propio A, y otro sin elementos $\emptyset$. Consecuentemente, el número total de subconjuntos de A es:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n-1} + \binom{n}{n} = (1+1)^2 = 2^n,$$

en virtud del desarrollo del binomio de Newton.

3.3.2 Diferencia de conjuntos y conjunto complementario

Definición 3.3.3 *Dados dos conjuntos A y B se llama diferencia de A y B, y se denota mediante $A \setminus B$, al conjunto formado por los elementos de A que no pertenecen a B.*

$$A \setminus B = \{x \in A : \ x \notin B\}.$$

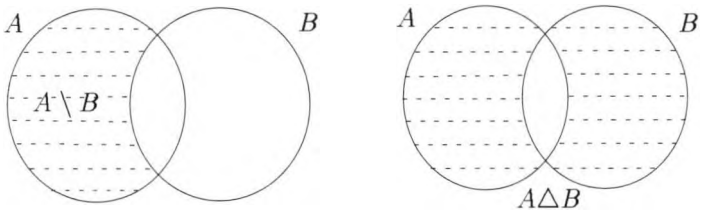


Figura 3.5: Diferencia y diferencia simétrica

Ejemplo 3.3.4

1. Sean $A = \{1, 2, 3, 4, 6, 8\}$ y $B = \{1, 4, 6\}$, entonces $A \setminus B = \{2, 3, 8\}$.
2. Sean $A = \{x \in \mathbb{Q} : -6 \leq x \leq \frac{3}{2}\}$ y $B = \{x \in \mathbb{Q} : -\frac{9}{2} \leq x < 4\}$, entonces $A \setminus B = \{x \in \mathbb{Q} : -6 \leq x < -\frac{9}{2}\}$.

□

Definición 3.3.5 *Dados dos conjuntos A y B se llama diferencia simétrica de A y B y se denota mediante $A\triangle B$ al conjunto $A\triangle B = (A \setminus B) \cup (B \setminus A)$.*

Ejemplo 3.3.6 Sean los conjuntos siguientes:
$A = \{x \in \mathbb{Q} : -6 \leq x \leq \frac{3}{2}\}$ y $B = \{x \in \mathbb{Q} : -\frac{9}{2} \leq x < 4\}$, entonces:
$A\triangle B = \{x \in \mathbb{Q} : -6 \leq x < -\frac{9}{2}\} \cup \{x \in \mathbb{Q} : \frac{3}{2} < x < 4\}$. □

Es fácil probar que:

Proposición 3.3.7 *Si A, B y C son conjuntos, se verifica que:*

1. $A\triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.
2. $A\triangle B = B\triangle A$.
3. $A\triangle A = \emptyset$.
4. $A\triangle\emptyset = \emptyset\triangle A = A$.
5. $(A\triangle B)\triangle C = A\triangle(B\triangle C)$.

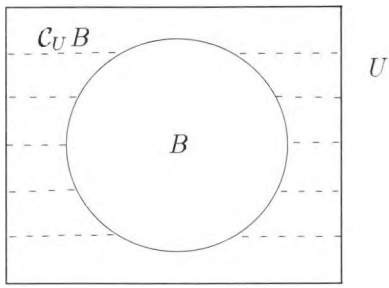


Figura 3.6: Conjunto complementario

Un caso particular y especialmente importante es cuando uno de los conjuntos está contenido en el otro.

Definición 3.3.8 *Dados dos conjuntos B y U tales que $B \subseteq U$, al conjunto $U \setminus B$ se le llama conjunto complementario de B respecto de U y se denota mediante $\mathcal{C}_U B$.*

Ejemplo 3.3.9 Sean $U = \{x \in \mathbb{R} : -8 \leq x \leq 6\}$ y $B = \{x \in \mathbb{R} : -6 \leq x \leq 2\}$. Desde luego $B \subseteq U$, entonces:
$\mathcal{C}_U B = \{x \in \mathbb{R} : -8 \leq x < -6\} \cup \{x \in \mathbb{R} : 2 < x \leq 6\}$. □

Cuando no haya lugar a dudas acerca del conjunto U respecto del que se determina el conjunto complementario de $B \subseteq U$, denotaremos a éste simplemente por B^c.

Cuando estamos operando con determinados subconjuntos de un conjunto dado U éste puede omitirse, considerándolo como un *universo de discurso*. En lo que sigue, mientras no se advierta lo contrario, consideraremos que todos los conjuntos con los que trabajemos son subconjuntos de un conjunto dado U, que será nuestro *universo de discurso*.

Es fácil comprobar que:

Proposición 3.3.10 *Se verifican las siguientes aserciones:*

1. $(A^c)^c = A$.
2. $\emptyset^c = U$ *y* $U^c = \emptyset$.
3. $A \cap A^c = \emptyset$ *y* $A \cup A^c = U$.
4. $A \subseteq B$ *si y sólo si* $B^c \subseteq A^c$.

Las propiedades más interesantes, que ligan el complemento de un conjunto con la unión y la intersección de conjuntos, se conocen como *Leyes de "De Morgan"*.

Proposición 3.3.11 *Cualesquiera que sean los conjuntos A y B, subconjuntos de un cierto conjunto U, se verifican las siguientes afirmaciones:*

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

Demostración. Sea $x \in (A \cap B)^c$, entonces $x \notin A \cap B$, de donde se sigue que $x \notin A$ o $x \notin B$, pero entonces $x \in A^c$ o $x \in B^c$, por lo que $x \in A^c \cup B^c$. Así pues $(A \cap B)^c \subseteq A^c \cup B^c$.

Sea ahora $x \in A^c \cup B^c$, entonces $x \in A^c$ o $x \in B^c$, por lo que $x \notin A$ o $x \notin B$, de donde $x \notin A \cap B$, luego $x \in (A \cap B)^c$. Esto prueba que $A^c \cup B^c \subseteq (A \cap B)^c$, quedando de esta forma demostrada la primera afirmación.

Dejamos como ejercicio la demostración de la segunda afirmación.

■

Proposición 3.3.12 *Si $\mathcal{C}$ es una colección no vacía de conjuntos y B es un conjunto cualquiera, se verifica que:*

1. $(\bigcup_{X \in \mathcal{C}} X) \cap B = \bigcup_{X \in \mathcal{C}} (X \cap B)$.
2. $(\bigcap_{X \in \mathcal{C}} X) \cup B = \bigcap_{X \in \mathcal{C}} (X \cup B)$.
3. $B \setminus (\bigcup_{X \in \mathcal{C}} X) = \bigcap_{X \in \mathcal{C}} (B \setminus X)$.
4. $B \setminus (\bigcap_{X \in \mathcal{C}} X) = \bigcup_{X \in \mathcal{C}} (B \setminus X)$.
5. $(\bigcup_{X \in \mathcal{C}} X)^c = \bigcap_{X \in \mathcal{C}} X^c$.
6. $(\bigcap_{X \in \mathcal{C}} X)^c = \bigcup_{X \in \mathcal{C}} X^c$.

Demostración.

Probaremos tres propiedades, dejando las restantes como ejercicio.

Veamos la primera afirmación. Sea $x \in (\bigcup_{X \in \mathcal{C}} X) \cap B$, equivalentemente $x \in X$ para algún $X \in \mathcal{C}$ y $x \in B$, luego $x \in X \cap B$ para algún $X \in \mathcal{C}$, lo que equivale a $x \in \bigcup_{X \in \mathcal{C}} (X \cap B)$.

Veamos la tercera propiedad. Sea $x \in B \setminus (\bigcup_{X \in \mathcal{C}} X)$, por lo que $x \in B$ y $x \notin (\bigcup_{X \in \mathcal{C}} X)$ y así $x \in B$ y $x \notin X$ cualquiera que sea $X \in \mathcal{C}$; es decir, $x \in B \setminus X$ cualquiera que sea $X \in \mathcal{C}$, luego $x \in \bigcap_{X \in \mathcal{C}} (B \setminus X)$. La otra inclusión es inmediata usando este mimo razonamiento en dirección contraria.

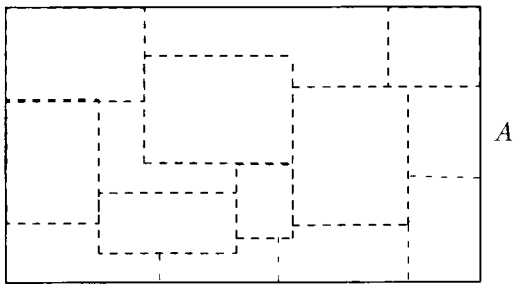


Figura 3.7: Partición de un conjunto

Por último probemos la quinta propiedad. Sea $x \in (\bigcup_{X \in \mathcal{C}} X)^c$, por lo que tendremos que $x \notin \bigcup_{X \in \mathcal{C}} X$, de donde $x \notin X$ cualquiera que sea $X \in \mathcal{C}$, entonces $x \in X^c$ para cada $X \in \mathcal{C}$, de donde $x \in \bigcap_{X \in \mathcal{C}} X^c$. El recíproco es inmediato.

■

Seguidamente introducimos el concepto de partición de un conjunto A.

Definición 3.3.13 *Si $\mathcal{C}$ es una colección o familia de subconjuntos propios de un conjunto dado A, verificando que todos ellos son no vacíos, que su unión es A y que son disjuntos dos a dos, se dice que $\mathcal{C}$ determina una partición de A.*

Ejercicios

1. Si A y B son conjuntos, probar que $(A \cup B)^c = A^c \cap B^c$.
2. Demostrar que $A \cap A^c = \emptyset$ y que $A \cup A^c = U$. Se supone que A es un subconjunto de U.
3. Demostrar que:
   (a) $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.
   (b) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.
4. Dar ejemplos de conjuntos A y B para los que $\mathcal{P}(A \cup B) \neq \mathcal{P}(A) \cup \mathcal{P}(B)$
5. Usar los diagramas de Venn para verificar las siguientes identidades:
   (a) $A \setminus (A \cap B) = A \setminus B$.
   (b) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$.

6. Probar que $(A \cup B) \setminus B \subseteq A$ y proporcionar varios ejemplos en los que $(A \cup B) \setminus B \subsetneq A$. ¿Cuándo $(A \cup B) \setminus B = A$?

7. Dar algunos ejemplos de conjuntos A, B y C para los que

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

8. Demostrar que:

   (a) $A \setminus B = A \cap B^c$.

   (b) $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

   (c) $A \cap (B \setminus C) = (A \cap B) \setminus C$.

9. Probar que $A \triangle B = (A \cup B) \setminus (A \cap B) = (A \cup B) \cap (A \cap B)^c$.

10. Demostrar que cualesquiera que sean los conjuntos A, B y C, se verifica:

    (a) $A \triangle B = B \triangle A$.

    (b) $A \triangle A = \emptyset$.

    (c) $A \triangle \emptyset = \emptyset \triangle A = A$.

    (d) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.

    (e) $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$.

11. Supongamos que A, B, C son conjuntos cualesquiera ¿Es cierto que si $A \triangle B = A \triangle C$, entonces $B = C$? Si no lo es indicar un contraejemplo y si lo es demostrarlo.

12. Sea $\mathcal{F}$ una colección de conjuntos y B un conjunto. Probar que $\mathcal{F} \subseteq \mathcal{P}(B)$ si y sólo si $\cup \mathcal{F} \subseteq B$.

13. Sea B un conjunto y $\mathcal{F}$ una colección no vacía de conjuntos:

    (a) Demostrar que $B \setminus (\cup_{X \in \mathcal{F}} X) = \cap_{X \in \mathcal{F}} (B \setminus X)$.

    (b) Conjeturar y demostrar un resultado "análogo" acerca de

$$B \setminus (\cap_{X \in \mathcal{F}} X).$$

14. Consideremos el siguiente enunciado:

    Sean $\mathcal{F}$ y $\mathcal{G}$ dos colecciones de conjuntos, entonces se verifica que $\cup(\mathcal{F} \setminus \mathcal{G}) \subseteq (\cup \mathcal{F}) \setminus (\cup \mathcal{G})$.

    del que se ha proporcionado la siguiente demostración:

    Supongamos que $x \in \cup(\mathcal{F} \setminus \mathcal{G})$. Entonces podemos elegir algún $A \in \mathcal{F} \setminus \mathcal{G}$ tal que $x \in A$. Ya que $A \in \mathcal{F} \setminus \mathcal{G}$, $A \in \mathcal{F}$ y $A \notin \mathcal{G}$. Ya que $x \in A$ y $A \in \mathcal{F}$, se tiene que $x \in \cup \mathcal{F}$. Ya que $x \in A$ y $A \notin \mathcal{G}$, se tiene que $x \notin \cup \mathcal{G}$. De esta manera $x \in (\cup \mathcal{F}) \setminus (\cup \mathcal{G})$.

(a) ¿Es correcta la demostración? Si lo es, indicar el tipo de demostración utilizada; si no lo es, indicar el error.

(b) ¿Es esta proposición correcta? En caso negativo indicar un contraejemplo.

15. Sea una familia de conjuntos $\mathcal{F}$. Probar que si $\mathcal{P}(\cup_{X\in\mathcal{F}} X) \subseteq \cup_{X\in\mathcal{F}} \mathcal{P}(X)$, entonces existe algún $Y \in \mathcal{F}$ tal que $X \subseteq Y$, cualquiera que sea $X \in \mathcal{F}$.

16. Sea $\mathcal{A}$ una colección de conjuntos. Probar que

$$\bigcup_{X\in\mathcal{A}} \mathcal{P}(X) \subseteq \mathcal{P}\left(\bigcup_{X\in\mathcal{A}} X\right).$$

17. Supongamos que $A \subseteq \mathcal{P}(A)$. Demostrar que $\mathcal{P}(A) \subseteq \mathcal{P}(\mathcal{P}(A))$.

18. Probar que, para cualquier conjunto A, se verifica que $\cup\mathcal{P}(A) = A$.

19. Demostrar que $A \subseteq B$ si y sólo si $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

20. Supongamos que B es un conjunto y $\mathcal{F}$ es una colección de conjuntos. Probar que $\cup\{A \setminus B : A \in \mathcal{F}\} \subseteq \cup(\mathcal{F} \setminus \mathcal{P}(B))$.

21. Sea la familia de subconjuntos del plano $(A_\alpha)_{\alpha\in\mathbb{R}}$, dada por

$$A_\alpha = \{(x, y) \in \mathbb{R}^2 : y = \alpha x\},$$

para cada $\alpha \in \mathbb{R}$. Estudiar si se trata de una partición del plano.

22. Sea el conjunto $A = \{a, b, c\}$. Determinar sus posibles particiones.

23. Probar que dado un conjunto H, si $P_1 = \{\alpha_1, \ldots, \alpha_k\}$ y $P_2 = \{\beta_1, \ldots, \beta_l\}$ son particiones de H, entonces

$$P = \{X \subseteq H : X = \alpha_i \cap \beta_j \neq \emptyset,\ 1 \leq i \leq k,\ 1 \leq j \leq l\}$$

es también una partición de H.

3.4 Sobre la axiomatización de la teoría de conjuntos

La teoría de conjuntos tal como fue considerada por Cantor produjo pronto algunas paradojas que exigieron una revisión de la misma. La necesidad de evitar contradicciones llevó al estudio de la teoría de conjuntos desde una perspectiva axiomática.

Aunque Cantor no formuló explícitamente ningún axioma, las demostraciones de sus teoremas se sustentan en tres principios o axiomas considerados implícitamente, que llamaremos el *axioma de extensión* (dos conjuntos son idénticos si tienen los mismos elementos), el *axioma de abstracción* (dada una propiedad existe un conjunto cuyos elementos son precisamente aquellas entidades que tienen tal propiedad) y el *axioma de elección* (dada una colección cualquiera de conjuntos no vacíos, existe entonces un conjunto formado tomando un elemento de cada uno de los conjuntos de la colección inicial). Detengámonos por un instante en el segundo de ellos.

"Axioma de Abstracción":
Dada una propiedad $p(x)$ existe un conjunto cuyos elementos son precisamente aquellos objetos que verifican dicha propiedad.

En definitiva, existe el conjunto $\{x : p(x)\}$.

En 1901 Bertrand Russell (1872–1970) consideró el conjunto de todas las cosas que tienen la propiedad de no ser elementos de sí mismas. Basándonos en el axioma de abstracción y llamando a este conjunto B, tenemos que

$$B = \{x : x \notin x\}.$$

Por tanto B es elemento de sí mismo ($B \in B$) si y sólo si no es elemento de sí mismo ($B \notin B$); lo que obviamente es una contradicción. Este hecho se conoce como *Paradoja de Russell* y junto con otras dieron lugar a un estudio más minucioso de la teoría de conjuntos.

En 1908 Zermelo (1871–1953) funda la teoría axiomática de conjuntos (en contraposición a la teoría descriptiva o intuitiva de conjuntos, terreno en el que se desarrolla nuestra exposición) sustituyendo el axioma de abstracción (origen de la paradoja anterior) por el *esquema axiomático de separación*, también conocido por algunos autores como *Axioma de Especificación* e introduciendo otros axiomas que permitían construir una teoría consistente.

Para Zermelo un conjunto es un objeto no definido que satisface una lista de axiomas dados; entre ellos el referido *Axioma de Especificación*, que permite separar los elementos de un conjunto dado que satisfacen alguna propiedad y constituyen el subconjunto que consta precisamente de esos elementos. En la teoría axiomática de conjuntos son conceptos primitivos los de conjunto y elemento y la relación de pertenencia.

A continuación nos detendremos sólo en el estudio del significado de aquellos axiomas que necesitamos para una formalización de los conceptos vistos en las secciones anteriores de este capítulo.

Podemos enunciar:

Axioma de Extensión:
Dos conjuntos son iguales si y sólo si tienen los mismos elementos.

Axioma de Especificación:
Para todo conjunto A y para toda propiedad $p(x)$ existe un conjunto B cuyos elementos son aquellos elementos x de A para los que se verifica $p(x)$.

El axioma de extensión nos garantiza que el conjunto determinado por el axioma de especificación es único.

Realmente más que un axioma es una colección de ellos (de ahí el nombre de *esquema axiomático de separación*), puesto que para cada propiedad $p(x)$ tenemos un axioma.

Hemos de aclarar que el origen de la paradoja de Russell radica en la aplicación del axioma de especificación a un *conjunto universal* (un algo que contiene a todo).

Dando por hecho que no es posible aceptar contradicciones en cualquier teoría matemática, la misma paradoja anterior nos servirá para poner en evidencia que no es posible aceptar la existencia de un *conjunto universal.* En efecto, cualquiera que sea el conjunto A, si $B = \{x \in A : x \notin x\}$, entonces cualquiera que sea b se tendrá que

$$b \in B \text{ si y solo si } (b \in A,\ b \notin b) \tag{3.1}$$

Ahora bien, si A es el conjunto universal deberá ocurrir que $B \in A$. Veamos, sin embargo, que esto no es posible. En efecto, sea $B \in A$, puede ocurrir que $B \in B$ o bien que $B \notin B$. Si $B \in B$, en virtud de (3.1), se tiene que $B \notin B$, lo que representa una contradicción. Si $B \notin B$, nuevamente por (3.1), se tendrá que $B \in B$, obteniéndose nuevamente una contradicción. Por tanto no es posible que $B \in A$, cualquiera que sea el conjunto A, o lo que es lo mismo existe B que no está en A, cualquiera que sea A; es decir no existe un conjunto universal. así, conviene recordar que:

Para formar un conjunto a partir de una propiedad, debemos tener un cierto conjunto dado a cuyos elementos sea aplicable la referida propiedad.

La formalización de la teoría de conjuntos se hace usualmente desde la axiomática de Zermelo-Fraenkel [2] y junto con los anteriores axiomas otros como los *axiomas de apareamiento, de regularidad*, etc. son necesarios. No obstante nuestro acercamiento a esta teoría será intuitivo, razón por la que sólo presentaremos algunos aspectos interesantes sobre la necesidad de la axiomatización.

El siguiente axioma nos permite formar nuevos conjuntos a partir de otros ya existentes.

Axioma de Apareamiento o de las parejas:
Si A y B son conjuntos, entonces existe un conjunto C al que pertenecen ambos: $A \in C$ y $B \in C$.

[2] Existen otras posibilidades de axiomatización, pero como ya se ha indicado ello excede al propósito de estas páginas.

Una consecuencia inmediata de este axioma, es que para dos conjuntos cualesquiera existe un conjunto que contiene a ambos y nada más, ya que si $A \in C$ y $B \in C$ y $p(x)$ es la propiedad "$x = A$ o $x = B$" y la aplicamos al conjunto C, tendremos por el axioma de especificación el conjunto $\{x \in C : x = A \text{ o } x = B\}$. El axioma de extensión nos garantiza que este conjunto que sólo contiene a A y a B es único. Lo denotamos por $\{A, B\}$ y se trata, como ya sabemos, de la pareja no ordenada formada por A y B.

A partir de un conjunto A podemos formar, como bien sabemos, haciendo uso del axioma de especificación el conjunto $\emptyset = \{x \in A : x \neq x\}$, que en virtud del axioma de extensión es único. También sabemos que, haciendo uso del axioma de apareamiento, podemos construir el conjunto unitario $\{A\} = \{A, A\}$.

El axioma de apareamiento nos asegura que todo conjunto es elemento de algún conjunto y que dos conjuntos cualesquiera son a la vez elementos de un mismo conjunto.

El axioma de apareamiento y la existencia del conjunto vacío nos permite la construcción de otros muchos conjuntos como ya vimos: $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, etc.

De momento, dos conjuntos se pueden "unir" en uno sólo como elementos. Si deseamos que tanto los elementos de uno como los de otro sean elementos de un nuevo conjunto necesitamos un nuevo axioma:

> **Axioma de las uniones**
> *Para toda colección de conjuntos existe un conjunto que contiene a todos los elementos que pertenecen al menos a uno de los conjuntos de la colección dada.*

Podemos simbolizar este axioma como sigue: "cualquiera que sea $\mathcal{C}$ existe un conjunto V tal que si $x \in X$ para algún $X \in \mathcal{C}$, entonces $x \in V$".

Este conjunto V, cuya existencia acabamos de garantizar, pudiera tener elementos que no pertenecieran a algún conjunto $X \in \mathcal{C}$, resultando "más grande" de lo deseado, pues nos gustaría que el nuevo conjunto tuviese como elementos única y exclusivamente a los elementos de los elementos de $\mathcal{C}$. Esto tiene fácil remedio mediante el axioma de especificación, pues con su auxilio podemos formar el conjunto:

$$U = \{x \in V : x \in X \text{ para algún } X \in \mathcal{C}\}.$$

Es claro que un elemento arbitrario x pertenecerá a U si y sólo si $x \in X$ para algún X en $\mathcal{C}$. Este conjunto U se denomina la *unión* de $\mathcal{C}$ y su unicidad es consecuencia del axioma de extensión. Como ya sabemos denotamos la unión mediante $U = \cup\{X : X \in \mathcal{C}\}$, o también mediante $U = \cup_{X \in \mathcal{C}} X$ o simplemente mediante $\cup\mathcal{C}$.

Nótese que muy bien pudiera ser $\mathcal{C} = \emptyset$ y, en tal caso, es inmediato que

$$\cup\{X : X \in \emptyset\} = \emptyset.$$

Es claro también que $\cup\{X : X \in \{A\}\} = A$. La unión de una pareja de conjuntos $\{A, B\}$ será $\cup\{X : X \in \{A, B\}\}$ o más simplemente $A \cup B$. Tras lo dicho, la definición que dimos de unión de dos conjuntos está totalmente justificada.

Detengámonos ahora en la intersección de conjuntos. Dijimos que "para cada colección no vacía $\mathcal{C}$ de conjuntos, existe un conjunto A, tal que $x \in A$ si y sólo si $x \in X$ para cada $X \in \mathcal{C}$. En efecto, como $\mathcal{C}$ no es vacía, sea $Y \in \mathcal{C}$ algún conjunto de $\mathcal{C}$, el axioma de especificación nos garantiza la existencia del conjunto:

$$A = \{x \in Y : x \in X \text{ para cada } X \in \mathcal{C}\}.$$

La dependencia de A de la elección arbitraria de Y es ilusoria, por lo que podemos escribir, si no hay posibilidad de confusión:

$$A = \{x : x \in X \text{ para cada } X \in \mathcal{C}\}.$$

Como ya sabemos,

$$A = \cap\{X : X \in \mathcal{C}\} = \cap_{X \in \mathcal{C}} X = \cap\mathcal{C}$$

recibe el nombre de la intersección de $\mathcal{C}$.

La exigencia de que $\mathcal{C}$ sea no vacía no es baladí, puesto que caso de ser $\mathcal{C} = \emptyset$ no podríamos garantizar la existencia de $\cap\mathcal{C}$.

En efecto,

$$\{x : x \in X \text{ para cada } X \in \emptyset\} \tag{3.2}$$

no define conjunto alguno, pues "¿qué elementos x no satisfacen la condición propuesta?" Si no es cierto que $x \in X$ para cada $X \in \emptyset$, deberá entonces existir algún $X \in \emptyset$ tal que $x \notin X$; pero como no existe $X \in \emptyset$, esto es absurdo, por tanto no existe x que deje de satisfacer la condición propuesta, es decir, todo x la satisface, por lo que (3.2) es el *conjunto universal*, llegando a contradicción.

Si deseamos formar un nuevo conjunto a partir de los subconjuntos de uno dado A necesitamos introducir un nuevo axioma.

Axioma de las potencias:
Para todo conjunto A, existe un conjunto $\mathcal{P}$ tal que si $X \subseteq A$, entonces $X \in \mathcal{P}$.

Es decir, para cada conjunto A existe un conjunto entre cuyos elementos están todos los subconjuntos de A. Haciendo uso del axioma de especificación podemos formar el conjunto de las partes de A:

$$\mathcal{P}(A) = \{X \in \mathcal{P} : X \subseteq A\},$$

cuya unicidad queda garantizada por el axioma de extensión.

Dados dos conjuntos A y B, la existencia y unicidad del conjunto diferencia $A \setminus B$ quedan garantizadas, respectivamente, por los axiomas de especificación y extensión. El lector ya sabrá que los axiomas hasta ahora contemplados también nos permiten garantizar la existencia y unicidad del conjunto $A \triangle B$.

En los capítulos 7 y 8 necesitaremos de nuevos axiomas para efectuar la formalización de nuevos conceptos. Será ese el momento de detenernos en analizar el significado de los mismos.

Capítulo 4

Relaciones binarias

4.1 Pares ordenados

El lector está ya familiarizado con la idea de par ordenado, así, por ejemplo, sabe que $(3,4)$ y $(4,3)$ representan puntos distintos del plano. Ahora vamos a formalizar desde la teoría de conjuntos la idea de par ordenado.

Hasta el momento nada hemos dicho sobre el "orden" (en el sentido intuitivo que todos tenemos de este concepto) de los elementos de un cierto conjunto. Así, si A es un conjunto que consta de dos elementos, $A = \{a, b\}$ y $A = \{b, a\}$ son una misma cosa. Si quisiéramos distinguir sus elementos en un determinado "orden", por ejemplo primero a y luego b, podríamos recurrir a la inclusión de subconjuntos de A, tomando $\{a\},\ \{a, b\} \in \mathcal{P}(A)$ y formando el conjunto $\mathcal{F} = \{\{a\},\ \{a, b\}\}$.

Es cierto que nada sabemos de la "ordenación" de los elementos de $\mathcal{F}$, pues $\{\{a\},\ \{a, b\}\}$ y $\{\{a, b\},\ \{a\}\}$ son el mismo conjunto, no obstante $\{a\} \subseteq \{a, b\}$, por lo que podríamos decir que $\{a\}$ es "anterior" a $\{a, b\}$, y en función de ello (puesto que uno y otro subconjunto de A sólo se diferencian en el elemento b) que a es el "primer" elemento y b el "segundo". En definitiva, podríamos recurrir a la construcción de un subconjunto de $\mathcal{P}(A)$ para determinar una "ordenación" en A.

Definición 4.1.1 *Dados dos conjuntos*[1] *a y b se denomina par ordenado (a, b) al conjunto*

$$(a, b) = \{\{a\},\ \{a, b\}\},$$

donde a y b reciben, respectivamente, el nombre de primer y segundo elemento del par.

[1] Excepcionalmente los denotaremos con letras minúsculas.

¿Podemos garantizar la existencia de este conjunto con los axiomas, hasta ahora conocidos, de Zermelo–Fraenkel?

En general $(a,b) \neq (b,a)$, toda vez que $\{\{a\},\ \{a,b\}\} \neq \{\{b\},\ \{a,b\}\}$.

Proposición 4.1.2 *(a,b) es un conjunto unitario si y sólo si $a = b$.*

Demostración. Si $(a,b) = \{\{a\},\ \{a,b\}\}$ es unitario, es porque $\{a\} = \{a,b\}$ y, por tanto, $a = b$.

Recíprocamente, si $a = b$, entonces

$$(a,b) = \{\{a\},\ \{a,a\}\} = \{\{a\}\}$$

es un conjunto unitario.

■

Debemos asegurarnos que (a,b) merece el calificativo de "ordenado", por lo que hemos de probar que si dos pares ordenados coinciden, entonces lo hacen sus elementos y en el mismo orden.

Proposición 4.1.3 *Dos pares ordenados (a,b) y (c,d) son iguales si y sólo si $a = c$ y $b = d$.*

Demostración. Sea $(a,b) = (c,d)$.

Supongamos, en primer lugar, que $a = b$, entonces

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

por tanto $\{a\} = \{c\}$, de donde $a = c$. Como (c,d) es un conjunto unitario, se sigue que $c = d$. Concluimos que $a = b = c = d$.

Supongamos ahora que $a \neq b$. El conjunto unitario $\{a\}$ pertenece al par (a,b). Por otra parte, $c \neq d$, pues de lo contrario (c,d) sería un conjunto unitario igual a (a,b), que no es unitario. Además, el conjunto unitario $\{c\}$ está en (c,d). De la igualdad $(a,b) = (c,d)$ se sigue que los dos conjuntos unitarios coinciden: $\{a\} = \{c\}$, por lo que $a = c$. Por otra parte, los pares no ordenados deben coincidir: $\{a,b\} = \{c,d\}$ y por tanto $b \in \{c,d\}$; ahora bien, no puede ser que $b = c$, pues entonces $b = a$, obteniéndose una contradicción, luego $b = d$.

Recíprocamente, si $a = c$ y $b = d$, tendremos que

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

■

4.2 Producto cartesiano

Supongamos ahora dos conjuntos A y B, ¿podremos formar un conjunto cuyos elementos sean todos los pares ordenados (x, y), con $x \in A$ e $y \in B$?

Veamos: un tal conjunto tendría como elemento a $(x, y) = \{\{x\}, \{x, y\}\}$; ahora bien, $\{x, y\} \subseteq A \cup B$ y $\{x\} \subseteq A \subseteq A \cup B$, por lo que

$$(x, y) = \{\{x\}, \{x, y\}\} \subseteq \mathcal{P}(A \cup B).$$

Es claro que, entonces, $(x, y) \in \mathcal{P}(\mathcal{P}(A \cup B))$.

Podemos, pues, concluir que la respuesta a nuestra pregunta es afirmativa. La existencia queda garantizada por aplicación sucesiva de los axiomas de las potencias, el de especificación y el de extensión. Queda así justificada la siguiente definición.

Definición 4.2.1 *Dados dos conjuntos A y B, llamamos producto cartesiano de A y B, y lo denotamos mediante $A \times B$, al conjunto de pares ordenados:* $A \times B = \{(x, y) : x \in A \text{ y } y \in B\}$.

Toda vez que hablamos de pares ordenados, es claro que, en general, el producto cartesiano de conjuntos "no es conmutativo": $A \times B \neq B \times A$.

Debemos plantearnos bajo qué condiciones el producto cartesiano es el conjunto vacío. La respuesta es la siguiente caracterización.

Proposición 4.2.2 *Dados dos conjuntos A y B, se verifica que $A \times B = \emptyset$ si y sólo si $A = \emptyset$ o $B = \emptyset$.*

Demostración. Supongamos que tanto A como B son no vacíos, entonces existirán $x \in A$ y $y \in B$, por lo que $(x, y) \in A \times B$, luego $A \times B \neq \emptyset$. Veamos el recíproco, sea $B = \emptyset$, y supongamos que $A \times \emptyset \neq \emptyset$, entonces existirá $x \in A$ e $y \in \emptyset$, lo que es absurdo, consecuentemente no existe $(x, y) \in A \times \emptyset$, por lo que $A \times B = A \times \emptyset = \emptyset$. Análogamente se demuestra que $\emptyset \times B = \emptyset$.

■

El producto cartesiano de dos conjuntos $A \times B$ se suele representar gráficamente señalando cada elemento de $A \times B$ como un punto del plano, con un *sistema de referencia cartesiano*, representando en el eje de ordenadas los elementos de B y en el de abscisas los elementos de A, como se pone de manifiesto en el próximo ejemplo.

Ejemplo 4.2.3

1. Sean $A = \{1, 2, 3\}$ y $B = \{a, b\}$, entonces
   $A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$.
   En la Figura 4.1, se representa el producto cartesiano $A \times B$.

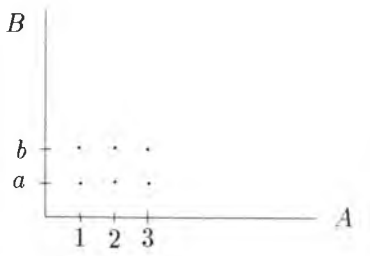


Figura 4.1: Producto Cartesiano

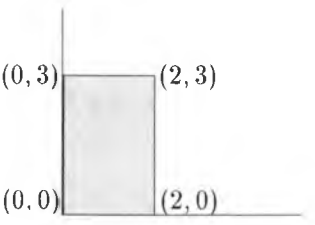


Figura 4.2: Producto Cartesiano

2. $\mathbb{Z} \times \mathbb{Z}$ es el conjunto de puntos del plano con coordenadas enteras.

3. $\mathbb{R} \times \mathbb{R}$ es el conjunto de todos los puntos del plano y se representa por $\mathbb{R}^2$.

4. Si $A = \{x \in \mathbb{R} : \ 0 \leq x \leq 2\}$ y $B = \{x \in \mathbb{R} : \ 0 \leq x \leq 3\}$, entonces

$$A \times B = \{(x, y) \in \mathbb{R}^2 : \ 0 \leq x \leq 2, \ 0 \leq y \leq 3\}$$

y representa a los puntos del plano del rectángulo de vértices: $(0, 0)$, $(2, 0)$, $(2, 3)$ y $(0, 3)$, como se indica en la Figura 4.2.

□

Si tenemos un conjunto de pares ordenados, C, éste es un subconjunto de algún producto cartesiano; es decir, existen dos conjuntos A y B tales que se verifica que $C \subseteq A \times B$.

Ejemplo 4.2.4 Sea $C = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$. Consideremos $D = H = \{1, 2, 3, a, b\}$, entonces

$$C \subseteq D \times H =$$
$$\{(1, 1), (1, 2), (1, 3), (1, a), (1, b), (2, 1), (2, 2), (2, 3),$$

$$(2,a),(2,b),(3,1),(3,2),(3,3),(3,a),(3,b),(a,1),(a,2),$$
$$(a,3),(a,a),(a,b),(b,1),(b,2),(b,3),(b,a),(b,b)\}.$$

Desde luego, otros subconjuntos de $D \times D$ contienen a C, pero si llamamos ahora $A = \{1,2,3\}$ y $B = \{a,b\}$ tendremos que $A \times B$ es el producto cartesiano "más pequeño" que contiene a los pares de C. □

Así, dado un conjunto de pares ordenados C, existen dos conjuntos D y H tales que $C \subseteq D \times H$. La demostración de este hecho es sencilla, sólo hay que generalizar el proceso seguido en el anterior ejemplo. Es conveniente observar que la solución no tiene por qué ser única y que, en general, podemos considerar productos cartesianos estrictamente contenidos en el anterior y que contengan a C. Para obtener el producto cartesiano "más pequeño" que contiene a los pares ordenados de C, basta aplicar el axioma de especificación al anterior conjunto D para obtener:

$$A = \{a \in D : \text{ existe } b \text{ tal que} (a,b) \in C\}$$

y

$$B = \{b \in D : \text{ existe } a \text{ tal que} (a,b) \in C\}.$$

Sabemos que, en general, $A \times B \neq B \times A$. El lector ya supondrá cuándo se da la igualdad.

Proposición 4.2.5 *Dados dos conjuntos A y B, $A \times B = B \times A$ si y sólo si $A = \emptyset$, o $B = \emptyset$ o $A = B$.*

Demostración. La condición suficiente es obvia a partir de la proposición 4.2.2. Veamos la otra implicación.

Sea ahora $A \times B = B \times A$. Si A o B son vacíos, no hay nada que demostrar. Supongamos entonces, que tanto A como B son no vacíos. Cualesquiera que sean $a \in A$ y $b \in B$ se tiene que $(a,b) \in A \times B$ y como, por hipótesis, $A \times B = B \times A$ resulta que $(a,b) \in B \times A$, de donde $a \in B$ y $b \in A$. Luego

$$A \subseteq B \quad \text{y} \quad B \subseteq A,$$

por lo que concluimos que $A = B$.

■

Veamos seguidamente algunas propiedades.

Proposición 4.2.6 *Si A, B y C son conjuntos, se verifica que:*

1. $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Demostración. Probaremos el primer aserto, dejando el otro como ejercicio.

Si alguno de los conjuntos es vacío, se tiene de inmediato que la propiedad enunciada es correcta, pues en ambos lados de la igualdad se tiene el conjunto $\emptyset$.

Si $B \cap C = \emptyset$, entonces $A \times (B \cap C) = \emptyset$ y $(A \times B) \cap (A \times C) = \emptyset$ también, pues de lo contrario existiría $(x, y) \in A \times B$ y $(x, y) \in A \times C$, de donde $x \in A$ e $y \in B \cap C$, lo que es absurdo.

Consideraremos entonces el caso en que ningún conjunto es vacío y que B y C no son disjuntos. Demostraremos la *propiedad distributiva del producto cartesiano respecto de la intersección* mediante doble inclusión.

Sea $(x, y) \in A \times (B \cap C)$, por lo que $x \in A$ e $y \in B \cap C$. Al ser $x \in A$ e $y \in B$, se tiene que $(x, y) \in A \times B$. De la misma forma, puesto que $y \in C$, se tendrá que $(x, y) \in A \times C$. Por tanto, $(x, y) \in (A \times B) \cap (A \times C)$ y así $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$.

Veamos la otra inclusión. Sea $(x, y) \in (A \times B) \cap (A \times C)$, por lo que tendremos que $(x, y) \in (A \times B)$ y $(x, y) \in (A \times C)$. De aquí que $x \in A$, $y \in B$ e $y \in C$, de donde $x \in A$ e $y \in B \cap C$, luego $(x, y) \in A \times (B \cap C)$. Por tanto $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$. Finalmente la propiedad antisimétrica de la inclusión nos permite obtener la igualdad buscada.

■

Ejercicios

1. Sean $A = \{x \in \mathbb{N} : 3 \leq x \leq 7\}$ y $B = \{5, 6, 7\}$

   (a) Determinar $A \times B$.

   (b) Sea $R \subseteq A \times B$ con $R = \{(x, y) \in A \times B : x + y \leq 11\}$. Definir R por extensión y representar $A \times B$ y R.

2. Sea $\mathbb{R}$ el conjunto de los números reales, ¿es cierto que $\mathbb{R} \subseteq \mathbb{R} \times \mathbb{R}$? Contestar razonadamente.

3. Probar que $(A_1 \times B_1) \cap (A_2 \times B_2) = (A_1 \cap A_2) \times (B_1 \cap B_2)$.

4. Demostrar que $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

5. ¿Qué error hay en la demostración del siguiente falso enunciado?:

   Cualesquiera que sean los conjuntos A, B, C y D, se verifica que: $(A \cup C) \times (B \cup D) \subseteq (A \times B) \cup (C \times D)$.

Demostración: *Supongamos que* $(x, y) \in (A \cup C) \times (B \cup D)$, *entonces* $x \in A \cup C$ *e* $y \in B \cup D$. *Así que, o bien* $x \in A$ *o* $x \in C$ *y, además, o* $y \in B$ *o* $y \in D$. *En el primer caso,* $x \in A$ *e* $y \in B$, *luego* $(x, y) \in A \times B$. *En el segundo,* $x \in C$ *e* $y \in D$, *así que* $(x, y) \in C \times D$. *En cualquier caso:* $(x, y) \in (A \times B) \cup (C \times D)$.

6. Demostrar que $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
7. Demostrar que $C \times D \subseteq A \times B$ si y sólo si $C \subseteq A$ y $D \subseteq B$.
8. Demostrar que $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.
9. Probar que si $(A \times B) \cap (C \times D) = \emptyset$, entonces $A \cap C = \emptyset$ o $B \cap D = \emptyset$.
10. Sean los subconjuntos A, B de un cierto conjunto U. Demostrar que

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

4.3 Relaciones binarias

Pensemos en todas las ciudades y países del mundo y consideremos pares ordenados (x, y), en los que x es una ciudad e y un país. Con (x, y) indicamos que la ciudad x está en el país y. Por ejemplo (Cádiz, España) o (Londres, Gran Bretaña). Conociendo la "relación" x está en y, conocemos el conjunto de pares ordenados que ella determina.

Y, aún más, si tenemos un conjunto de pares ordenados conocemos la "relación". Si nada supiéramos de geografía y nos dieran el conjunto de pares ordenados (x, y), siendo x una ciudad e y un país, podríamos siempre decir con seguridad cuando una ciudad está en un determinado país y cuando no, con sólo comprobar si el par ordenado correspondiente pertenece o no al conjunto.

Por lo dicho, es claro que intuitivamente podemos entender una "relación" entre ciertos objetos como un concepto estrechamente vinculado con un conjunto de pares ordenados; de forma que una "relación" queda determinada por un conjunto de pares ordenados y que un tal conjunto determina una cierta "relación".

De forma más general, sean A y B dos conjuntos y $P(x, y)$ un predicado relativo a los elementos $x \in A$ e $y \in B$, en ese orden; es decir, una expresión caracterizada por ser $P(a, b)$ cierta o falsa para cualquier par ordenado $(a, b) \in A \times B$. Este predicado determina un subconjunto de $A \times B$, el de aquellos pares ordenados (x, y) para los que $P(x, y)$ es verdadera. Es decir:

Si $\mathcal{R}$ *es el conjunto determinado por* $P(x, y)$, *se tiene que* $(x, y) \in \mathcal{R}$ *si y sólo si* $P(x, y)$ *es verdadero. Cuando* $P(a, b)$ *es falso se tendrá que* $(a, b) \notin \mathcal{R}$.

Ejemplo 4.3.1

1. Sean A el conjunto de asignaturas de Matemáticas de la Facultad y P el de profesores, entonces si $P(x, y)$ significa "x es impartida por y", se trata de una relación entre A y P.
2. Sean $A = B$ el conjunto de rectas del plano y $P(x, y)$ el predicado "x es paralela a y", que es una relación entre A y A.

□

Definición 4.3.2 *Dados dos conjuntos A y B, una relación de A a B es un subconjunto $\mathcal{R}$ de $A \times B$. Decimos que $x \in A$ e $y \in B$ están relacionados mediante $\mathcal{R}$ si $(x, y) \in \mathcal{R}$ y que no están relacionados mediante $\mathcal{R}$ si $(x, y) \notin \mathcal{R}$.*

Para indicar que x e y están relacionados, es más usual escribir $x \mathcal{R} y$ que $(x, y) \in \mathcal{R}$ y, del mismo modo, para indicar que no lo están se suele escribir $x \not\mathcal{R} y$.

Ya que $\emptyset$ es subconjunto de cualquier conjunto, se tiene que determina una relación binaria, que se denomina "relación vacía".

$\mathcal{R} = A \times B$ es otro ejemplo, igualmente aburrido, de relación entre A y B. Afortunadamente, además de estos casos triviales, hay otros ejemplos más interesantes.

Ejemplo 4.3.3

1. Sean $A = \{2, 3\}$ y $B = \{3, 4, 5, 6\}$ y la relación determinada por el predicado "x divide a y". La relación es
$$\mathcal{R} = \{(2, 4), (2, 6), (3, 3), (3, 6)\} \subseteq A \times B.$$
2. $\mathcal{R} = \{(x, y) \in \mathbb{R}^2 : x > y\}$ determina una relación en $\mathbb{R}$ (de $\mathbb{R}$ a $\mathbb{R}$) y podemos decir, por ejemplo, que $3 \mathcal{R} 2$, mientras que $3 \not\mathcal{R} 5$.
3. Consideremos $A = \{1, 2\}$ y $B = \mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ y sea
$$\mathcal{R} = \{(x, y) \in A \times B : x \in y\}.$$
Entonces la relación dada, expresada por extensión, es
$$\mathcal{R} = \{(1, \{1\}), (1, \{1, 2\}), (2, \{2\}), (2, \{1, 2\})\}.$$
4. Sean $A = B = \mathbb{R}$ y la relación $\mathcal{R} = \{(x, y) \in \mathbb{R}^2 : y > x^2\}$, entonces esta relación viene determinada por el conjunto de puntos del plano que se encuentran entre las dos ramas de la parábola $y = x^2$, tal y como se indica en la Figura 4.3.

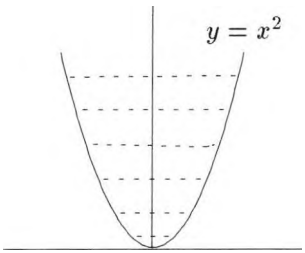


Figura 4.3: Relación "$y > x^2$"

5. Para un cierto conjunto A, la relación de igualdad entre los elementos de A, viene dada por $\mathcal{R} = \{(x, y) \in A \times A : x = y\}$.

6. Para un cierto conjunto A, la relación de pertenencia entre los elementos de A y los subconjuntos de A, es $\mathcal{R} = \{(x, X) \in A \times \mathcal{P}(A) : x \in X\}$. Si $x \in A$ y $X \in \mathcal{P}(A)$, entonces decir $x \mathcal{R} X$ es lo mismo que decir que $x \in X$.

□

4.3.1 Dominio, rango y relación inversa

Definición 4.3.4 *Dada una relación $\mathcal{R}$ de A a B, los conjuntos:*

$$Dom\ (\mathcal{R}) = \{x \in A : \text{existe } y \in B \text{ tal que } (x, y) \in \mathcal{R}\},$$

$$Rang\ (\mathcal{R}) = \{y \in B : \text{existe } x \in A \text{ tal que } (x, y) \in \mathcal{R}\},$$

se denominan, respectivamente, dominio y rango de la relación.

Ejemplo 4.3.5

1. Para $A = \{2, 3\}$, $B = \{3, 4, 5, 6\}$ y $\mathcal{R} = \{(2, 4), (2, 6), (3, 3), (3, 6)\}$, se tiene que $Dom\ (\mathcal{R}) = \{2, 3\} = A$ y $Rang\ (\mathcal{R}) = \{3, 4, 6\} \subsetneq B$.

2. Para $\mathbb{R} = A = B$ y $\mathcal{R} = \{(x, y) : x > y\}$, se tiene que

$$Dom\ (\mathcal{R}) = Rang\ (\mathcal{R}) = \mathbb{R}.$$

3. Si $A = \{1, 2\}$, $B = \mathcal{P}(A)$ y $\mathcal{R} = \{(x, y) : x \in y\}$, entonces

$$Dom\ (\mathcal{R}) = \{1, 2\} = A \text{ y } Rang\ (\mathcal{R}) = \{\{1\}, \{2\}, \{1, 2\}\}.$$

4. Si $A = B = \mathbb{R}$ y $\mathcal{R} = \{(x, y) \in \mathbb{R}^2 : y > x^2\}$, entonces

$$Dom\ (\mathcal{R}) = \mathbb{R} \text{ y } Rang\ (\mathcal{R}) = \{x \in \mathbb{R} : x > 0\}.$$

□

Definición 4.3.6 *Si $\mathcal{R}$ es una relación binaria entre A y B, se denomina relación inversa de ella y se denota por $\mathcal{R}^{-1}$, a la relación de B a A dada por*

$$\mathcal{R}^{-1} = \{(y, x) \in B \times A : (x, y) \in \mathcal{R}\}.$$

Ejemplo 4.3.7 Si $A = \{2, 3\}$ y $B = \{3, 4, 5, 6\}$ y $\mathcal{R}$ es la relación definida por "x divide a y", entonces $\mathcal{R}^{-1} = \{(4, 2), (6, 2), (3, 3), (6, 3)\}$, que representa los números de B que son múltiplos de 2 o de 3. □

4.3.2 Relaciones definidas en un conjunto

Cuando $A = B$, se dice que $\mathcal{R} \subseteq A \times B$ es una *relación definida en A* o *sobre A*.

Definición 4.3.8 *Sea $\mathcal{R}$ una relación sobre A, decimos que es:*

1. **Reflexiva**, *si $x\ \mathcal{R}\ x$ cualquiera que sea $x \in A$.*
2. **Simétrica**, *si para cualesquiera $x, y \in A$ tales que $x\ \mathcal{R}\ y$ se sigue que $y\ \mathcal{R}\ x$.*
3. **Antisimétrica**, *si para cualesquiera $x, y \in A$ tales que $x\ \mathcal{R}\ y$ e $y\ \mathcal{R}\ x$, se sigue que $x = y$.*
4. **Transitiva**, *si para cualesquiera $x, y, z \in A$ tales que $x\ \mathcal{R}\ y$ e $y\ \mathcal{R}\ z$, se sigue que $x\ \mathcal{R}\ z$.*

Ejemplo 4.3.9

1. Consideremos en $\mathbb{R}$ la relación $\mathcal{R}$ definida por $x\ \mathcal{R}\ y$ si y sólo si $x - y \in \mathbb{Z}$. Esta relación es reflexiva, pues $x - x = 0 \in \mathbb{Z}$; es simétrica pues si $x - y \in \mathbb{Z}$, entonces $y - x = -(x - y) \in \mathbb{Z}$; es transitiva, pues de $x\ \mathcal{R}\ y$ y de $y\ \mathcal{R}\ z$, se sigue que $x - y, y - z \in \mathbb{Z}$, por lo que sumando ambos se tiene que $x - z \in \mathbb{Z}$, luego $x\ \mathcal{R}\ z$; y, finalmente, no es antisimétrica, así, por ejemplo, $2\ \mathcal{R}\ 4$ y $4\ \mathcal{R}\ 2$, pero $2 \neq 4$.
2. En $\mathbb{N}$ consideramos la relación definida por $x\ \mathcal{R}\ y$ si y sólo si $x < y$. Claramente no es reflexiva, ni simétrica, pero si es transitiva.

3. Sea A un conjunto y consideremos $\mathcal{P}(A)$ y en él la relación $X \mathcal{R} Y$ si y sólo si $X \subseteq Y$. La relación es reflexiva pues todo conjunto es subconjunto de sí mismo; es transitiva, pues si $X \subseteq Y$ e $Y \subseteq Z$, se tiene que $X \subseteq Z$ y, por último, es antisimétrica, pues si $X \subseteq Y$ e $Y \subseteq X$, entonces $X = Y$.

□

4.3.3 Representación gráfica de relaciones

Cuando los conjuntos son finitos se pueden representar las relaciones mediante algún diagrama que ayude a entender el tipo de relación ante el que nos encontramos y sus propiedades. Ello puede hacerse mediante:

1. Un diagrama de Venn, en el que los elementos de A relacionados con los de B se unen mediante flechas "orientadas", con origen en el elemento de A y fin en el elemento de B.

2. Un gráfico cartesiano, situando sobre el eje de ordenadas los elementos de B y los de A sobre el de abscisas, y encerrando los pares de la relación en un recinto cerrado.

3. Una matriz de unos y ceros, asignando un 1 cuando los elementos están relacionados y 0 en caso contrario.

4. Un grafo dirigido, para el caso de relaciones definidas sobre un conjunto A, representando dicho conjunto y uniendo mediante flechas los elementos relacionados.

Ejemplo 4.3.10 Sean $A = \{a, b, c\}$, $B = \{1, 2\}$ y la relación

$$\mathcal{R} = \{(a, 1), (a, 2), (c, 2)\}.$$

Podemos representar esta relación mediante:

1. Un diagrama de Venn, como se puede ver en la Figura 4.4.

2. Un gráfico cartesiano, en la forma que se indica en la Figura 4.5

3. Una matriz de ceros y unos:

$\mathcal{R}$	1	2
a	1	1
b	0	0
c	0	1

.

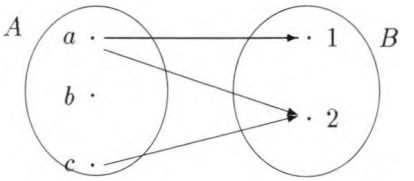


Figura 4.4: Diagrama de Venn

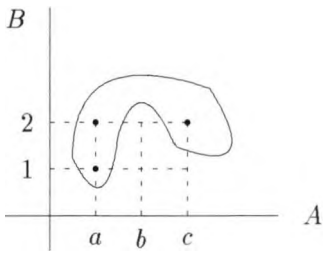


Figura 4.5: Gráfico cartesiano

□

Ejemplo 4.3.11 Sea $A = \{1, 2\}$ y consideremos en $B = \mathcal{P}(A)$ la relación $\mathcal{R} = \{(x, y) \in B \times B : x \subseteq y\}$; es decir:

$$\begin{aligned}\mathcal{R} = \{&(\emptyset, \emptyset), (\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{1, 2\}), (\{1\}, \{1\}),\\ &(\{1\}, \{1, 2\}), (\{2\}, \{2\}), (\{2\}, \{1, 2\}), (\{1, 2\}, \{1, 2\})\}.\end{aligned}$$

La representación sería la indicada en la Figura 4.6

Notemos que hay una flecha de $\emptyset$ a $\emptyset$, etc., lo que indica que esos elementos están relacionados consigo mismos. □

Ejercicios

1. ¿Qué propiedades cumple la relación, sobre $\mathbb{R}$, $x \leq y$?
2. Sea $\mathbb{N}$ con la relación "a es divisor de b", que denotaremos por $a|b$. ¿Qué propiedades verifica?
3. En $\mathbb{Z}$ se define la relación $x \mathcal{R} y$ si y sólo si $x^2 + x = y^2 + y$. Estudiar $\mathcal{R}$.

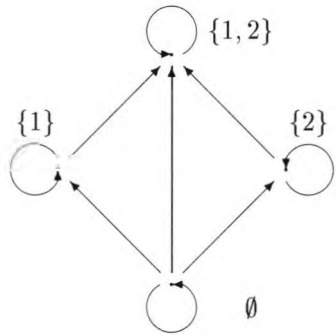


Figura 4.6: Grafo dirigido

4. Sean $\mathcal{R}$ y $\mathcal{S}$ dos relaciones sobre un conjunto A. Para cada uno de los casos siguientes, dar una demostración o un contraejemplo que justifique la respuesta.

   (a) Si $\mathcal{R}$ y $\mathcal{S}$ son reflexivas, ¿lo es $\mathcal{R} \cap \mathcal{S}$?, ¿y $\mathcal{R} \cup \mathcal{S}$?

   (b) Si $\mathcal{R}$ y $\mathcal{S}$ son transitivas, ¿lo es $\mathcal{R} \cap \mathcal{S}$?, ¿y $\mathcal{R} \cup \mathcal{S}$?

   (c) Si $\mathcal{R}$ y $\mathcal{S}$ son antisimétricas, ¿lo es $\mathcal{R} \cap \mathcal{S}$?, ¿y $\mathcal{R} \cup \mathcal{S}$?

5. ¿Puede una relación simétrica ser antisimétrica? (Contestar razonadamente y proporcionar algún ejemplo).

6. Consideremos el siguiente enunciado:

   Sea $\mathcal{R}$ una relación sobre A. Si $\mathcal{R}$ es simétrica y transitiva, entonces $\mathcal{R}$ es reflexiva.

   del que se ha proporcionado la siguiente demostración:

   Sea $x \in A$ un elemento cualquiera de A y sea $y \in A$ tal que

   $$x \mathcal{R} y, \tag{4.1}$$

   como $\mathcal{R}$ es simétrica se sigue que

   $$y \mathcal{R} x \tag{4.2}$$

   y como $\mathcal{R}$ es transitiva, de (4.1) y (4.2), se sigue que $x \mathcal{R} x$, siendo x un elemento arbitrario de A, por lo que $\mathcal{R}$ es reflexiva.

   (a) ¿Es correcta la demostración? Caso de no serlo señalar el error y si lo es identificar el tipo de demostración realizada.

(b) ¿Es el enunciado correcto?

7. Sean $A = \{1, 2, 3, 4, 5\}$, $B = \{1, 4, 6, 16\}$ y $C = \{2, 3, 8, 10\}$ y las relaciones: $\mathcal{R} \subseteq A \times B$ y $\mathcal{S} \subseteq B \times C$, definidas mediante:

$$(x, y) \in \mathcal{R} \quad \text{si y sólo si} \quad y = x^2,$$

$$(x, y) \in \mathcal{S} \quad \text{si y sólo si} \quad y = \frac{x}{2}.$$

(a) Determinar $\mathcal{R}$ y $\mathcal{S}$ por extensión.

(b) Determinar los dominios y rangos de las dos relaciones.

8. Obtener los gráficos cartesianos de las siguientes relaciones definidas en $\mathbb{R}$:

(a) $(x, y) \in \mathcal{R}$ si y sólo si $y = 3$.

(b) $(x, y) \in \mathcal{S}$ si y sólo si $x + y = 1$.

(c) $(x, y) \in \mathcal{T}$ si y sólo si $x + y < 1$.

9. Dada una relación $\mathcal{R}$ y su inversa $\mathcal{R}^{-1}$, demostrar que $\mathcal{R} \cup \mathcal{R}^{-1}$ es siempre una relación simétrica. Demostrar que si $\mathcal{R}$ es simétrica, también lo es $\mathcal{R}^{-1}$ y que si $\mathcal{R}$ es transitiva también lo es $\mathcal{R}^{-1}$.

4.4 Relación de equivalencia

Es frecuente encontrarse con conjuntos, en los que, desde un cierto punto de vista, unos elementos pueden considerarse "equivalentes" a otros, "como si se tratasen de una misma cosa". Este es el caso de las fracciones $\frac{3}{5}$ y $\frac{6}{10}$, o el de dos vectores del plano que tienen el mismo módulo, dirección y sentido. Estos casos hacen referencia a ciertos conjuntos, el conjunto de las fracciones y el de los vectores del plano, respectivamente, y a unas relaciones sobre ellos:

$$\frac{a}{b} \; \mathcal{R} \; \frac{c}{d} \quad \text{si y sólo si} \quad a \cdot d = b \cdot c$$

y

$$\vec{x} \; \mathcal{R} \; \vec{y} \quad \text{si y sólo si} \quad \vec{x} \text{ es equipolente con } \vec{y}.$$

En ambos casos las relaciones tienen las propiedades reflexiva, simétrica y transitiva.

Definición 4.4.1 *Una relación $\mathcal{R}$ sobre un conjunto A se dice que es de equivalencia si es reflexiva, simétrica y transitiva.*

La relación, no vacía, de equivalencia "más pequeña" sobre un conjunto A es la relación de igualdad en A y la "más grande" precisamente $A \times A$. En lo que sigue, toda relación $\mathcal{R}$ de equivalencia que se contemple se considerará no vacía.

Ejemplo 4.4.2

1. En $A = \{1, 2, 3\}$, $\mathcal{R} = \{(1,1), (2,2), (3,3), (2,3), (3,2)\}$ es de equivalencia.

2. En $\mathbb{N} \times \mathbb{N}$, consideramos la relación dada por

$$a + d = b + c \quad \text{para} \quad (a, b), (c, d) \in \mathbb{N} \times \mathbb{N},$$

que es: reflexiva, puesto que $a+b = b+a$; claramente simétrica y finalmente transitiva, pues si $(a, b)\ \mathcal{R}\ (c, d)$ y $(c, d)\ \mathcal{R}\ (e, f)$, entonces $a + d = b + c$ y $c + f = d + e$, y sumando, miembro a miembro, ambas igualdades se tiene que $a + d + c + f = b + c + d + e$, de donde $a + f = b + e$, por lo que $(a, b)\ \mathcal{R}\ (e, f)$.

3. En $\mathbb{Z} \times \mathbb{Z}$, la relación determinada por $a \cdot d = b \cdot c$ para $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$, es una relación de equivalencia, como puede comprobarse fácilmente.

□

Existe una estrecha conexión entre las relaciones de equivalencia sobre un conjunto A y las particiones de dicho conjunto.

Definición 4.4.3 *Dados un conjunto $A \neq \emptyset$ y una relación $\mathcal{R}$ de equivalencia sobre él, si $a \in A$, el subconjunto de A: $[a] = \{x \in A : x\ \mathcal{R}\ a\}$ se denomina la clase de equivalencia de a respecto la relación $\mathcal{R}$, recibiendo a el nombre de representante de la clase $[a]$.*

Desde luego, dos elementos cualesquiera de una clase están relacionados entre sí, ya que si $b, c \in [a]$, entonces $b\ \mathcal{R}\ a$ y $c\ \mathcal{R}\ a$ y, en virtud de las propiedades simétrica y transitiva, se tiene que $b\ \mathcal{R}\ c$.

Proposición 4.4.4 *Dos clases de equivalencia o son disjuntas o coinciden.*

Demostración. En efecto, si $[a] \cap [b] \neq \emptyset$, entonces existe $x \in [a] \cap [b]$, por lo que $x\ \mathcal{R}\ a$ y $x\ \mathcal{R}\ b$, de donde

$$a\ \mathcal{R}\ b. \tag{4.3}$$

Ahora bien, si $y \in [a]$, se tiene que $y\ \mathcal{R}\ a$ y, en virtud de (4.3), obtenemos que $y\ \mathcal{R}\ b$, de donde $y \in [b]$; es decir $[a] \subseteq [b]$. Del mismo modo, si $y \in [b]$, se tiene que $y\ \mathcal{R}\ b$ y, en virtud de (4.3) y de la propiedad simétrica, obtenemos que $y\ \mathcal{R}\ a$, de donde $y \in [a]$; es decir $[b] \subseteq [a]$. La propiedad antisimétrica de la inclusión nos permite concluir que $[a] = [b]$.

■

Proposición 4.4.5 *Si $\mathcal{R}$ es una relación de equivalencia sobre un conjunto $A \neq \emptyset$, entonces determina una partición de A en clases de equivalencia.*

Demostración. Como acabamos de ver anteriormente, si $[x] \neq [y]$, entonces $[x] \cap [y] = \emptyset$.

Cualquiera que sea la clase considerada $[x]$, se tiene que $[x] \neq \emptyset$, pues obviamente $x \in [x]$. Por último, es claro que $\bigcup_{x \in A} [x] = A$. Concluimos que efectivamente el conjunto de las clases de equivalencia determinadas por $\mathcal{R}$ es una partición de A.

■

De lo dicho, es evidente que puede tomarse como representante de una clase de equivalencia a cualquiera de los elementos que la componen.

Es claro que las clases de equivalencia determinadas por una relación $\mathcal{R}$ de equivalencia sobre un conjunto $A \neq \emptyset$ son subconjuntos de A, por lo que el conjunto de todas ellas será un subconjunto de $\mathcal{P}(A)$.

Definición 4.4.6 *El conjunto de las clases de equivalencia que determina una relación de equivalencia $\mathcal{R}$ sobre un conjunto A se denomina conjunto cociente de A por $\mathcal{R}$ y lo denotaremos mediante $A/\mathcal{R}$.*

Ejemplo 4.4.7

1. En el caso de la relación definida en 1 del Ejemplo 4.4.2, hay dos clases: $[1] = \{1\}$ y $[2] = \{2, 3\} = [3]$ y el conjunto cociente será:

$$A/\mathcal{R} = \{[1], [2]\} = \{\{1\}, \{2, 3\}\}.$$

2. Sea $A = \{0, 1, \ldots, 9\}$. Consideremos la relación sobre A dada por $a \mathcal{R} b$ si y sólo si $a - b = \dot{3}$.

   La relación es reflexiva pues $a - a = 0 = \dot{3}$. Es simétrica ya que si $a - b = \dot{3}$, obviamente también lo es $b - a$. Finalmente, es transitiva, ya que si $a \mathcal{R} b$, entonces $a - b = \dot{3}$ y si $b \mathcal{R} c$, entonces $b - c = \dot{3}$ y la diferencia de ambos también será múltiplo de 3, $a - c = \dot{3}$.

   El conjunto cociente es $A/\mathcal{R} = \{[0], [1], [2]\}$, siendo: $[0] = \{0, 3, 6, 9\}$, $[1] = \{1, 4, 7\}$ y $[2] = \{2, 5, 8\}$.

3. Consideremos el conjunto $\mathbb{Z}$ de los enteros y sea $m \in \mathbb{Z}^+$ un entero positivo fijo. Definimos en $\mathbb{Z}$ la relación $\mathcal{R}$ determinada por:

$$a \mathcal{R} b \text{ si y sólo si } m|(b - a).$$

   Esta relación es: reflexiva, puesto que $m|0$; simétrica, ya que si $m|(b - a)$ también se verifica que $m|(a - b)$; y es transitiva, pues si m es divisor de

dos números también lo es de su suma, así que de $a \mathcal{R} b$ y $b \mathcal{R} c$ se sigue que $m|(b-a)$ y $m|(c-b)$, por lo que $m|(c-a)$, de donde $a \mathcal{R} c$.

Las clases de equivalencia son de la forma:

$$[a] = \{x \in \mathbb{Z} : m|(x-a)\} = \{x \in \mathbb{Z} : x = a+km, \text{con } k \in \mathbb{Z}\} = \{a+\dot{m}\}.$$

Así la clase del 0 es: $[0] = \{\ldots, -2m, -m, 0, m, 2m, \ldots\}$. El conjunto cociente es $\mathbb{Z}/\mathcal{R} = \{[0], [1], \ldots, [m-1]\}$.

Esta relación recibe el nombre de "relación de congruencia módulo m". Para indicar que a y b están relacionados se suele escribir $a \equiv b$ (mód. m) o también $a \equiv b \,_{(m}$ y se lee "a es congruente con b módulo m".

□

Hemos visto que toda relación de equivalencia determina una partición. Veamos ahora que también toda partición de un conjunto determina una relación de equivalencia sobre el mismo. Dos elementos $a, b \in A$ están relacionados si y sólo si pertenecen al mismo subconjunto de la partición.

Proposición 4.4.8 *Sea A un conjunto no vacío y sea $\mathcal{C}$ una partición de A, entonces existe una relación de equivalencia $\mathcal{R}$ sobre A cuyo conjunto cociente es precisamente $\mathcal{C}$.*

Demostración. Sea $\mathcal{R}$ la relación sobre A dada por "cualesquiera que sean $x, y \in A$, $x \mathcal{R} y$ si y sólo si x e y pertenecen al mismo subconjunto, elemento de la partición".

Las propiedades reflexiva y simétrica son inmediatas. Veamos la transitividad: si $x \mathcal{R} y$, entonces x e y pertenecen a un mismo elemento de la partición, llamémosle D, e $y \mathcal{R} z$, entonces y y z pertenecen a un mismo elemento de la partición, llamémosle E; pero entonces $y \in D \cap E$, pero $D, E \in \mathcal{C}$, que es una partición, luego $D = E$, por lo que $x \mathcal{R} z$. Consecuentemente $\mathcal{R}$ es de equivalencia y la clase de equivalencia de x es el elemento de la partición $\mathcal{C}$ que lo contiene, por lo que $A/\mathcal{R} = \mathcal{C}$.

■

Ejercicios

1. Si A es el conjunto de las rectas del plano y $\mathcal{R}$ es la relación de paralelismo, ¿quién es el conjunto cociente?
2. En $\mathbb{N}$, la relación de congruencia módulo 2, ¿qué partición determina?
3. ¿Qué relación determina en $\mathbb{R} \setminus \{0\}$, la partición en números positivos y negativos?

4. El conjunto $\{\{1\},\{2,3\},\{4\}\}$ es una partición de $\{1,2,3,4\}$. Obtener la relación de equivalencia asociada.

5. (a) En $A=\{1,2,3,4\}$ se considera la relación

$$\mathcal{R} =\{(x,y)\in A\times A:\ x=y \text{ o } x+y=3\}$$

Determinar $\mathcal{R}$ por extensión, probar que es de equivalencia y determinar la correspondiente partición de A.

(b) Consideremos ahora la anterior relación $\mathcal{R}$ extendida a todo $\mathbb{R}$. Probar que es de equivalencia, determinar el conjunto cociente y la clase de equivalencia del número 201.

6. En $\mathbb{R}\setminus\{0\}$ se define la relación:

$$a\ \mathcal{R}\ b \text{ si y sólo si } a+\frac{1}{a}=b+\frac{1}{b}.$$

Probar que $\mathcal{R}$ es una relación de equivalencia. Determinar la expresión de las clases de equivalencia.

7. Sean $A=\{a\in\mathbb{N}:\ a\leq 10\}$ y $B=\{x\in\mathcal{P}(A):\ \text{card}(x)\geq 8\}$, donde $\text{card}(x)$ se lee "cardinal de x" y es el número de elementos que tiene el subconjunto x de A. Se define en B la relación:

$$x\ \mathcal{R}\ x' \text{ si y sólo si } x\cap x'\neq\emptyset.$$

Probar que es de equivalencia y determinar el conjunto cociente.

8. En $\mathbb{R}$ se define:

$$\mathcal{R} =\{(x,y)\in\mathbb{R}^2:\ |x-1|=|y-1|\}.$$

Probar que se trata de una relación de equivalencia y representar la relación.

9. Se dice que una relación $\mathcal{R}$ definida en un conjunto A es circular si y sólo si de $(a,b)\in\mathcal{R}$ y $(b,c)\in\mathcal{R}$ se deduce que $(c,a)\in\mathcal{R}$. Demostrar que una relación es reflexiva y circular si y sólo si es de equivalencia.

10. Dado $A=\{1,2,3\}$ y $B=\{1\}$, se considera el conjunto $\mathcal{P}(A)$ y en él la siguiente relación:

$$P\ \mathcal{R}\ Q \text{ si y sólo si } P\cap B=Q\cap B.$$

Probar que es de equivalencia y determinar el conjunto cociente.

11. Encontrar todas las relaciones de equivalencia que se puedan definir en el conjunto $A=\{1,2,3\}$. Si A es un conjunto con n elementos, ¿cuántas relaciones de equivalencia distintas se pueden definir en A?

12. Sea $\mathcal{R}$ una relación de equivalencia sobre A y sea $\mathcal{F} = A/\mathcal{R}$. Sea $\mathcal{S}$ la relación de equivalencia determinada por $\mathcal{F}$. Demostrar que $\mathcal{S}$ y $\mathcal{R}$ coinciden.

13. Supongamos que $\mathcal{R}$ y $\mathcal{S}$ son dos relaciones de equivalencia sobre A y que $A/\mathcal{R} = A/\mathcal{S}$. Demostrar que $\mathcal{R} = \mathcal{S}$.

14. Supongamos que $\mathcal{R}$ y $\mathcal{S}$ son dos relaciones de equivalencia sobre A. ¿Lo es $\mathcal{R} \cap \mathcal{S}$?, ¿y $\mathcal{R} \cup \mathcal{S}$?

15. Sea $\mathcal{R}$ una relación reflexiva y transitiva sobre A. Sea $\mathcal{S} = \mathcal{R} \cap \mathcal{R}^{-1}$. Probar que $\mathcal{S}$ es una relación de equivalencia.

16. En $\mathbb{R}$ se define la siguiente relación: $x \mathcal{R} y$ si y sólo si $E(x) = E(y)$, siendo $E(x)$ la función *parte entera de* x definida en $\mathbb{R}$.

    (a) Demostrar que se trata de una relación de equivalencia.

    (b) Determinar las clases de equivalencia y el conjunto cociente.

    Nota: es usual denotar *parte entera* de x mediante $[x]$. Para evitar posibles errores con la notación que hemos utilizado para las clases de equivalencia, hemos optado por denotarla por $E(x)$ (mayor entero menor o igual que x).

Capítulo 5

Relaciones de orden

5.1 Conjuntos ordenados

Si consideramos el conjunto $\mathbb{R}$ de los números reales y en él la relación "ser menor o igual", ésta verifica las propiedades reflexiva, antisimétrica y transitiva. Este orden *usual* en $\mathbb{R}$ es bien conocido de la enseñanza elemental. Otras relaciones en diversos conjuntos tienen idénticas propiedades; así si U es un conjunto no vacío y en $\mathcal{P}(U)$ consideramos la relación de "inclusión", sabemos que también es reflexiva, antisimétrica y transitiva y que nos permitía establecer "un orden" por el "tamaño" de los conjuntos, de forma que si $A \subseteq B$ podemos decir que "A precede a B" o también que "A es menor que B".

No obstante, en estos dos ejemplos, los conjuntos manifiestan un comportamiento distinto respecto de la relación. En el primer caso, siempre es posible, dados dos números $a, b \in \mathbb{R}$, indicar si $a \leq b$ o bien si $a \geq b$. En el segundo ejemplo, por el contrario, no siempre es posible "comparar" dos subconjuntos; en general no siempre es cierto que o bien $A \subseteq B$ o bien que $B \subseteq A$, cualesquiera que sean $A, B \in \mathcal{P}(U)$, para lo que basta pensar en dos subconjuntos, de U, distintos y unitarios.

Definición 5.1.1 *En un conjunto A, una relación $\mathcal{R}$ se llama de orden parcial si es reflexiva, antisimétrica y transitiva. Se dice que el par $(A, \mathcal{R})$ es un conjunto ordenado.*

Que $\mathcal{R}$ es de orden, en A, también suele señalarse con alguna de estas otras tres expresiones: $\mathcal{R}$ ha ordenado a A, $\mathcal{R}$ es una relación de orden sobre A, A es un conjunto ordenado mediante $\mathcal{R}$.

Usualmente simplemente diremos que $\mathcal{R}$ es una relación de orden, sobrentendiéndose que estamos hablando de orden parcial.

Si $\mathcal{R}$ es una relación de orden y $x \mathcal{R} y$, se dice que x *es anterior a* y o que

x precede a y, también puede decirse que *y es posterior a x* o que *y sigue a x*.

Cuando se tiene una sola relación $\mathcal{R}$ de orden sobre un conjunto A, para denotar que dos elementos x e y están relacionados suele escribirse $x \preceq y$, en lugar de $x \mathcal{R} y$, e incluso $x \leq y$, utilizando el propio símbolo $\leq$ del orden usual de $\mathbb{R}$, si no hay lugar a confusión. En esta circunstancia diremos que A está ordenado mediante $\preceq$. Para indicar que a no es anterior a b escribimos $a \not\preceq b$.

Si A es un conjunto ordenado, mediante $\preceq$, y $a, b \in A$ son tales que $a \preceq b$ y $a \neq b$, se dice que *a es estrictamente anterior a b* y lo denotaremos por $a \prec b$.

Ejemplo 5.1.2

1. En $\mathbb{Z}^+$ la relación "a es divisor de b", que denotaremos por $a|b$, es de orden. En efecto:

   - Es reflexiva, pues $a|a$ cualquiera que sea $a \in \mathbb{Z}^+$.
   - Si $a|b$, entonces $b = na$, para algún $n \in \mathbb{Z}^+$. Si $b|a$, entonces $a = kb$, para algún $k \in \mathbb{Z}^+$. De ambos se tiene que $b = nkb$, por lo que $nk = 1$, y siendo tanto k como n enteros positivos, se deduce que $k = n = 1$ y, por tanto, que $a = b$. Luego la relación es antisimétrica.
   - Si $a|b$ y $b|c$, se tiene que $b = na$, para algún entero positivo n y que $c = kb$, para algún entero positivo k, luego $c = kna$, para algún entero positivo kn, de donde $a|c$, resultando la relación transitiva.

2. Dada una semirrecta con origen en O, sus puntos pueden ordenarse mediante la relación:

   $$a \preceq b \text{ si y sólo si } d(O,a) \leq d(O,b),$$

   donde $d(O,x)$ indica la longitud del segmento de extremos O y x (lo que usualmente conocemos como distancia de O a x). Es fácil comprobar que efectivamente se trata de una relación de orden.

□

Definición 5.1.3 *Una relación $\mathcal{R}$ en A es asimétrica si $x \mathcal{R} y$ implica que $y \mathcal{R} x$ no se verifica, cualesquiera que sean $x, y \in A$.*

Definición 5.1.4 *Una relación $\mathcal{R}$ sobre un conjunto A se dice que es de orden estricto si es asimétrica y transitiva.*

Ejemplo 5.1.5 La relación "ser menor que" es una relación de orden estricto sobre $\mathbb{R}$. Pues si $x < y$ e $y < z$, entonces $x < z$ y si $x < y$ entonces no es posible que $y < x$. Y ello cualesquiera que sean $x, y, z \in \mathbb{R}$. □

Los siguientes resultados relacionan el orden y el orden estricto, poniendo de manifiesto que a partir de una relación de orden podemos definir una de orden estricto y viceversa.

Proposición 5.1.6 *Sea A un conjunto y $\mathcal{R}$ una relación de orden sobre él. Sea $\mathcal{S}$ una relación sobre A definida por: $x\ \mathcal{S}\ y$ si y sólo si $x\ \mathcal{R}\ y$ e $y \neq x$. Entonces $\mathcal{S}$ es una relación de orden estricto sobre A.*

Demostración. Veamos que $\mathcal{S}$ es transitiva. Si $x\ \mathcal{S}\ y$ e $y\ \mathcal{S}\ z$, se sigue de la definición de $\mathcal{S}$ que $x\ \mathcal{R}\ z$. Además $x \neq z$, pues de lo contrario se tendría que $x\ \mathcal{R}\ y$ e $y\ \mathcal{R}\ x$, de donde $x = y$, lo que no es posible, pues $x\ \mathcal{S}\ y$.

Veamos ahora que $\mathcal{S}$ es asimétrica. Si no lo fuera existirían $x, y \in A$ tales que $x\ \mathcal{S}\ y$ e $y\ \mathcal{S}\ x$. Pero entonces, de la definición de $\mathcal{S}$, se sigue que $x\ \mathcal{R}\ y$ e $y\ \mathcal{R}\ x$, por lo que $x = y$, siendo a la vez $x \neq y$.

■

Un proceso similar al anterior le permitirá al lector demostrar la siguiente proposición, con la que se cierra la relación anunciada entre orden y orden estricto.

Proposición 5.1.7 *Sea A un conjunto y $\mathcal{S}$ una relación de orden estricto sobre él. Sea $\mathcal{R}$ una relación sobre A definida por: $x\ \mathcal{R}\ y$ si y sólo si $x\ \mathcal{S}\ y$ o $x = y$. Entonces $\mathcal{R}$ es una relación de orden sobre A.*

En general una relación de orden sobre un conjunto A no permite "ordenar" todos los elementos del conjunto; es decir, no siempre es posible dados dos elementos cualesquiera establecer cual es anterior al otro. Este es el caso de la inclusión en $\mathcal{P}(U)$ y también el de la relación "ser divisor de" en $\mathbb{Z}^+$, pues para dos enteros positivos cualesquiera no siempre podremos decir que uno es divisor del otro, como por ejemplo pasa con 2 y 3. Esta circunstancia confiere un carácter especial a las relaciones que permiten ordenar todos los elementos del conjunto en el que está definida.

Dados $a, b \in A$ y una relación de orden $\preceq$ sobre el conjunto A, si $a \preceq b$ o $b \preceq a$, se dice que a y b son *comparables* mediante $\preceq$; en caso contrario se dirá que ambos elementos de A *no son comparables* mediante $\preceq$.

Cuando no haya lugar a dudas sobre el orden considerado, basta decir que los elementos son o no son comparables.

Definición 5.1.8 *Dado un conjunto A y una relación de orden $\preceq$ sobre A, se dice que A está totalmente ordenado mediante $\preceq$, o que $\preceq$ es una relación de orden total sobre A, si cualesquiera que sean $a, b \in A$ son comparables.*

Naturalmente, sobre un mismo conjunto se pueden definir distintas relaciones de orden y puede ocurrir que con una relación esté totalmente ordenado y con

otra no. Así si en $\mathbb{Z}^+$ consideramos el orden usual $\leq$, éste se trata de un orden total, mientras que si consideramos la relación "ser divisor de", el orden no es total.

Definición 5.1.9 *Si A es un conjunto ordenado mediante $\preceq$ y $B \subseteq A$ está totalmente ordenado mediante $\preceq$, se dice que B es una cadena.*

Ejemplo 5.1.10 Si consideramos $\mathbb{Z}^+$ ordenado mediante la relación "ser divisor de", entonces el conjunto de las potencias de 3 es una cadena, pues es claro que $\{x : x = 3^i,\ i \in \mathbb{N}\}$ está totalmente ordenado mediante dicha relación. □

5.1.1 Diagramas de Hasse

Los conjuntos finitos y ordenados se pueden representar mediante el llamado *diagrama de Hasse*, consistente en representar cada elemento del conjunto por un punto del plano o del espacio y uniendo cada par de "elementos consecutivos" mediante una flecha con sentido el que va del elemento anterior al posterior.

Definición 5.1.11 *Sea A un conjunto ordenado mediante la relación $\preceq$ y sea $x \in A$, entonces diremos que un elemento $y \in A$ es siguiente de x en A, respecto del orden $\preceq$, si se verifican las dos condiciones siguientes:*

1. *$x \prec y$.*
2. *Cualquiera que sea $z \in A$ tal que $x \prec z \preceq y$, entonces $z = y$.*

También se dice que los elementos x e y son consecutivos.

En un conjunto ordenado, un elemento puede no tener *siguiente*, o bien tener más de un elemento *siguiente*.

Ejemplo 5.1.12

1. Sea $A = \{2, 3, 6, 9, 12, 36\}$ ordenado por la relación "ser divisor de", que se trata de una relación de orden que no es total. Podemos observar que tanto 6 como 9 son elementos siguientes de 3. El correspondiente diagrama de Hasse es el que se indica en la Figura 5.1 y observemos en ella que $\{2, 6, 12, 36\}, \{3, 6, 12, 36\}, \{3, 9, 36\}, \{6, 12, 36\}, \{12, 36\}$, etc. son ejemplos de cadenas, de manera que toda "poligonal orientada" nos indica una cadena en A, con la relación de orden dada.
2. Sea $\mathbb{Q}$ con el orden usual "$\leq$", mediante el cual $\mathbb{Q}$ está totalmente ordenado, sin embargo ningún número racional tiene siguiente. En efecto sea $\frac{a}{b}$ y supongamos que $\frac{c}{d}$ es su siguiente; pero

$$\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d},$$

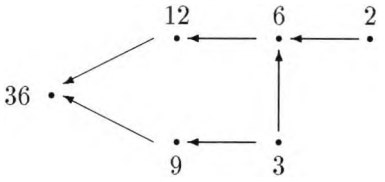


Figura 5.1: Diagrama de Hasse

llegando a contradicción. De hecho entre dos racionales cualesquiera existe una infinidad de racionales.

□

Para conjuntos totalmente ordenados la situación es bien diferente a la de 1 del ejemplo anterior, como vemos seguidamente.

Proposición 5.1.13 *Sea A totalmente ordenado, mediante la relación $\preceq$, si un elemento $x \in A$ tiene siguiente, entonces éste es único.*

Demostración. Sean $y, y' \in A$ dos elementos siguientes de x, respecto de $\preceq$, por lo que:

$$x \prec y \tag{5.1}$$

y

$$x \prec y' \tag{5.2}$$

y cualquiera que sea $z \in A$,

$$\text{si } x \prec z \preceq y, \text{ entonces } z = y \tag{5.3}$$

y

$$\text{si } x \prec z \preceq y', \text{ entonces } z = y'. \tag{5.4}$$

Toda vez que $\preceq$ es de orden total, se sigue que y e y' son comparables.

Si es $y \preceq y'$, como $x \prec y$, por (5.1), estamos en las condiciones de la premisa de (5.4), de donde tenemos que $y = y'$.

Si es $y' \preceq y$, como $x \prec y'$, por (5.2), estamos en las condiciones de la premisa de (5.3), de donde tenemos que $y' = y$.

Luego, en cualquier caso, el elemento siguiente es único.

■

Veamos otro ejemplo de diagrama de Hasse.

Ejemplo 5.1.14 Sea $D = \{1, 2, 3\}$ y consideramos $A = \mathcal{P}(D)$ con la relación de inclusión, que sabemos que es de orden parcial. El diagrama de Hasse es el de la Figura 5.2.

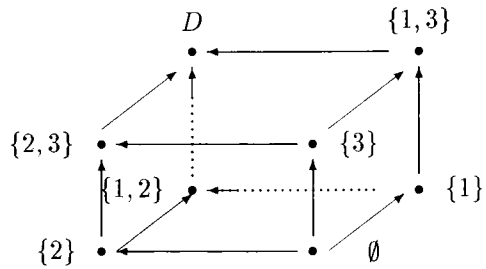


Figura 5.2: Diagrama de Hasse

Hemos de resaltar que el diagrama pone de relieve como $\emptyset$ está contenido en cualquier otro subconjunto, y como D contiene a todo subconjunto, pues cualquiera que sea la cadena considerada, ésta puede comenzar en $\emptyset$ y puede finalizar en D. Debemos también observar que para dos elementos cualesquiera de A, siempre hay otro elemento (subconjunto de D) que contiene a ambos y también hay otro elemento de A que está contenido en ambos; así, por ejemplo, para $\{1,3\}$ y $\{2,3\}$, $\{3\}$ es subconjunto de ambos y D los contiene. □

Ejercicios

1. ¿Son de orden las siguientes relaciones? En su caso, indicar si el orden es total:

   (a) Sea $A = \{1,2\}$ y $B = \mathcal{P}(A)$ y sea $\mathcal{R}$ la relación sobre B definida como sigue:

   $$x \mathcal{R} y \text{ si y sólo si } y \text{ tiene al menos tantos elementos como } x.$$

   (b) $\mathcal{R} = \{(x,y) \in \mathbb{R}^2 : x \geq y\}$.

2. Indicar cuándo $\mathcal{R}$ es o no un orden sobre A y, en su caso, el tipo de orden.

   (a) $A = \{a,b,c\}$, $\mathcal{R} = \{(a,a),(b,a),(b,b),(b,c),(c,c)\}$.
   (b) $A = \mathbb{R}$, $\mathcal{R} = \{(x,y) \in \mathbb{R}^2 : |x| \leq |y|\}$.
   (c) $A = \mathbb{R}$, $\mathcal{R} = \{(x,y) \in \mathbb{R}^2 : |x| < |y| \text{ o } x = y\}$.

3. Sea $A = \{1,2,3,4,5,6\}$ y la relación de orden dada por:

   $$\begin{aligned}\mathcal{R} = \{&(1,1),(2,2),(3,3),(4,4),(5,5),(6,2),(6,6),(6,5),\\ &(5,1),(1,2),(6,4),(4,1),(4,2),(3,2),(5,2),(6,1)\}.\end{aligned}$$

   Representar mediante un diagrama de Hasse la relación de orden.

4. Sea $\mathbb{N}$ con la relación de orden "ser divisor de". Sean los conjuntos

$$A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\} \text{ y } B = \{3, 4, 6, 12\}.$$

Representar mediante diagramas de Hasse, la relación en A y B.

5. En $\mathbb{Q}$ se define la relación:

$$x \mathcal{R} y \text{ si y sólo si existe } n \in \mathbb{N} \text{ tal que } y = x + n.$$

(En $\mathbb{N}$ consideramos incluido el 0).

(a) Demostrar que es de orden, ¿es orden total?

(b) Demostrar que si $x \mathcal{R} z$ e $y \mathcal{R} z$ entonces $x \mathcal{R} y$ o $y \mathcal{R} x$.

6. En el conjunto $\mathbb{C}$ de los números complejos se define la relación:

$$(a + bi) \mathcal{R} (c + di) \quad \text{si y sólo si} \quad \begin{cases} a < c \\ \text{o} \\ a = c \text{ y } b \leq d. \end{cases}$$

(a) Demostrar que $\mathcal{R}$ es de orden, ¿es de orden total?

(b) Ordenar los números: 1, $1 + i$, $3 - 4i$, 0, $1 - i$.

7. Sea $(\mathbb{R} \setminus \{0\}) \times \mathbb{R}$ y la relación:

$$(x_1, y_1) \mathcal{R} (x_2, y_2) \quad \text{si y sólo si} \quad \frac{y_1}{x_1} = \frac{y_2}{x_2} \text{ y } x_1 \leq x_2.$$

(a) Demostrar que es una relación de orden y estudiar si es orden total.

(b) Representar el conjunto de los puntos comparables con $(1, 1)$.

8. Demostrar que si A y B admiten orden total, entonces también lo admite $A \times B$.

9. Sean $\mathcal{R}$ y $\mathcal{S}$ dos relaciones de orden parcial sobre A y B, respectivamente. Definimos sobre $A \times B$ una relación $\mathcal{T}$ como sigue:

$$\mathcal{T} = \{((a, b), (a', b')) \in (A \times B) \times (A \times B) : a \mathcal{R} a' \text{ y } b \mathcal{S} b'\}.$$

Demostrar que $\mathcal{T}$ es de orden. Si $\mathcal{R}$ y $\mathcal{S}$ son de orden total, ¿lo será también $\mathcal{T}$?

10. Si $\mathcal{R}$ es un orden parcial sobre A, demostrar que $\mathcal{R}^{-1}$ también lo es. Si $\mathcal{R}$ es de orden total, ¿lo será también $\mathcal{R}^{-1}$?

5.2 Elementos notables de un conjunto ordenado

Si A es un conjunto ordenado mediante una relación $\preceq$, algunos elementos de A adquieren una naturaleza "destacada".

Definición 5.2.1 *Sea A un conjunto ordenado mediante una relación $\preceq$ y sea $B \subseteq A$. Un elemento $b \in B$ se dice que es elemento mínimo de B, respecto de la relación $\preceq$, si precede a todos los elementos de B; es decir, si $b \preceq x$, cualquiera que sea $x \in B$.*

Cuando no haya lugar a dudas sobre la relación de orden $\preceq$ considerada, basta decir elemento mínimo de B.

Definición 5.2.2 *Sea A un conjunto ordenado mediante una relación $\preceq$ y sea $B \subseteq A$. Un elemento $b \in B$ se dice que es elemento minimal de B, respecto de la relación $\preceq$, si no hay elemento alguno en B que sea estrictamente anterior a él; es decir, si no existe $x \in B$ tal que $x \preceq b$ y $x \neq b$, o equivalentemente si para cualquiera que sea $x \in B$, si $x \preceq b$, entonces $x = b$.*

Elemento mínimo y minimal, aunque guardan cierta relación, son conceptos diferentes. Veamos la diferencia en los siguientes ejemplos.

Ejemplo 5.2.3

1. Para $D = \{1, 2, 3\}$ consideremos $A = \mathcal{P}(D)$ con la relación de inclusión, y también el subconjunto de A:

$$B = \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}.$$

   Es claro que cada conjunto unitario es un elemento minimal; así, por ejemplo, no hay en B elemento alguno que esté estrictamente contenido en $\{1\}$ (es decir, no hay elemento alguno de B que sea estrictamente anterior a $\{1\}$). También es evidente que B no tiene mínimo, pues no hay en B un conjunto que esté contenido en todos los demás (es decir, no hay elemento alguno de B que sea anterior a todos los demás).

   El diagrama de Hasse correspondiente podemos verlo en la Figura 5.3.

2. Sea $A = \mathbb{R}$ con la relación de orden usual "$\leq$" y sea el subconjunto

$$B = \{x \in \mathbb{R} : \ x \geq 5\}.$$

   Desde luego 5 es elemento minimal, pues no existe $x \in B$ tal que $x \leq 5$ y $x \neq 5$. También es cierto que $5 \leq x$, cualquiera que sea $x \in B$; es decir 5 precede a todos los elementos de B, por lo que es elemento mínimo de B.

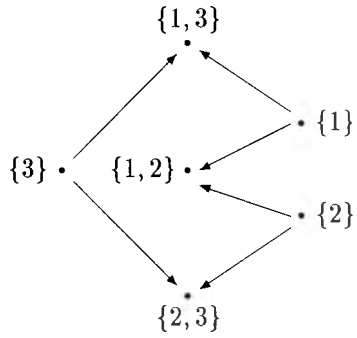


Figura 5.3: Diagrama de Hasse

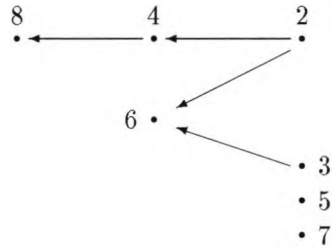


Figura 5.4: Diagrama de Hasse

3. Sea $A = \mathbb{Z}^+$ con la relación "ser divisor de" y sea $B = \{2, 3, 4, 5, 6, 7, 8\}$. Observemos que 4, 6 y 8 tienen un predecesor al menos, pero que 2, 3, 5 y 7 no tienen en B elementos (distintos de ellos mismos) que los precedan, por lo que son elementos minimales de B. Es obvio que ningún elemento de B divide a todos los demás, por lo que B no tiene elemento mínimo.

   El diagrama de Hasse correspondiente podemos verlo en la Figura 5.4.

□

Como se ha visto, un subconjunto B, de un conjunto ordenado A, puede tener varios elementos minimales; sin embargo, es fácil probar que si existe un elemento mínimo, éste es único.

Proposición 5.2.4 *Sea A un conjunto ordenado mediante una relación $\preceq$ y sea $B \subseteq A$. Si B tiene un elemento mínimo, entonces es único.*

Demostración. Supongamos que b y c son elementos mínimos de B, por lo que cualquiera que sea $x \in B$ se tiene que $b \preceq x$ y $c \preceq x$. En particular para $x = c$,

en el primer caso, y $x = b$, en el segundo, se tiene que $b \preceq c$ y $c \preceq b$, de donde $b = c$.

■

Ya que si existe elemento mínimo, es único, se puede hablar con propiedad **del** elemento mínimo de B, y lo denotaremos por $\min(B)$. Como éste precede a todos los demás, también se le denomina *el primer elemento de* B. Pero aún más, si B tiene elemento mínimo b, entonces existe un elemento minimal y este es precisamente b.

Proposición 5.2.5 *Sea A un conjunto ordenado mediante una relación $\preceq$ y sea $B \subseteq A$. Si $b \in B$ es elemento mínimo de B, entonces también b es un elemento minimal de B y además es el único elemento minimal de B.*

Demostración. Sea $b \in B$ el elemento mínimo de B y consideremos $x \in B$ tal que $x \preceq b$. Como b es el elemento mínimo de B se tiene que $b \preceq x$. En virtud de la propiedad antisimétrica del orden se sigue que $x = b$. Concluimos que b es minimal y obviamente es único.

■

Hay que advertir que si bien cuando B tiene mínimo, entonces tiene un único elemento minimal, no es cierto que si B tiene un único elemento minimal, entonces podamos concluir que dicho elemento sea el mínimo de B, pudiendo ocurrir que éste no exista.

Ejemplo 5.2.6 Consideremos en el conjunto $\mathbb{N}$ de los números naturales la relación de orden:

$$x \preceq y \quad \text{si y sólo si} \quad (x \geq y \text{ e } y \neq 0) \text{ o } (x = 0 \text{ e } y = 0).$$

Veamos que 0 es el único elemento minimal y que sin embargo $\mathbb{N}$, con este orden, no tiene mínimo.

Observemos, en primer lugar, que si x e y son no nulos entonces son comparables, toda vez que siempre es posible decir si $x \preceq y$ ($x \geq y$) o $y \preceq x$ ($y \geq x$).

Si x o y, pero no ambos, es cero, entonces no son comparables. En efecto, si $y \neq 0$ entonces $0 \not\preceq y$ pues no puede ser que $0 \geq y \neq 0$ e $y \not\preceq 0$, por la definición de la relación; y, evidentemente, estamos en la misma situación si $x \neq 0$ e $y = 0$. Puesto que $0 \preceq 0$, se sigue, de lo anterior, que 0 sólo está relacionado consigo mismo y, por tanto, no hay elemento alguno, distinto de 0, anterior a 0, por lo que 0 es elemento minimal.

Además no hay otros elementos minimales, pues cualquiera que sea el número natural considerado $x \neq 0$, siempre hay infinitos naturales anteriores a él, pues $x + k$ verifica que $x + k \preceq x$ ya que $x + k \geq x$, con $k \in \mathbb{N}$.

Sin embargo, aún siendo 0 el único elemento minimal, no existe mínimo. En efecto, 0 no puede ser mínimo porque no es anterior a los demás, de hecho no está relacionado con otros naturales; y, por otra parte, cualquiera que sea $x \in \mathbb{N}$, $x \neq 0$, siempre hay infinitos que lo preceden, por lo que ningún x puede ser el mínimo. □

No obstante lo dicho anteriormente, en determinada circunstancia sí se puede asegurar que un único elemento minimal garantiza la existencia de mínimo.

Proposición 5.2.7 *Sea A un conjunto totalmente ordenado mediante la relación $\preceq$, y sea $B \subseteq A$. Si $b \in B$ es minimal, entonces b es el elemento mínimo de B.*

Demostración. Puesto que $\preceq$ es de orden total, cualquiera que sea $x \in B$ se ha de verificar que $x \preceq b$ o $b \preceq x$. Ahora bien, si $x \neq b$, no puede ser que $x \preceq b$, ya que b es minimal, lo que significa que no hay elementos de B distintos de él que le precedan. Por tanto, se sigue que $b \preceq x$, cualquiera que sea $x \in B$ y así que b es el elemento mínimo de B.

■

Conceptos análogos al de elementos minimales y mínimo de un subconjunto, de un conjunto ordenado, son los de elementos maximales y máximo.

Definición 5.2.8 *Sea A un conjunto ordenado mediante una relación $\preceq$ y sea $B \subseteq A$. Un elemento $b \in B$ se dice que es elemento máximo de B, respecto de la relación $\preceq$, si es posterior a todos los elementos de B; es decir, si $x \preceq b$, cualquiera que sea $x \in B$.*

Definición 5.2.9 *Sea A un conjunto ordenado mediante una relación $\preceq$ y sea $B \subseteq A$. Un elemento $b \in B$ se dice que es elemento maximal de B, respecto de la relación $\preceq$, si no hay elemento alguno en B que sea estrictamente posterior a él; es decir, si no existe $x \in B$ tal que $b \preceq x$ y $x \neq b$, o equivalentemente si para cualquiera que sea $x \in B$, si $b \preceq x$, entonces $x = b$.*

Ejemplo 5.2.10

1. Sea $D = \{1, 2, 3\}$ y consideremos en $A = \mathcal{P}(D)$ la relación de inclusión. Para $B = \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\} \subseteq A$ es claro que cada conjunto binario es un elemento maximal; así, por ejemplo, no hay en B elemento alguno (subconjunto de D) que contenga estrictamente a $\{1, 2\}$. También es evidente que B no tiene máximo, pues no hay en B un conjunto que contenga a todos los demás (es decir, no hay elemento alguno de B que sea posterior a todos los demás).

   El correspondiente diagrama de Hasse podemos verlo en la Figura 5.3.

2. Sea $A = \mathbb{R}$ con la relación de orden usual "$\leq$" y sea el subconjunto

$$B = \{x \in \mathbb{R} : \ x \geq 5\}.$$

Cualquiera que sea el elemento $x \in B$ considerado, existen infinitos elementos posteriores a él, por lo que B no tiene elemento maximal. Del mismo modo es claro que no hay elemento alguno de B que sea posterior a todos los demás, por lo que B no tiene máximo.

3. Sea $A = \mathbb{Z}^+$ con la relación "ser divisor de" y sea $B = \{2, 3, 4, 5, 6, 7, 8\}$. Vemos que 5, 6, 7 y 8 no tienen elementos estrictamente posteriores, por lo que se tratan de elementos maximales de B. Observe el lector, comparando este ejemplo con el ejemplo 5.2.3, que un elemento puede ser maximal y minimal de un conjunto, este es el caso del 5 y del 7 aquí. Es también claro que B no tiene elemento máximo, pues no hay elemento alguno de B que sea divisible por todos los demás.

El diagrama de Hasse en este caso podemos verlo en la Figura 5.4.

□

El lector comprenderá que pueden trasladarse aquí todos los comentarios y resultados relativos a elementos minimales y mínimos, con sólo considerar maximales y máximos; por lo que no insistiremos en ello. Se le deja las demostraciones de las siguientes proposiciones como ejercicios de interés.

Proposición 5.2.11 *Sea A un conjunto ordenado mediante una relación $\preceq$ y sea $B \subseteq A$, entonces se verifica que: 1) Si B tiene un elemento máximo, entonces es único. 2) Si $b \in B$ es el elemento máximo de B, entonces también b es un elemento maximal de B y además es el único elemento maximal de B.*

Ya que el elemento máximo es único y es posterior a todos los demás, también se le denomina *el último elemento de B* y lo denotaremos por $\max(B)$.

Proposición 5.2.12 *Sea A un conjunto totalmente ordenado mediante una relación $\preceq$, y sea $B \subseteq A$. Si $b \in B$ es maximal entonces se verifica que es el elemento máximo de B.*

Naturalmente no todo subconjunto de un conjunto ordenado tiene primero o último elemento. Puede tener uno y no otro, puede tener ambos o no tener ninguno de ellos. Veamos algunos nuevos ejemplos.

Ejemplo 5.2.13

1. $\mathbb{N}$ con la relación de orden usual, tiene primer elemento, pero no tiene último elemento. Por otra parte, cualquier subconjunto finito de números naturales tiene tanto primero como último elemento.

2. Consideremos $\mathbb{Q}$ con el orden usual y sea:

   (a) $B = \{x \in \mathbb{Q} : 1 < x < 2\}$. B, es un conjunto totalmente ordenado, pero no tiene ni primer ni último elemento, ¿por qué?

   (b) $B = \{x \in \mathbb{Q} : x < 0 \text{ y } 1 \leq x^2 \leq 4\}$, tiene mínimo que es -2 y máximo que es -1.

   (c) $B = \{x \in \mathbb{Q} : x < 0 \text{ y } 0 \leq x^2 \leq 4\}$, tiene mínimo que es -2, pero no tiene máximo.

   (d) $B = \{x \in \mathbb{Q} : x > 0 \text{ y } 2 \leq x^2 \leq 3\}$. Este conjunto no tiene ni máximo, ni mínimo. Sin embargo, si en lugar de contemplar B como subconjunto de $\mathbb{Q}$, lo consideramos como subconjunto de $\mathbb{R}$, con el orden usual en $\mathbb{R}$, entonces tiene máximo y mínimo, que son, respectivamente, $\sqrt{3}$ y $\sqrt{2}$.

□

Cuando un conjunto carece de mínimo o máximo resulta relevante el concepto de cota.

Definición 5.2.14 *Sea A un conjunto ordenado, mediante $\preceq$, y $B \subseteq A$. Decimos que $a \in A$ es una cota inferior de B en A, con la relación $\preceq$, si a es anterior a todos los elementos de B; es decir, si $a \preceq x$, cualquiera que sea $x \in B$.*

Definición 5.2.15 *Sea A un conjunto ordenado, mediante $\preceq$, y $B \subseteq A$. Decimos que $a \in A$ es una cota superior de B en A, con la relación $\preceq$, si a es posterior a todos los elementos de B; es decir, si para cada $x \in B$ se tiene que $x \preceq a$.*

Usualmente diremos simplemente que a es una cota inferior de B (cota superior de B) con la relación de orden $\preceq$ o, si no hay lugar a confusión respecto del orden, simplemente que a es una cota inferior de B (es una cota superior de B).

Si un conjunto posee una cota inferior se dice que *está acotado inferiormente*. Análogamente, si posee una cota superior se dice que *está acotado superiormente*. Cuando un conjunto está acotado superior e inferiormente, se dice simplemente que *está acotado*.

Hemos de observar que para que a sea una cota inferior o superior de B no necesita ser elemento de B. Esta es una diferencia sustancial entre cota inferior (cota superior) y elemento mínimo (máximo). En caso de existir, el mínimo de B (máximo de B) es la única cota inferior (superior) que pertenece a B.

Ejemplo 5.2.16 Sea $B = \{x \in \mathbb{Q} : 1 < x < 2\}$. En la segunda parte del ejemplo 5.2.13 vimos que B no tiene ni mínimo ni máximo, porque $1 \notin B$ y

$2 \notin B$. Ahora bien, 1 es una cota inferior para B, de hecho cualquier número racional menor que 1 es una cota inferior para B. Del mismo modo, 2 es una cota superior para B, como lo es cualquier número racional que sea mayor que 2.

Por otra parte, observemos también que si un número es mayor que 1 y menor que 2, entonces no es ni cota inferior ni superior, por lo que

$$\{x \in \mathbb{Q} : \ x \leq 1\}$$

es el conjunto de las cotas inferiores de B y

$$\{x \in \mathbb{Q} : \ x \geq 2\}$$

es el conjunto de las cotas superiores de B. En el primer caso, 1 es la mayor de las cotas inferiores y, en el segundo, 2 es la menor de las cotas superiores. □

Definición 5.2.17 *Sea A un conjunto ordenado mediante $\preceq$, y $B \subseteq A$ que está acotado inferiormente. Decimos que $i \in A$ es el ínfimo de B en A con el orden $\preceq$ (o simplemente el ínfimo de B, cuando no hay lugar a dudas) si se verifican las siguientes dos condiciones:*

1. *i es una cota inferior de B en A, con el orden $\preceq$.*
2. *Si x es una cota inferior de B, en A con el orden $\preceq$, entonces $x \preceq i$.*

Es decir, el ínfimo es "la mayor" de las cotas inferiores. Además tiene sentido hablar **del** ínfimo pues, si existe, es único. En efecto, si $x \in A$ e $y \in A$ son ínfimos de B en A, con el orden considerado, entonces ambos serán cotas inferiores de B, luego, aplicando la segunda condición de la definición a x e y, resulta que $y \preceq x$ y que $x \preceq y$, de donde $x = y$.

Al ínfimo de B, que es único, lo denotaremos por $i = \inf(B)$.

Análogamente podemos hablar de la "menor" de las cotas superiores de un conjunto acotado superiormente.

Definición 5.2.18 *Sea A un conjunto ordenado mediante $\preceq$, y $B \subseteq A$ que está acotado superiormente. Decimos que $s \in A$ es el supremo de B en A con el orden $\preceq$ (o simplemente el supremo de B, cuando no hay lugar a dudas) si se verifican las siguientes dos condiciones:*

1. *s es una cota superior de B en A, con el orden $\preceq$.*
2. *Si x es una cota superior de B, en A con el orden $\preceq$, entonces $s \preceq x$.*

Es decir, el supremo es "la menor" de las cotas superiores. Además tiene sentido hablar **del** supremo pues, si existe, es único, como puede el lector probar siguiendo un razonamiento análogo al que se efectuó para el ínfimo.

Al supremo de B, que es único, lo denotaremos por $s = \sup(B)$.

Ejemplo 5.2.19

1. Como en 2.b del ejemplo 5.2.13, consideremos $\mathbb{Q}$ con la relación de orden usual y $B = \{x \in \mathbb{Q} : x < 0 \text{ y } 1 \leq x^2 \leq 4\}$, que está acotado tanto inferiormente como superiormente. El ínfimo es -2, que como sabemos es también el mínimo, y el supremo y también máximo es -1.

2. Como en 2.c del ejemplo 5.2.13, sean $B = \{x \in \mathbb{Q} : x < 0 \text{ y } 0 \leq x^2 \leq 4\}$ y $\mathbb{Q}$ con el orden usual. B está acotado. Su ínfimo, que es a la vez el mínimo, es -2. El supremo es 0, pero no tiene máximo.

□

Seguidamente vamos a ver una caracterización del ínfimo de un subconjunto, de un conjunto totalmente ordenado.

Proposición 5.2.20 *Sea A un conjunto totalmente ordenado, mediante la relación $\preceq$ y sea $B \subseteq A$. Entonces $i \in A$ es el ínfimo de B si y sólo si se verifica que:*

1. *i es cota inferior de B en A, respecto de la relación $\preceq$.*

2. *Cualquiera que sea $x \in A$, si $i \prec x$, entonces $i \preceq y \prec x$, para algún $y \in B$.*

Demostración. Veamos la condición necesaria. Si $i = \inf(B)$, se tiene que i es cota inferior de B.

Supongamos que no existe $y \in B$ verificando que $i \preceq y \prec x$. Ello significa que cualquiera que sea $z \in B$, entonces $i \not\preceq z$ o $z \not\prec x$.

Supongamos que $i \not\preceq z$. Como A está totalmente ordenado, tenemos que $i \preceq z$ o $z \preceq i$, pero como $i \not\preceq z$, será $z \preceq i$, lo que es absurdo pues i es el ínfimo.

Si fuera $z \not\prec x$. Al ser A totalmente ordenado, entonces $z \preceq x$ o $x \preceq z$, luego $x \preceq z$. Resultando que x es cota inferior de B verificando $i \prec x$, lo que contradice que i es el ínfimo de B.

Recíprocamente, sea i una cota inferior de B tal que si $i \prec x$, con $x \in A$, entonces existe $y \in B$ verificando $i \preceq y \prec x$.

Supongamos que i no es el ínfimo de B, entonces existirá $i' \in A$ cota inferior de B tal que no es anterior a i; es decir, $i' \not\preceq i$. Como A está totalmente ordenado, entonces será $i \prec i'$ y, en virtud de la segunda condición de la hipótesis, se tendrá que existe $y \in B$ verificando que $i \preceq y \prec i'$, contradiciendo que i' es cota inferior de B.

■

Podemos obtener un resultado análogo para el supremo de un subconjunto, de un conjunto totalmente ordenado, cuya demostración es en todo similar a la precedente.

Proposición 5.2.21 *Sea A un conjunto totalmente ordenado, mediante la relación $\preceq$ y sea $B \subseteq A$. Entonces $s \in A$ es el supremo de B si y sólo si se verifica que:*

1. *s es cota superior de B en A, respecto de la relación $\preceq$.*
2. *Cualquiera que sea $x \in A$, si $x \prec s$, entonces $x \prec y \preceq s$, para algún $y \in B$.*

En los resultados anteriores es esencial exigir que A esté totalmente ordenado, como ponemos de manifiesto seguidamente.

Ejemplo 5.2.22 Sean cuatro conjuntos M, N, P, T distintos entre sí. Sean el conjunto

$$\mathcal{A} = \{M, N, P, T\}$$

y la relación de orden en $\mathcal{A}$ dada por el subconjunto de $\mathcal{A} \times \mathcal{A}$:

$$\{(M,M),(N,N),(P,P),(T,T),(M,T),(N,T),(P,T)\},$$

que no es un orden total. Si llamamos $\mathcal{B} = \{M, N\}$, entonces se verifica que $T = \sup(\mathcal{B})$, $P \in \mathcal{A}$ y $P \prec T$ y sin embargo no existe $Y \in \mathcal{B}$ tal que

$$P \prec Y \preceq T.$$

□

El ejemplo anterior pone de manifiesto que las caracterizaciones realizadas para el ínfimo y el supremo no son válidas, en general, en conjuntos que no son totalmente ordenados.

Ejercicios

1. Sean $A = \{1,2,3,4,5\}$ y $B = \{\emptyset, \{3\}, \{2,3,4\}, \{1,2,3,4\}, A\}$.
   (a) Ordenar B por inclusión, ¿es de orden total?
   (b) Determinar cotas inferiores y superiores, elementos minimales, maximales, ínfimo y supremo de B, en el que caso de que existan.

2. Sea $A = \{2,3,4,6,12,18,36\} \subseteq \mathbb{N}$ y la relación: $x \mathcal{R} y$ si y sólo si $x|y$. Hallar los elementos primero y último de A, los elementos maximales y minimales de A y las cotas superiores e inferiores del subconjunto $B = \{2,4,6,12\}$.

3. Sea $\mathbb{R}$ con el orden usual $\leq$ y los conjuntos $A = \{x \in \mathbb{R} : 4 < x < 9\}$, $B = \{x \in \mathbb{R} : 4 \leq x < 9\}$ y $C = \{x \in \mathbb{R}; 4 \leq x \leq 9\}$. Determinar:
   (a) Cotas superiores e inferiores de A, B y C.
   (b) Supremos e ínfimos de A, B y C.
   (c) Máximos y mínimos, si existen, de A, B y C.

4. Sea $\mathbb{Q}^+$ el conjunto de los números racionales positivos con la relación de orden usual $\leq$. Sea $A = \{x \in \mathbb{Q}^+ : 9 < x^2 < 15\}$. Determinar cotas superiores e inferiores de A, ínfimo, supremo, mínimo y máximo de A, si existen.

5. Sea $A = \{1, 2, 3, 4, 5, 6\}$ y la relación de orden dada por:

$$\begin{aligned}\mathcal{R} = \{&(1,1),(2,2),(3,3),(4,4),(5,5),(6,6),(6,5),(6,1),\\ &(5,1),(1,2),(6,4),(4,1),(4,2),(3,2),(5,2),(6,2)\}.\end{aligned}$$

   (a) Determinar las cotas superiores e inferiores de $B = \{1, 4, 5\}$.
   (b) Determinar los elementos minimales y maximales de A.

6. Consideremos en el conjunto $\mathbb{N}$ de los números naturales la relación:

$$x \preceq y \quad \text{si y sólo si} \quad (x \leq y \text{ y } x \neq 0) \text{ o } (x = 0 \text{ e } y = 0).$$

   Probar que se trata de un orden parcial en $\mathbb{N}$, que 0 es el único elemento maximal y que no existe elemento máximo.

7. Demostrar que un conjunto ordenado que posee dos elementos maximales distintos no posee máximo.

8. Demostrar que en todo conjunto finito en el que se ha definido una relación de orden, hay al menos un elemento maximal.

9. Sean $\mathbb{N}$ con la relación de "ser divisor de", $B = \{3, 4, 6, 12\}$ y finalmente $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Determinar cotas superiores e inferiores, elementos minimales y maximales de A y B.

10. Supongamos que $\mathcal{R}$ es un orden parcial sobre A y que $B \subseteq A$ y $b \in B$.
    (a) Demostrar que b es el elemento máximo de B, respecto de la relación $\mathcal{R}$, si y sólo si b es el elemento mínimo de B, respecto de la relación $\mathcal{R}^{-1}$.
    (b) Demostrar que b es un elemento maximal de B, respecto de la relación $\mathcal{R}$, si y sólo si b es un elemento minimal de B, respecto de la relación $\mathcal{R}^{-1}$.

11. Sea $\mathcal{I}$ el conjunto formado por los intervalos de $\mathbb{R}$ cerrados y de longitud finita (es decir, del tipo $[a, b]$ con $a \leq b$). Se considera $\mathcal{I}$ ordenado por la inclusión usual de conjuntos.

(a) Indicar si existen en $\mathcal{I}$: máximo, mínimo, maximales y minimales.

(b) Calcular el supremo y el ínfimo para los siguientes subconjuntos de $\mathcal{P}$: $\{[0,1],[2,3]\}$ y $\{[1,3],[-1,2]\}$.

(c) ¿Existen siempre el supremo y el ínfimo de $\{[a,b],[c,d]\}$? En caso afirmativo demostrarlo, y en caso negativo indicar de qué dependerá.

12. Sea E un conjunto ordenado mediante una relación que denotaremos por $\leq$. *Una parte X de E se dice* **libre** *si no es vacía y si dos elementos distintos cualesquiera de X no son comparables* . Sea L el conjunto de las partes libres de E. Se define en L la relación $\mathcal{R}$ dada por $X \mathcal{R} Y$ *si y sólo si para todo $x \in X$ existe un $y \in Y$ tal que $x \leq y$.* Demostrar que:

(a) $\mathcal{R}$ es una relación de orden en L.

(b) Si $X \subseteq Y$ y $X, Y \in L$, entonces $X \mathcal{R} Y$.

(c) L está totalmente ordenado mediante $\mathcal{R}$ si y sólo si E está totalmente ordenado mediante $\leq$.

13. En $\mathbb{R}^2$ se define la siguiente relación: $(a,b) \mathcal{R} (c,d)$ si y sólo si $a \leq c$ y $b \leq d$.

(a) Demostrar que se trata de una relación de orden. ¿Es el orden total?

(b) Dado $A = \{(a,b) \in \mathbb{R}^2 : (a,b) \mathcal{R} (1,1)\}$, representarlo gráficamente.

(c) Determinar las cotas, supremo, ínfimo, y los elementos minimales y maximales si los hubiera, de los siguientes conjuntos:

i. $B = \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$.

ii. $C = \{(x,y) \in \mathbb{R}^2 : |x| = 1 \text{ o } |y| = 1\}$.

iii. $D = \{(-1,1), (2,3), (1,7)\}$.

14. Sea X un conjunto totalmente ordenado mediante la relación $\mathcal{R}$. Para $r \in X$ sea $S_r = \{x \in X : x \mathcal{R} r\}$. Demostrar que si $r \in A$ es tal que $S_r \cap A \neq \emptyset$, entonces A tiene mínimo si y sólo si $S_r \cap A$ lo tiene.

5.3 Retículos

Definición 5.3.1 *Sea A un conjunto ordenado, mediante la relación $\preceq$. Decimos que A es un retículo, respecto de dicha relación, si cualquiera que sea el subconjunto formado por dos elementos de A posee ínfimo y supremo.*

Ejemplo 5.3.2

1. Si $D = \{1,2,3\}$, entonces $A = \mathcal{P}(D)$ con la relación de inclusión es un retículo, como hemos puesto de manifiesto en el ejemplo 5.1.14.

2. En general, si tenemos un conjunto cualquiera $D \neq \emptyset$, entonces su conjunto potencia $\mathcal{P}(D)$, con la relación de inclusión, es un retículo. Cada dos subconjuntos de D tiene supremo, la unión de ambos, y tiene ínfimo, la intersección de ambos.

□

Si A es un retículo, respecto de la relación $\preceq$, y $x, y \in A$, el supremo y el ínfimo los denotaremos como sigue: $\sup(\{x, y\}) = x \veebar y$ e $\inf(\{x, y\}) = x \barwedge y$.

No todo conjunto ordenado es un retículo, respecto del orden considerado; así, el orden parcial del apartado 1 del ejemplo 5.1.12 no es un retículo, pues si bien 3 y 2 tienen supremo en A, que es su mínimo común múltiplo $6 = 2 \veebar 3$, no tiene ínfimo en A, pues éste sería el máximo común divisor que es $2 \barwedge 3 = 1 \notin A$.

No obstante, un conjunto que no está totalmente ordenado puede ser un retículo, como es el caso del ejemplo 5.1.14. Otro ejemplo es:

Ejemplo 5.3.3 $\mathbb{N}$, excluido el 0, con la relación "ser divisor de", es un conjunto ordenado que es retículo, pues cualesquiera que sean $x, y \in \mathbb{N}$ se tiene que existe $x \veebar y = \text{m.c.m.}(x, y)$, en el "peor" de los casos el producto de x e y, y también existe $x \barwedge y = \text{m.c.d.}(x, y)$, en el "peor" de los casos 1. □

El siguiente resultado nos indica cuando podemos asegurar que un conjunto ordenado es un retículo.

Proposición 5.3.4 *Si A es un conjunto totalmente ordenado con la relación $\preceq$, entonces es un retículo.*

Demostración. Cualesquiera que sean $x, y \in A$ se tiene que $x \preceq y$ o bien $y \preceq x$. En el primer caso $x \veebar y = y$ y $x \barwedge y = x$. En el segundo caso $x \veebar y = x$ y $x \barwedge y = y$.

■

Definición 5.3.5 *Decimos que un retículo A es completo si cualquier subconjunto suyo tiene supremo e ínfimo.*

Ejemplo 5.3.6 Para cualquier conjunto $D \neq \emptyset$ se tiene que $\mathcal{P}(D)$ con la relación de inclusión es un retículo completo. □

5.4 Buen orden

En el ejemplo 5.1.12 hemos visto un conjunto parcialmente ordenado que no tiene primer elemento. Podemos también considerar conjuntos ordenados que tengan primer elemento, pero que algún subconjunto suyo no lo tuviese; así, por ejemplo, $\mathbb{Z}^+$ con la relación "ser divisor de" tiene primer elemento, ya que

$1|n$, cualquiera que sea $n \in \mathbb{Z}^+$ y, sin embargo, $A = \{2, 3, 6, 9, 12, 36\}$ no tiene primer elemento. Cuando tal circunstancia no se dé estaremos ante un tipo de orden muy especial: el buen orden.

Definición 5.4.1 *Sea A un conjunto ordenado, mediante una relación $\preceq$. Si cualquiera que sea $B \subseteq A$ y $B \neq \emptyset$, B tiene un primer elemento, se dice que A es un conjunto* **bien ordenado** *o que tiene una buena ordenación mediante $\preceq$.*

Ejemplo 5.4.2

1. El conjunto de los números naturales con la relación de orden usual es un conjunto bien ordenado.
2. El conjunto de los números enteros $\mathbb{Z}$ con el orden usual no está bien ordenado.
3. $\mathbb{R}$ con el orden usual no es un conjunto bien ordenado. Por ejemplo el intervalo $(0, 1)$ es no vacío y no tiene primer elemento.
4. $B = \{\emptyset, \{1\}, \{1, 2\}, \{1, 2, 3\}\}$ con la relación de inclusión es un conjunto bien ordenado.
5. $A = \{2, 3, 6, 9, 12, 36\}$ con la relación "ser divisor de" no es un conjunto bien ordenado. Por ejemplo, $\{2, 3, 6\}$ no tiene primer elemento.

□

Un detenido examen de los ejemplos anteriores pone de manifiesto que los conjuntos que no están totalmente ordenados, tampoco están bien ordenados. Veamos que podemos elevar esta conjetura a la categoría de hecho irrefutable.

Proposición 5.4.3 *Si A es un conjunto bien ordenado, mediante una relación $\preceq$, entonces está totalmente ordenado mediante dicha relación.*

Demostración. Cualesquiera que sean $a, b \in A$, sea el conjunto $\{a, b\} \subseteq A$. Como A está bien ordenado, entonces $\{a, b\}$ tendrá un primer elemento, por lo que o bien $a \preceq b$ o bien $b \preceq a$.

■

Que el recíproco, de esta proposición, no es cierto es evidente. Basta pensar en $\mathbb{R}$, con el orden usual $\leq$, que está totalmente ordenado pero no está bien ordenado.

El buen orden "es hereditario". En efecto:

Proposición 5.4.4 *Cualquier subconjunto no vacío de un conjunto bien ordenado está bien ordenado.*

Demostración. Sea $B \subseteq A$, $B \neq \emptyset$. Cualquiera que sea el subconjunto $M \neq \emptyset$ de B, $M \subseteq B$, se tiene que $M \subseteq A$, y como A tiene un buen orden, M tiene primer elemento. Concluimos que B es un conjunto bien ordenado.

■

Ejercicios

1. En $\mathbb{R}$, ordenado por la relación de menor o igual, se considera

$$A = \{x \in \mathbb{R} : \ x = \frac{1}{n}, n \in \mathbb{N}\}.$$

   Estudiar si A tiene primero o último elemento, si está bien ordenado y si admite cotas, ínfimo o supremo.

2. Se considera el conjunto $\mathbb{Q}$ con el orden usual $\leq$. ¿Qué subconjuntos de $\mathbb{Q}$ de los siguientes están bien ordenados?

   (a) $\mathbb{Q}$.

   (b) Los enteros mayores que 9.

   (c) Los enteros pares menores que 0.

   (d) Los enteros positivos múltiplos de 5.

3. En el conjunto de las aplicaciones de $\mathbb{R}$ en $\mathbb{R}$, $\mathcal{A} = \{f : \mathbb{R} \longrightarrow \mathbb{R}\}$, se define la relación $f \preceq g$ si y sólo si $f(x) \leq g(x)$, para todo $x \in \mathbb{R}$.

   (a) Demostrar que es de orden. ¿Es orden total?, ¿es un buen orden?

   (b) Se considera $\mathcal{B} = \{\varphi_n\}_{n \in \mathbb{N}^+} \subseteq \mathcal{A}$, siendo para cada $n \in \mathbb{N}^+$,

$$\varphi_n(x) = -\frac{x}{n}.$$

   Determinar, caso de existir, máximo, mínimo, maximales, minimales, supremo e ínfimo de $\mathcal{B}$.

   Nota: Ver el concepto de aplicación en el próximo capítulo.

Capítulo 6

Aplicaciones

6.1 Concepto de aplicación

Dedekind (1831–1916) introduce en 1880, en su obra *Was sind und was sollen die Zahlen* el lenguaje conjuntista, como forma de precisar expresiones ambiguas de los textos matemáticos. Este tipo de lenguaje se impone, en el siglo XX, en todos los campos de las matemáticas, siendo hoy día utilizado universalmente por la comunidad matemática y sin el cual la comunicación científica se haría tremendamente farragosa y opaca.

En ese trabajo Dedekind aporta un concepto general de función, en el que quedan englobados las funciones numéricas, las "sustituciones" introducidas por Cauchy y las transformaciones geométricas. Para dos conjuntos arbitrarios A y B indica que una función f de A en B es una "ley" que a cada elemento $x \in A$ le hace corresponder un elemento bien determinado de B, su valor en x, que se escribe de manera general $f(x)$.

El concepto de producto cartesiano de dos conjuntos fue introducido posteriormente por Cantor. A partir de aquí se puede relacionar la noción de función con la de producto cartesiano, de tal manera que el *grafo* de la función f, de A en B, no es otro que el siguiente subconjunto del producto cartesiano $A \times B$:

$$\Gamma = \{(x, y) : \ y = f(x), \text{ para cada } x \in A\},$$

lo que obviamente es una generalización del concepto de gráfica de una función real de variable real.

El lector observará que "la expresión de f" como ley que liga los elementos de los conjuntos A y B, no es más que la definición de una relación de A a B, por lo que, a la postre, una función no es otra cosa que un tipo particular de relación entre dos conjuntos, a saber el de aquellas cuyo dominio es todo A y de forma que un mismo $x \in A$ no puede estar en dos pares ordenados distintos que pertenezcan a dicha relación.

Se podría aducir, y de hecho podría haberse hecho ya en el capítulo 4, que una cosa es la "ley" o "propiedad" que determina el conjunto Γ y otra cosa el propio conjunto Γ; pues la primera "**actúa**" (a un cierto x le asocia un cierto y), mientras que el segundo simplemente **es**. Esta posición se correspondería con una cierta tradición en la forma de expresarse matemáticamente y, en la cual, la palabra función se reserva para la "ley" que actúa y al conjunto de pares ordenados se le reserva la palabra gráfica o grafo (según los casos). Desde nuestra posición, dentro de la teoría de conjuntos, ésta es una disquisición absolutamente estéril y no volveremos a hacer referencia alguna a tal cuestión.

Es usual hablar de aplicación en lugar de función, reservando esta última expresión, habitualmente, para el caso en el cual los conjuntos A y B son numéricos. Si A y B son conjuntos de puntos, se suele hablar de *transformación geométrica* (movimientos, simetrías, etc.).

Definición 6.1.1 *Si A y B son conjuntos, una aplicación f de A en B es una relación entre A y B, tal que Dom $(f) = A$ y para cada $x \in A$ existe un único $y \in B$ verificando que $(x, y) \in f$.*

La condición de que $y \in B$ ha de ser único, para cada x, puede formularse también como sigue:

$$\text{si} \quad (x, y) \in f \quad \text{y} \quad (x, y') \in f, \quad \text{entonces} \quad y = y'.$$

Es claro que el conjunto de todas las aplicaciones de A en B es un subconjunto del conjunto potencia $\mathcal{P}(A \times B)$, que denotaremos mediante B^A.

Para indicar que f es una aplicación de A en B escribiremos $f : A \longrightarrow B$. Para cada $x \in A$ el único $y \in B$ tal que $(x, y) \in f$ se escribe como $f(x)$, se denomina *la imagen de x mediante f* o también "el valor que toma x mediante f" y se lee "f de x". A veces, para referirse a una aplicación, suele también escribirse:

$$\begin{array}{rccc} f: & A & \longrightarrow & B \\ & x & \longmapsto & f(x) = y. \end{array}$$

Si $f : A \longrightarrow B$ es una aplicación de A a B, los conjuntos A y B se llaman conjunto origen y final, respectivamente, de la aplicación.

Si $x \in A$ es tal que su imagen es $y \in B$, $y = f(x)$, entonces se dice que x es un elemento original de y, mediante la aplicación f. Si no hay posibilidad de confusión acerca de la aplicación considerada basta decir que "x es un elemento original de y". En ocasiones nos encontraremos con situaciones análogas a la hora de denominar algún elemento o conjunto de elementos que tienen "algo en común", respecto de una aplicación f; si no hay lugar a dudas, sobre la aplicación a la que nos estemos refiriendo, obviaremos seguir utilizando la coletilla "mediante la aplicación ..." o "respecto de la aplicación ...".

Naturalmente el original de $y \in B$ no tiene por qué ser único, pues distintos pares ordenados pueden tener un mismo segundo elemento. Para $y \in B$ fijo, el

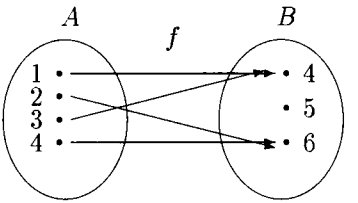


Figura 6.1: Diagrama de Venn de f

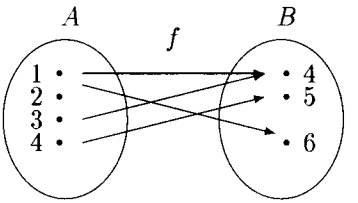


Figura 6.2: f no es aplicación

conjunto $\{x \in A : f(x) = y\}$, se denomina el *conjunto original del elemento* y. Es claro que la unión de todos los conjuntos originales es $Dom\ (f) = A$, también suele escribirse $Dom\ f$.

El conjunto de todos los elementos $y \in B$ tales que son original de algún $x \in A$ se denomina la *imagen de la aplicación* f y se denota por $Im\ (f)$, también por $Im\ f$, o por $f(A)$. Observemos que ésta no es otra que el rango de la relación f:

$$Im\ f = \{y \in B : \text{ existe } x \in A \text{ tal que } y = f(x)\}.$$

Ejemplo 6.1.2

1. Sean $A = \{1, 2, 3, 4\}$, $B = \{4, 5, 6\}$ y $f = \{(1, 4), (2, 6), (3, 4), (4, 6)\}$. f es una aplicación $f : A \longrightarrow B$.

   Podemos representar gráficamente las aplicaciones al igual que hicimos con las relaciones, en general. La figura 6.1 representa el diagrama de Venn de la aplicación anterior.

2. Sean $A = \{1, 2, 3, 4\}$, $B = \{4, 5, 6\}$ y $f = \{(1, 4), (1, 6), (3, 4), (4, 5)\}$. Ahora f no es una aplicación, toda vez que 1 tiene dos imágenes: 4 y 6. Vemos la representación en la figura 6.2.

3. Sea $f = \{(x, y) \in \mathbb{R}^2 : y = x - 3\}$, que se trata de una aplicación

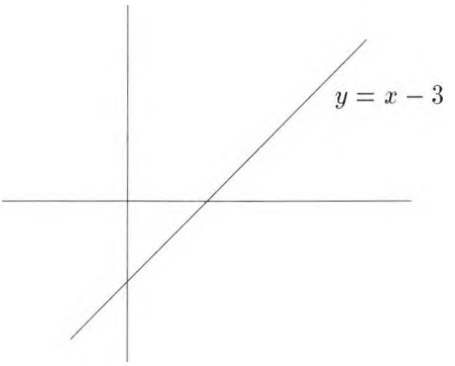


Figura 6.3: Gráfico cartesiano

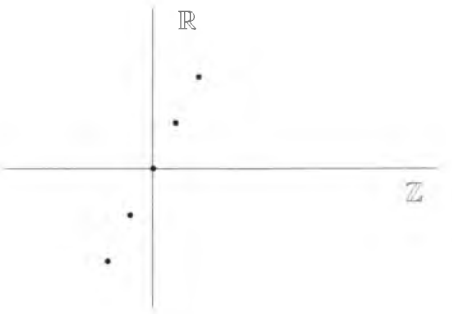


Figura 6.4: Gráfico cartesiano

$f : \mathbb{R} \longrightarrow \mathbb{R}$, ya que para cada $x \in \mathbb{R}$ existe un único valor $y \in \mathbb{R}$, tal que $y = f(x)$.

En este caso es más apropiado utilizar un gráfico cartesiano (ver figura 6.3) para representar la aplicación.

4. Sea la aplicación $f : \mathbb{Z} \longrightarrow \mathbb{R}$ dada por $f(x) = 2x$, que es "la condición" que determina de manera inequívoca los pares ordenados de la aplicación. En efecto:

$$f = \{(x, y) \in \mathbb{Z} \times \mathbb{R} : \ y = f(x)\} \ = \ \{(x, y) \in \mathbb{Z} \times \mathbb{R} : \ y = 2x\} \ .$$

Es evidente que para cada entero x existe un único valor real que es su imagen, $2x$. La representación de esta aplicación mediante un gráfico cartesiano la podemos ver en la figura 6.4.

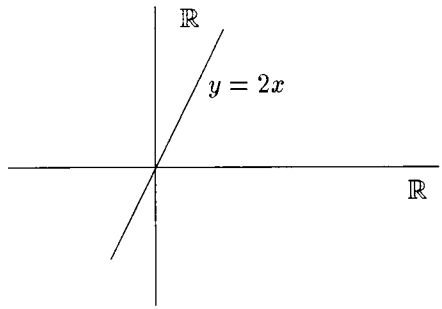


Figura 6.5: Gráfico cartesiano

5. Sea la aplicación f de $\mathbb{R}$ en $\mathbb{R}$ dada por $f(x) = 2x$. La ley o "condición" que determina a esta aplicación es la misma que la del ejemplo anterior, sin embargo, la aplicación es distinta; ahora, por ejemplo, $(\sqrt{3}, 2\sqrt{3}) \in f$, mientras que en el caso anterior no. En la figura 6.5 podemos ver la representación gráfica de esta aplicación.

□

En algunos de los ejemplos precedentes, implícitamente ha quedado constancia de que la "ley", "regla" o "condición" (ordinariamente una fórmula matemática), que nos sirve para "definir una aplicación", determina inequívocamente a ésta porque permite conocer $f(x)$ para cada $x \in A$; es decir, estamos dando por sentado que existe una y sólo una aplicación que satisface la condición propuesta. Ello requiere precisar que si dos "reglas" resultan ser dos expresiones matemáticas equivalentes, las correspondientes aplicaciones han de ser iguales.

Proposición 6.1.3 *Sean f y g dos aplicaciones de A en B, entonces $f = g$ si y sólo si $f(x) = g(x)$ para cada $x \in A$.*

Demostración. Si $f = g$ entonces los pares ordenados (x, y) pertenecientes a f y g han de ser los mismos, por lo que $f(x) = g(x)$, para cada $x \in A$.

Recíprocamente, si $(x, y) \in f$, entonces $y = f(x)$ y por hipótesis se tendrá que $y = g(x)$, por lo que $(x, y) \in g$, de donde $f \subseteq g$. Análogamente se prueba que $g \subseteq f$. Concluimos que $f = g$.

■

6.1.1 Algunas aplicaciones especiales

A continuación haremos referencia a algunas aplicaciones particulares que aparecen frecuentemente en matemáticas.

Sea $A \subseteq B$, la aplicación $f : A \longrightarrow B$ definida por $f(x) = x$ para cada $x \in A$ se denomina la *inmersión* de A en B. La inmersión de A en A es la *aplicación identidad*[1] en A.

Si consideramos $A \subseteq B$ y una aplicación $f : B \longrightarrow C$, podemos construir una aplicación de A en C, $g : A \longrightarrow C$, dada por $g(x) = f(x)$ para cada $x \in A$. Esta aplicación g recibe el nombre de *restricción de f a A* y se suele denotar por $g = f|_A$, recibiendo f el nombre de *extensión de g a B*. Observemos que $Im\ f|_A = f(A)$.

Es pertinente indicar que la inclusión de A en B no es otra cosa que la restricción, a A, de la identidad definida en B.

Si A y B son dos conjuntos no vacíos, la aplicación $f : A \times B \longrightarrow A$, definida, para cada $(x, y) \in A \times B$, por[2] $f(x, y) = x$, se denomina la *proyección de $A \times B$ sobre A*. Análogamente se puede definir la proyección de $A \times B$ sobre B.

Otra aplicación de gran interés es la denominada *función característica* de un conjunto. Si A es un subconjunto de un conjunto B, $A \subseteq B$, la aplicación $\chi_A : B \longrightarrow \{0, 1\}$ definida por

$$\chi_A(x) = \begin{cases} 1 & \text{si} \quad x \in A \\ 0 & \text{si} \quad x \in B \setminus A \end{cases}$$

se denomina la *función característica del conjunto A*.

6.2 Clases de aplicaciones

A continuación damos algunas definiciones que nos serán de particular utilidad.

Definición 6.2.1 *Una aplicación $f : A \longrightarrow B$ se dice que es inyectiva si cualesquiera que sean $x, x' \in A$ con $x \neq x'$ se sigue que $f(x) \neq f(x')$.*

Equivalentemente, podemos decir que $f : A \longrightarrow B$ es inyectiva si y sólo si cualesquiera que sean $x, x' \in A$ tales que $f(x) = f(x')$ se tiene que $x = x'$.

La representación gráfica, mediante un diagrama de Venn, sería como se indica en la figura 6.6, de forma que en cada elemento de A se tiene el origen de una flecha y en cada elemento de $f(B)$ el final, también, de una única flecha. Por esta razón también se suele denominar a las aplicaciones inyectivas como *aplicaciones uno a uno*, traducción castellana de la expresión inglesa "one–to–one" (que es como la denominan usualmente los libros anglosajones).

[1] En términos de relaciones, la identidad en A no es otra que la relación de igualdad en A.

[2] Deberíamos escribir $f((x, y)) = x$, pero no existiendo peligro de confusión abreviamos con la notación utilizada.

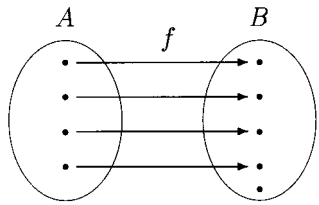


Figura 6.6: Aplicación inyectiva

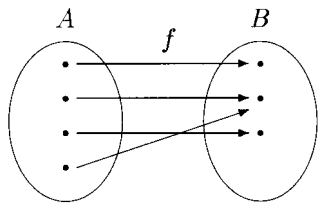


Figura 6.7: Aplicación sobreyectiva

Definición 6.2.2 *Una aplicación $f : A \longrightarrow B$ se dice que es sobreyectiva si todo elemento del conjunto final de la aplicación, B, es imagen de algún elemento del conjunto inicial A; es decir, si para cada $y \in B$ existe $x \in A$ tal que $y = f(x)$.*

De forma equivalente, podemos decir que la aplicación $f : A \longrightarrow B$ es sobreyectiva si y sólo si $Im\ f = B$.

En la representación gráfica, mediante un diagrama de Venn, no puede ocurrir que haya elementos de B al que no le corresponda el final de una flecha, tal y como se indica en la figura 6.7.

Definición 6.2.3 *Una aplicación $f : A \longrightarrow B$ se dice que es biyectiva cuando es inyectiva y sobreyectiva.*

En este caso a cada elemento de A le corresponde un único elemento de B y recíprocamente. Una representación mediante diagrama de Venn sería como se indica en la figura 6.8.

Ejemplo 6.2.4

1. $f : \mathbb{N} \longrightarrow \mathbb{N}$ tal que $f(n) = n + 1$, para cada $n \in \mathbb{N}$, es una aplicación inyectiva, pues si $n + 1 = m + 1$, entonces $n = m$. Sin embargo no es

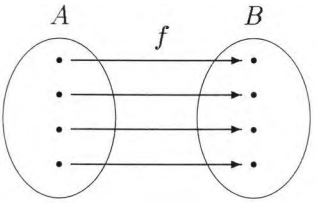


Figura 6.8: Aplicación biyectiva

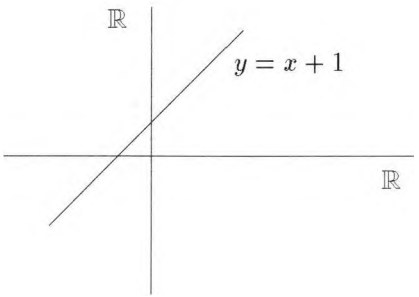


Figura 6.9: Aplicación biyectiva

sobreyectiva pues 0 no tiene original.

2. $f : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f(x) = x + 1$, para cada $x \in \mathbb{R}$, es una aplicación biyectiva. Su representación gráfica podemos verla en la figura 6.9

3. $f : \mathbb{N} \longrightarrow \mathbb{N}$ tal que $f(n) = 0$, que es la aplicación constante 0, no es inyectiva ni sobreyectiva.

4. Sea $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ definida por $f(x, y) = (x, xy - y^3)$, para cada par ordenado $(x, y) \in \mathbb{R}^2$.

   Es sobreyectiva, pues para cada $(x', y') \in \mathbb{R}^2$ existe $(x, y) \in \mathbb{R}^2$ tal que $f(x, y) = (x, xy - y^3)$, precisamente los (x, y) que sean solución del sistema:

$$\begin{cases} x' = x \\ y' = xy - y^3. \end{cases}$$

   Este sistema tiene solución para cada x e y, pues $x' = x$ e

$$y^3 - x'y + y' = 0$$

   tiene al menos una solución y real, ya que se trata de una ecuación polinómica de grado impar.

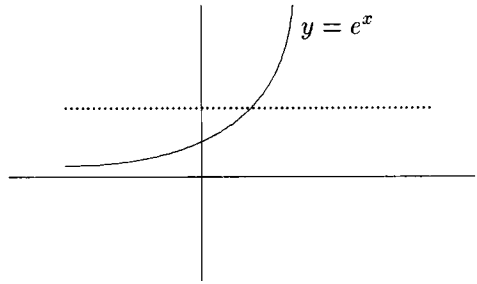


Figura 6.10: Aplicación inyectiva

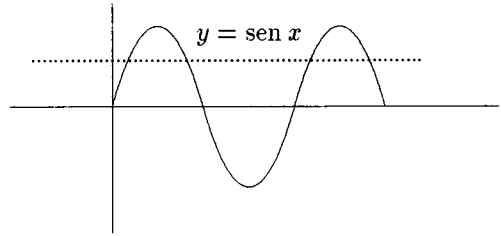


Figura 6.11: No es inyectiva ni sobreyectiva

Sin embargo no es inyectiva, toda vez que las anteriores ecuaciones polinómicas (una para cada valor de x' y de y') pueden tener más de una solución real; por ejemplo, si $(x', y') = (7, 6)$, entonces $y^3 - 7y + 6 = 0$ tiene tres raíces reales: 1, 2 y -3, por lo que

$$f(7,1) = f(7,2) = f(7,-3) = (7,6).$$

5. Sea $f : \mathbb{R} \longrightarrow \mathbb{R}$, tal que $f(x) = e^x$. Es inyectiva pues si $x \neq x'$, entonces $e^x \neq e^{x'}$ y no es sobreyectiva, ya que $Im\ f = \mathbb{R}^+$. Podemos ver su representación gráfica, en la figura 6.10, en la que también se ha representado una recta paralela al eje de abscisas.

6. $f : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f(x) = \text{sen } x$, no es inyectiva de forma obvia y tampoco es sobreyectiva, pues $Im\ f = [-1, 1]$. En la figura 6.11 podemos ver como sería la representación gráfica de esta aplicación, junto con una recta paralela al eje de abscisas.

□

Las figuras 6.9, 6.10 y 6.11 ponen de manifiesto, desde una perspectiva geométrica, que: si una aplicación es inyectiva no puede haber una recta paralela

al eje de abscisas que corte a la gráfica en más de un punto y si es sobreyectiva, cualquiera que sea la recta que se trace paralela al eje de abscisas ha de cortar a la gráfica en al menos un punto.

Ejercicios

1. Indicar si las siguientes relaciones son aplicaciones, y en su caso qué tipo de aplicación:

   (a) $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, tal que $f(x) = y$, si y es divisor de x.

   (b) Sea A el conjunto de las rectas del plano y $f : A \longrightarrow A$ tal que $f(x) = y$, donde la recta y es perpendicular a la recta x.

   (c) $f : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f(x) = \frac{x}{x^2+1}$.

   (d) $f = \{(x, y) : x^2 + y^2 = 9\}$.

   (e) $g = \{(x, y) : x = 7\}$.

   (f) $h = \{(x, y) : y = 17\}$.

   (g) $l = \{(x, y) : x - y - 7 = 0\}$.

   (h) $p = \{(x, y) : x = y^2\}$.

2. Probar que la relación, $f : A \longrightarrow B$ tal que $f(x) = x^3$, es una aplicación, indicando su tipo, cuando:

   (a) $A = B = \mathbb{R}$.

   (b) $A = B = \mathbb{C}$.

3. Sea E un conjunto no vacío y A, B subconjuntos de E, demostrar que:

   (a) $\chi_A = \chi_B$ si y sólo si $A = B$.

   (b) $\chi_{A \cup B} = \chi_A + \chi_B - \chi_{A \cap B}$.

   (c) $\chi_{A \setminus B} = \chi_A(1 - \chi_B)$.

   Donde, para $D \subseteq E$, χ_D es la función característica del subconjunto D.

4. Sean X e Y dos conjuntos, $G \subseteq X \times Y$. Sea $\Pi_1 : X \times Y \longrightarrow X$ la proyección en el primer conjunto, es decir tal que $\Pi_1((x, y)) = x$ y sea p_1 la restricción a G de Π_1. Consideremos $g = \{(x, y) : (x, y) \in G\}$, demostrar que g es una aplicación si y sólo si p_1 es biyectiva.

6.3 Composición de aplicaciones

Consideremos dos aplicaciones $f : A \longrightarrow B$ y $g : B \longrightarrow C$. Como $f(x) \in B$ para cada $x \in A$, tiene sentido considerar las imágenes de $f(x)$, mediante g, para cada $x \in A$. Si queremos asignar a cada $x \in A$ un elemento en C basta determinar $f(x)$ y a continuación la imagen de éste mediante g, $g(f(x))$. Como todo elemento de la imagen de f pertenece al dominio de g, tiene sentido la expresión $g(f(x))$, para cada $x \in A$.

Definición 6.3.1 *Dadas dos aplicaciones $f : A \longrightarrow B$ y $g : B \longrightarrow C$, llamamos composición de f y g a la aplicación $h : A \longrightarrow C$ tal que $h(x) = g(f(x))$, para cada $x \in A$, y que denotaremos por $g \circ f$.*

Debería probarse, y lo dejamos como ejercicio, que efectivamente la "aplicación" así definida es efectivamente una aplicación.

Así pues, $g \circ f(x) = g(f(x))$ para cada $x \in A$ y $g \circ f$ se lee "f compuesta con g". Observemos que la composición de f y g, $g \circ f$ y la composición de g y f, $f \circ g$, son cosas muy distintas. Para que $g \circ f$ tenga sentido, hemos visto que ha de ser $Im\ f \subseteq Dom\ g$, pero de aquí no puede deducirse que $Im\ g \subseteq Dom\ f$; es más, en general ello no sólo no será cierto sino que incluso carecerá de sentido, salvo que $A = C$ y aún en este caso, en general, $g \circ f \neq f \circ g$.

Ejemplo 6.3.2 Sean $f : \mathbb{R} \longrightarrow \mathbb{R}$ y $g : \mathbb{R} \longrightarrow \mathbb{R}$ funciones reales de variable real, tales que $f(x) = 3x$ y $g(x) = 5x + 2$. Entonces:

$$g \circ f(x) = g(f(x)) = g(3x) = 15x + 2,$$

$$f \circ g(x) = f(g(x)) = f(5x + 2) = 15x + 6.$$

□

Si bien es cierto que la composición de aplicaciones no es conmutativa, sin embargo sí es asociativa.

Proposición 6.3.3 *Sean las aplicaciones*

$$f : A \longrightarrow B, \quad g : B \longrightarrow C \quad y \quad h : C \longrightarrow D,$$

entonces se verifica que $(h \circ g) \circ f = h \circ (g \circ f)$.

Demostración. Es claro que en los dos casos estamos hablando de una aplicación de A en D. Veamos que son iguales.

Para $x \in A$ arbitrario,

$$(h \circ g) \circ f(x) = (h \circ g)(f(x)) = h(g(f(x)))$$

y, por otra parte,

$$h \circ (g \circ f)(x) = h(g \circ f)(x)) = h(g(f(x))).$$

Concluimos que las dos aplicaciones coinciden.

■

Es fácil probar, y se deja al lector que lo haga, que:

1. La composición de aplicaciones inyectivas es una aplicación inyectiva.
2. La composición de aplicaciones sobreyectivas es una aplicación sobreyectiva.
3. La composición de aplicaciones biyectivas es una aplicación biyectiva.

Ejercicios

1. Las funciones $f : \mathbb{Z} \longrightarrow \mathbb{Q}$ y $g : \mathbb{Q} \longrightarrow \mathbb{Z}$ son tales que $f(x) = \dfrac{x^2}{2} + 1$ y $g(x) = E(x)$, donde $g(x) = E(x)$ es la función *parte entera de* x, que, como es sabido, a cada número real x le asigna el mayor entero que no supera a x (si $E(x) = a$ entonces $a \leq x < a + 1$).
   (a) Definir $g \circ f$, $f \circ g$.
   (b) Determinar $(g \circ f)(-2)$, $(f \circ g)(-\dfrac{1}{2})$.
2. Se consideran las siguientes aplicaciones de $\mathbb{R}$ en $\mathbb{R}$ definidas por:
   $$f(x) = \frac{3x - 5}{x^2 + 1}, \quad g(x) = 7x^2 - 2x + 5.$$
   Determinar $f \circ g$ y $g \circ f$.
3. Demostrar que si $g \circ f$ es sobreyectiva, entonces también lo es g.
4. Las aplicaciones $f : A \longrightarrow B$, $g : B \longrightarrow C$, y $h : C \longrightarrow D$ son tales que $g \circ f$ y $h \circ g$ son biyectivas. Demostrar que f, g y h son biyectivas.
5. Las funciones $f : A \longrightarrow B$, $g : B \longrightarrow C$, y $h : C \longrightarrow A$ son tales que $h \circ g \circ f$ y $f \circ h \circ g$ son sobreyectivas, mientras que $g \circ f \circ h$ es inyectiva. Demostrar que f, g y h son biyectivas.

6.4 Familias de conjuntos

En ocasiones la imagen de una aplicación es considerada más importante que la aplicación misma; éste es el caso de las sucesiones de números reales, que son aplicaciones $f : \mathbb{N} \longrightarrow \mathbb{R}$ tales que para cada $n \in \mathbb{N}$ se obtiene un valor $f(n)$. De la enseñanza media sabemos que no es usual hablar de la sucesión $f : \mathbb{N} \longrightarrow \mathbb{R}$ tal que $f(n) = \frac{n+1}{2n-3}$, para cada $n \in \mathbb{N}$, sino de la sucesión cuyo término general es $a_n = \frac{n+1}{2n-3}$, confundiendo intencionadamente la aplicación con su imagen.

Ahora nos planteamos una situación similar, en relación a conjuntos.

Una familia es una aplicación f entre dos conjuntos $\mathcal{I}$ y $\mathcal{F}$, $f : \mathcal{I} \longrightarrow \mathcal{F}$, llamados, respectivamente, conjunto de índices y conjunto indexado.

Si $i \in \mathcal{I}$, se dice que i es un índice y en lugar de escribir $f(i)$ denotaremos a la imagen de i por f_i, que lo denominaremos *término* de la familia.

Ya que la importancia se la estamos dando a la imagen de la aplicación, en vez de hablar de la familia $f : \mathcal{I} \longrightarrow \mathcal{F}$, diremos la familia $\{f_i\}_{i\in\mathcal{I}}$ de elementos de $\mathcal{F}$.

Naturalmente el conjunto de índices puede ser cualquiera, el más usual es $\mathbb{N}$, pero también aparecerá $\mathbb{R}$ y otros conjuntos $\mathcal{I}$ de índices arbitrarios.

Un caso de particular interés es el de una familia de subconjuntos de un conjunto dado X. Si decimos que $\{A_i\}_{i\in\mathcal{I}}$ es una familia de subconjuntos de X, estamos diciendo que tenemos una aplicación $A : \mathcal{I} \longrightarrow \mathcal{P}(X)$, tal que $A(i) = A_i \subseteq X$.

Si $\{A_i\}_{i\in\mathcal{I}}$ es una familia de subconjuntos de X, llamamos unión de la familia a la unión de la imagen de la familia; es decir, si denotamos por $\mathcal{C}$ a la imagen (colección de los subconjuntos A_i: $\mathcal{C} = \{A_i\}_{i\in\mathcal{I}}$), la unión de la familia $\bigcup\mathcal{C}$, la denotaremos por $\bigcup_{i\in\mathcal{I}} A_i$. Es obvio que $x \in \bigcup_{i\in\mathcal{I}} A_i$ si y sólo si $x \in A_i$ para algún A_i, lo que también suele decirse así:

$$x \in \bigcup_{i\in\mathcal{I}} A_i \quad \text{si y sólo si} \quad x \in A_i \quad \text{para algún } i \in \mathcal{I}.$$

Si el conjunto de índices es $\mathcal{I} = \{1, \ldots, n\} \subseteq \mathbb{N}$, entonces escribiremos $\bigcup_{i=1}^{n} A_i$ para hablar de la unión de la familia.

Análogamente para la intersección tenemos:

$$x \in \bigcap_{i\in\mathcal{I}} A_i \quad \text{si y sólo si} \quad x \in A_i \quad \text{para cada } i \in \mathcal{I}.$$

Cuando el conjunto de índices es $\mathcal{I} = \{1, 2, \ldots, n\}$, escribiremos $\bigcap_{i=1}^{n} A_i$ para indicar la intersección de la familia.

Es claro que no se pierde generalidad si en lugar de hablar de una colección arbitraria $\mathcal{C}$ de conjuntos, consideramos una familia de conjuntos, pues toda

colección $\mathcal{C}$ de conjuntos es la imagen de alguna familia. En efecto, si tomamos a la propia $\mathcal{C}$ como conjunto de índices y como conjunto indexado, la aplicación identidad:

$$\begin{array}{rccc} i: & \mathcal{C} & \longrightarrow & \mathcal{C} \\ & X & \longmapsto & i(X) = X_X \end{array}$$

es una familia de conjuntos. Ha de advertir el lector que la anterior i representa a la aplicación identidad, aquella que transforma un objeto en sí mismo, o si se prefiere $i = \{(X, X) : X \in \mathcal{C}\}$, que no ha de confundirse en este caso (aunque usemos la misma letra) con un elemento de un conjunto de índices.

Sabemos, con claridad, qué significa una colección $\mathcal{C}$ no vacía de conjuntos. Precisemos que por una familia no vacía de conjuntos entendemos una familia cuyo dominio $\mathcal{I}$ es no vacío.

Todo lo dicho en su momento, para la unión y la intersección de colecciones de conjuntos, se puede trasladar aquí para hablar de la unión e intersección de una familia de conjuntos. En particular son válidas las propiedades asociativas y conmutativas de la unión y la intersección, las leyes de De Morgan y la generalización de las propiedades distributivas:

$$B \cap \left(\bigcup_{i \in \mathcal{I}} A_i \right) = \bigcup_{i \in \mathcal{I}} (B \cap A_i),$$

$$B \cup \left(\bigcap_{i \in \mathcal{I}} A_i \right) = \bigcap_{i \in \mathcal{I}} (B \cup A_i),$$

siendo $\{A_i\}_{i \in \mathcal{I}}$ una familia de subconjuntos de X y $B \subseteq X$.

El lector podrá hacer aquí la pertinente traslación de lo estudiado en el capítulo 3.

6.5 Inversa de una aplicación

Dada una aplicación $f : A \longrightarrow B$, sabemos qué es una relación de A en B. Tiene sentido considerar la relación inversa de B en A (ver definición 4.3.6), que denotaremos por f^{-1}, pero ahora no podemos asegurar que ésta sea una aplicación, pues si existen varios elementos de A con la misma imagen, al considerar f^{-1} nos encontraríamos con que hay elementos de B que tienen más de una imagen mediante f^{-1}, por lo que ésta no puede ser una aplicación; también puede ocurrir que haya elementos de B que no tengan original mediante f, en cuyo caso mediante f^{-1} habría elementos de B sin imagen, resultando de nuevo que f^{-1} no sería una aplicación.

Desde luego, si $f : A \longrightarrow B$ es tal que su inversa es una aplicación, entonces $f(a) = b$ si y sólo si $f^{-1}(b) = a$. En efecto, si $f(a) = b$, entonces $(a, b) \in f$, por lo que $(b, a) \in f^{-1}$, luego $a \in \{x : x = f^{-1}(b)\}$ y como f^{-1} es aplicación

la imagen de b es única, por lo que $f^{-1}(b) = a$. Recíprocamente si $f^{-1}(b) = a$ tendremos que $(a, b) \in f$ y así $b \in \{y : y = f(a)\}$, como f es aplicación se tiene que $f(a) = b$.

Ejemplo 6.5.1 Si $A = \{-2, -1, 0, 1, 2\}$, $B = \{0, 1, 2, 3, 4\}$ y $f : A \longrightarrow B$ viene dada por $f(x) = x^2$, entonces $f = \{(-2, 4), (-1, 1), (0, 0), (1, 1), (2, 4)\}$ y f es claramente una aplicación. Pero $f^{-1} = \{(4, -2), (1, -1), (0, 0), (1, 1), (4, 2)\}$, por lo que a 4 y a 1 le corresponden dos imágenes y además 2 y 3 carecen de imagen. Consecuentemente la relación f^{-1} no es una aplicación. □

De lo dicho hasta ahora se intuye que si la aplicación f es inyectiva y sobreyectiva (es decir, biyectiva) es imposible que se presenten los problemas apuntados, resultando que efectivamente f^{-1} es una aplicación.

Proposición 6.5.2 *Sea una aplicación $f : A \longrightarrow B$ tal que su inversa es una aplicación $f^{-1} : B \longrightarrow A$, entonces se verifica que $f^{-1} \circ f = i_A$ y $f \circ f^{-1} = i_B$.*

Demostración. Cualquiera que sea $a \in A$, sea $f(a) = b$ y por tanto $f^{-1}(b) = a$. Así

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a = i_A(a),$$

de donde $f^{-1} \circ f = i_A$.

Análogamente, cualquiera que sea $b \in B$, sea $f^{-1}(b) = a \in A$, de donde $f(a) = b$.

Como

$$(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b = i_B(b),$$

se tiene que $f \circ f^{-1} = i_B$.

■

Proposición 6.5.3 *Sea $f : A \longrightarrow B$ una aplicación entre A y B, entonces las siguientes afirmaciones son equivalentes:*

1. *f es biyectiva.*
2. *La inversa de f es una aplicación, $f^{-1} : B \longrightarrow A$.*

Demostración.

1) $\Rightarrow$ 2) Si b es un elemento cualquiera de B, como f es sobreyectiva se tiene que existe $a \in A$ tal que $f(a) = b$, de donde $(a, b) \in f$, por lo que $(b, a) \in f^{-1}$ y, por tanto, $a \in \{x : x = f^{-1}(b)\}$. Además si $a' \in \{x : x = f^{-1}(b)\}$, entonces $f(a') = b = f(a)$ y por ser f inyectiva se sigue que $a = a'$. Concluimos que para todo $b \in B$ existe un único $a \in A$ tal que $a = f^{-1}(b)$.

2) $\Rightarrow$ 1) Veamos, en primer lugar, que f es inyectiva.

Sean $a, a' \in A$ tales que $f(a) = f(a')$. Como f^{-1} es una aplicación, tendremos que $f^{-1}(f(a)) = f^{-1}(f(a'))$, por lo que

$$(f^{-1} \circ f)(a) = (f^{-1} \circ f)(a')$$

y, en virtud de la proposición 6.5.2, $i_A(a) = i_A(a')$, de donde $a = a'$.

Por otra parte, sea b un elemento arbitrario de B. Como f^{-1} es una aplicación, la imagen de b debe ser única; sea ésta $a = f^{-1}(b)$, luego $f(a) = b$. Luego f es sobreyectiva.

■

Proposición 6.5.4 *Si $f : A \longrightarrow B$ es una aplicación y existe una aplicación $g : B \longrightarrow A$ tal que $g \circ f = i_A$ y $f \circ g = i_B$, entonces se verifica que la inversa de f es una aplicación $f^{-1} : B \longrightarrow A$ biyectiva y tal que $g = f^{-1}$.*

Demostración. Sean $a, a' \in A$ tales que $f(a) = f(a')$, entonces $g(f(a)) = g(f(a'))$, por lo que $i_A(a) = i_A(a')$ y de aquí que $a = a'$. Por tanto f es inyectiva.

Por otra parte, cualquiera que sea $b \in B$, existe $a \in A$ tal que $g(b) = a$ y

$$b = i_B(b) = (f \circ g)(b) = f(g(b)) = f(a),$$

de donde resulta que f es sobreyectiva.

Ya que f es biyectiva, de la proposición 6.5.3, se sigue que la inversa de f es una aplicación y, por la proposición 6.5.2, se tiene que $f^{-1} \circ f = i_A$ y $f \circ f^{-1} = i_B$. Ahora bien,

$$g = g \circ i_B = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = i_A \circ f^{-1} = f^{-1}.$$

Puesto que f^{-1} es aplicación y f es su inversa, se sigue de la proposición 6.5.3 que f^{-1} es biyectiva.

■

Ejemplo 6.5.5

1. Sea $f : \mathbb{R} \longrightarrow (-1, 1)$ tal que para cada $x \in \mathbb{R}$ se tiene que $f(x) = \frac{x}{1+|x|}$. Veamos que admite aplicación inversa probando que es biyectiva.

   Sean $x, x' \in \mathbb{R}$ tales que $f(x) = f(x')$, luego

$$\frac{x}{1+|x|} = \frac{x'}{1+|x'|}, \tag{6.1}$$

de donde se deduce que $x + x|x'| = x' + x'|x|$ o de forma equivalente

$$x + xx' \operatorname{sign}(x') = x' + x'x \operatorname{sign}(x), \tag{6.2}$$

siendo $\operatorname{sign}(x)$ la función que vale 1 si $x > 0$, -1 si $x < 0$ y 0 si $x = 0$, y que se denomina la función *signo de* x. Se ha tenido en cuenta que $|x| = x \cdot \operatorname{sign}(x)$.

De (6.1) se sigue que $\operatorname{sign}(x) = \operatorname{sign}(x')$, y sustituyendo en (6.2) resulta finalmente que $x = x'$, por lo que f es inyectiva.

Sea $y \in (-1, 1)$, entonces si $x = \frac{y}{1-|y|}$, tendremos que $\operatorname{sign}(x) = \operatorname{sign}(y)$ y que $y = x - x|y| = x - xy \operatorname{sign}(y)$, por lo que $x = y + yx \operatorname{sign}(x) = y + y|x|$. De aquí resulta que $y = \frac{x}{1+|x|}$. Por tanto, existe $x = \frac{y}{1-|y|} \in \mathbb{R}$ tal que $f(x) = y$; es decir, f es sobreyectiva.

Concluimos, por la proposición 6.5.3 que f^{-1} es una aplicación, consecuentemente, por la proposición 6.5.4, es además biyectiva y $f^{-1}(x) = \frac{x}{1-|x|}$. Puede comprobar el lector como la composición de f y f^{-1} es la identidad en $\mathbb{R}$ y que la composición en el otro orden es la identidad en $(-1, 1)$.

2. Sea $f : \mathbb{R} \setminus \{0\} \longrightarrow \mathbb{R} \setminus \{2\}$ tal que $f(x) = \frac{1}{x} + 2$. Veamos que f es biyectiva, acudiendo ahora a la determinación de la aplicación inversa de f.

   Si $y = \frac{1}{x} + 2$, entonces $xy = 1 + 2x$ y de aquí que $x = \frac{1}{y-2}$. Veamos que si llamamos $f^{-1}(x) = \frac{1}{x-2}$ entonces efectivamente f^{-1} es la aplicación inversa de f.

   En efecto $f^{-1} : \mathbb{R} \setminus \{2\} \longrightarrow \mathbb{R} \setminus \{0\}$ es una aplicación, pues cualquiera que sea $x \in \mathbb{R} \setminus \{2\}$ se tiene que existe $\frac{1}{x-2}$ y que es única y desde luego $f^{-1}(x) \neq 0$.

   Por otra parte $f^{-1}(f(x)) = f^{-1}(\frac{1}{x} + 2) = \frac{1}{\frac{1}{x}+2-2} = \frac{1}{\frac{1}{x}} = x$, por lo que

$$f^{-1} \circ f = i_{\mathbb{R}\setminus\{0\}}. \tag{6.3}$$

   Análogamente,

$$f(f^{-1}(x)) = f(\frac{1}{x-2}) = \frac{1}{\frac{1}{x-2}} + 2 = x - 2 + 2 = x,$$

   de donde

$$f \circ f^{-1} = i_{\mathbb{R}\setminus\{2\}}. \tag{6.4}$$

   De (6.3), (6.4) y la proposición 6.5.4 se sigue que f^{-1} es la aplicación inversa y consecuentemente, en virtud de la proposición 6.5.3, que f es biyectiva.

□

Ejercicios

1. Para cada relación f hallar f^{-1} indicando en cada caso si se trata de una aplicación:
   (a) $f : \mathbb{R} \longrightarrow \mathbb{R}$, tal que $f(x) = x^2$.
   (b) $f : \mathbb{R} \longrightarrow \mathbb{R}$, tal que $f(x) = \dfrac{x+81}{2}$.
   (c) $f = \{(x, y) \in \mathbb{R}^2 : \ 3x - 2y + 5 = 0\}$.
   (d) $f = \{(x, y) \in \mathbb{R}^2 : \ \dfrac{x}{5} + \dfrac{y}{6} = 1\}$.
2. Hallar $f^{-1} \circ g$, $g \circ f^{-1}$ y $(h \circ g^{-1}) \circ f^{-1}$, donde f, g y h son funciones reales de variable real definidas como sigue: $f(x) = x^3$, $g(x) = 2x - 3$, $h(x) = 2^x$.
3. Demostrar que si dos aplicaciones $f : A \longrightarrow B$ y $g : B \longrightarrow C$ son biyectivas, se verifica que $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
4. Demostrar que la aplicación $f : \mathbb{R} \setminus \{-\frac{1}{2}\} \longrightarrow \mathbb{R} \setminus \{\frac{1}{2}\}$, definida de la forma $f(x) = \dfrac{x+3}{1+2x}$ es biyectiva y determinar la aplicación inversa f^{-1}.

6.6 Imágenes de subconjuntos e imágenes inversas de subconjuntos

Definición 6.6.1 *Sea la aplicación $f : A \longrightarrow B$ y sean $A_1 \subseteq A$ y $B_1 \subseteq B$. Llamamos imagen de A_1, por f, y lo denotamos mediante $f(A_1)$ al conjunto*

$$f(A_1) = \{f(x) : \ x \in A_1\} = \{y \in B : \ \text{existe } x \in A_1 \text{ tal que } f(x) = y\}.$$

Y llamamos imagen inversa de B_1, por f, y lo denotamos por $f^{-1}(B_1)$ al conjunto

$$f^{-1}(B_1) = \{x \in A : f(x) \in B_1\}.$$

Ejemplo 6.6.2 Sea f la función real de variable real tal que $f(x) = x^2$ y sean los subconjuntos de $\mathbb{R}$: $A = \{x \in \mathbb{R} : \ 0 \leq x < 2\}$ y $B = \{x \in \mathbb{R} : \ 0 \leq x < 4\}$. Entonces:

$$f(A) = \{x \in \mathbb{R} : \ 0 \leq x < 4\}$$

y

$$f^{-1}(B) = \{x \in \mathbb{R} : \ 0 \leq x^2 < 4\} = \{x \in \mathbb{R} : \ -2 < x < 2\}.$$

□

Algunas propiedades interesantes relativas a la imagen de subconjuntos se recogen en la siguiente proposición que se deja como ejercicio al lector.

Proposición 6.6.3 *Sea la aplicación $f : A \longrightarrow B$ y sean $A_1 \subseteq A$ y $A_2 \subseteq A$, entonces se verifican las siguientes afirmaciones:*

1. *Si $A_1 \subseteq A_2$ entonces $f(A_1) \subseteq f(A_2)$.*
2. $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.
3. $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$.

En relación a la imagen inversa de un subconjunto de B enunciamos a continuación algunas propiedades de interés, cuya demostración por parte del lector será provechosa.

Proposición 6.6.4 *Sea la aplicación $f : A \longrightarrow B$ y sean $B_1 \subseteq B$ y $B_2 \subseteq B$, entonces se verifican las siguientes afirmaciones:*

1. *Si $B_1 \subseteq B_2$ entonces $f^{-1}(B_1) \subseteq f^{-1}(B_2)$.*
2. $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.
3. $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

Se pueden generalizar algunas de estas propiedades, como indicamos seguidamente.

Proposición 6.6.5 *Sea la aplicación $f : A \longrightarrow B$ y sean $\{A_i\}_{i\in\mathcal{I}}$ y $\{B_j\}_{j\in\mathcal{J}}$ dos familias de subconjuntos, respectivamente, de A y B, entonces se verifican las siguientes afirmaciones:*

1. $f\left(\bigcup_{i\in\mathcal{I}} A_i\right) = \bigcup_{i\in\mathcal{I}} f(A_i)$.
2. $f\left(\bigcap_{i\in\mathcal{I}} A_i\right) \subseteq \bigcap_{i\in\mathcal{I}} f(A_i)$.
3. $f^{-1}\left(\bigcup_{j\in\mathcal{J}} B_j\right) = \bigcup_{j\in\mathcal{J}} f^{-1}(B_j)$.
4. $f^{-1}\left(\bigcap_{j\in\mathcal{J}} B_j\right) = \bigcap_{j\in\mathcal{J}} f^{-1}(B_j)$.

Resaltemos finalmente que:

1. $A_1 \subseteq f^{-1}(f(A_1))$, para $A_1 \subseteq A$, ya que si $x \in A_1$, entonces $f(x) \in f(A_1)$, por lo que $x \in f^{-1}(f(A_1))$.
2. $f(f^{-1}(B_1)) \subseteq B_1$, para $B_1 \subseteq B$. En efecto, si $y \in f(f^{-1}(B_1))$, entonces existe $x \in f^{-1}(B_1)$ tal que $f(x) = y$, por lo que $y = f(x) \in B_1$.

Ejercicios

1. Sea $f : X \longrightarrow Y$ una aplicación y sean los subconjuntos $A \subseteq X$ y $B \subseteq Y$. Demostrar:

   (a) $f(X) \setminus f(A) \subseteq f(X \setminus A)$.

   (b) $f^{-1}(Y \setminus B) = X \setminus f^{-1}(B)$.

   (c) $f(A \cap f^{-1}(B)) = f(A) \cap B$.

2. Sea $f : A \longrightarrow B$ una aplicación y A_1 y A_2 subconjuntos de A. Probar que, en general, $f(A_1 \cap A_2) \neq f(A_1) \cap f(A_2)$. ¿Bajo qué condiciones se puede asegurar la igualdad?

3. Sea A un conjunto y $f : \mathcal{P}(A) \longrightarrow \mathbb{R}$ una aplicación con valores reales, tal que si X e Y son subconjuntos de A entonces $f(X \cup Y) = f(X) + f(Y)$. Probar que:

   (a) $f(\emptyset) = 0$.

   (b) $f(X \cup Y) = f(X) + f(Y) - f(X \cap Y)$.

6.7 Relación de equivalencia asociada a una aplicación. Descomposición canónica

La existencia de una aplicación $f : A \longrightarrow B$ permite definir una relación de equivalencia en A, si establecemos que dos elementos están relacionados si tienen la misma imagen. Así, pues, definimos la relación $\mathcal{R}$ en A de la siguiente manera:

$$x \mathcal{R} y \qquad \text{si y sólo si} \qquad f(x) = f(y).$$

Evidentemente es una relación de equivalencia, que se denomina "la relación de equivalencia asociada a la aplicación f en A". Una clase de equivalencia $[a]$ es de la forma $[a] = \{x \in A : f(x) = f(a) = b\} = f^{-1}(b)$. El conjunto cociente se representa por $A/_{\mathcal{R}}$ o también por $A/_f$.

Definición 6.7.1 *Sea $f : A \longrightarrow B$ una aplicación y $\mathcal{R}$ su relación de equivalencia asociada. A la aplicación*

$$\begin{array}{rccc} \varphi : & A & \longrightarrow & A/_{\mathcal{R}} \\ & a & \longmapsto & [a] \end{array}$$

se le denomina "aplicación canónica o natural asociada a f".

La anterior definición tiene sentido toda vez que de forma evidente φ es una aplicación, y además es sobreyectiva, pues cualquiera que sea $[a] \in A/_f$, es obvio que existe el propio $a \in A$ tal que $\varphi(a) = [a]$.

Ejemplo 6.7.2 Sea $f : \mathbb{Z} \longrightarrow \mathbb{N}$ tal que $f(x) = |x|$. En este caso

$$a \mathcal{R} b \qquad \text{si y sólo si} \qquad |a| = |b|,$$

o equivalentemente si y sólo si $b = a$ o bien $b = -a$, de donde $[a] = \{-a, a\}$ y por tanto $\mathbb{Z}/_f = \{[a] : a \in \mathbb{Z}\}$. □

Proposición 6.7.3 *$g : A/_f \longrightarrow Im\ f$, tal que $g([a]) = f(a)$, es una aplicación biyectiva.*

Demostración. Es claro que g se trata de una aplicación.

Veamos que es inyectiva. Si $g([a]) = g([b])$ entonces $f(a) = f(b)$, por lo que $a, b \in [a]$ y de aquí que $[a] = [b]$.

También es sobreyectiva. Si $b \in Im\ f$ entonces existe $a \in A$ tal que $f(a) = b$, pero $a \in A$ ha de pertenecer a alguna clase de equivalencia, por lo que existe $[a] \in A/_f$ tal que $g([a]) = f(a) = b$.

■

Para una aplicación $f : A \longrightarrow B$, si consideramos: la aplicación canónica asociada a f, la aplicación g definida anteriormente y la aplicación inyectiva inmersión $i : Im\ f :\longrightarrow B$, obtenemos el siguiente resultado.

Proposición 6.7.4 *Si $f : A \longrightarrow B$ es una aplicación, entonces se verifica que $f = i \circ g \circ \varphi$.*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \varphi \downarrow & & \uparrow\ i \\ A/_f & \xrightarrow{g} & Im\ f \end{array}$$

Demostración. Sea $a \in A$, entonces

$$i \circ g \circ \varphi(a) = i \circ g(\varphi(a)) = i \circ g([a]) = i(g([a])) = i(f(a)) = f(a),$$

de donde se sigue que $i \circ g \circ \varphi = f$.

■

La expresión de f como composición de φ, g e i se denomina *la descomposición canónica de la aplicación f.*

Ejemplo 6.7.5 Sea $f : \mathbb{Z} \longrightarrow \mathbb{N}$ tal que $f(x) = |x|$, tenemos que:

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{f} & \mathbb{N} \\ \varphi \downarrow & & \uparrow\ i \\ \mathbb{Z}/_f & \xrightarrow{g} & Im\ f \end{array}$$

Y

1. $\varphi(a) = [a] = \{-a, a\}$.
2. $g(\{-a, a\}) = f(a) = |a|$.
3. $i(|a|) = |a|$.

Por lo tanto,

$$i \circ g \circ \varphi(a) = i \circ g(\varphi(a)) = i \circ g(\{-a, a\}) = i(g(\{-a, a\})) = i(|a|) = |a| = f(a),$$

por lo que $i \circ g \circ \varphi = f$. □

Ejercicios

1. Se considera la aplicación $f : \mathbb{Z} \longrightarrow \mathbb{N}$ tal que $f(x) = x^2$ y la relación $\mathcal{R}$ asociada a f. Hallar las clases de equivalencia, el conjunto cociente y la aplicación canónica asociada a f.

2. Se considera la aplicación $f : A \longrightarrow B$, tal que $f(x) = x^2$, siendo

   $$A = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7\} \text{ y } B = \{x \in \mathbb{N} : \ x \leq 50\}.$$

   Hallar la descomposición canónica de f.

3. Sean $A = \{a, b, c, d, e, f\}$ y $\mathcal{P}(A)$. Entre $\mathcal{P}(A)$ y $B = \{0, 1, 2, 3, 4, 5, 6\}$ se define la aplicación h dada por $h(x) = card(x)$ (donde $card(x)$ indica el número de elementos de $x \in \mathcal{P}(A)$). Estudiar la relación de equivalencia asociada a h, hallar las clases de equivalencia y el conjunto cociente. Obtener la descomposición canónica de h.

4. Dados los conjuntos $A = \{a, b, c, d, e, f, g, h\}$ y $B = \{1, 2, 3, 4, 5, 6\}$ y la aplicación $f : A \longrightarrow B$ dada por

   $$\{(a, 1), (b, 1), (c, 3), (d, 3), (e, 3), (f, 4), (g, 4), (h, 5)\},$$

   estudiar la relación de equivalencia asociada a f, determinar las clases de equivalencia y el conjunto cociente.

5. Sea P el conjunto de todos los polígonos regulares y sea la aplicación $f : P \longrightarrow \mathbb{N}$ tal que $f(p) =$ "número de lados del polígono p". Estudiar la relación de equivalencia asociada a f y determinar las clases de equivalencia y el conjunto cociente. Hallar la descomposición canónica de f.

6. Se considera la función parte entera de x, $E(x)$, definida en $\mathbb{R}$. Hallar la descomposición canónica de f.

7. Sean U un conjunto, $A \subseteq U$ y tanto f como g dos aplicaciones de $\mathcal{P}(U)$ en sí mismo, definidas por $f(X) = A \cap X$ y $g(X) = A \cup X$, siendo $X \in \mathcal{P}(U)$.
   (a) Hallar la descomposición canónica de f.
   (b) Hallar la descomposición canónica de g.
   (c) Demostrar que existe una biyección de $g(\mathcal{P}(U))$ en $\mathcal{P}(U \setminus A)$.

8. Sea X el conjunto de todas las aplicaciones de $\mathbb{R}$ en $\mathbb{R}$. Se define en X la siguiente relación:
   $f \mathcal{R} g$ si y sólo si existe $c \in \mathbb{R}^+$ tal que $f(t) = g(t)$ para todo $t \in \mathbb{R}$ tal que $|t| < c$.
   (a) Demostrar que se trata de una relación de equivalencia.
   (b) Sea q un polinomio arbitrario, ¿qué funciones polinómicas pertenecen a la clase de q?

6.8 Aplicaciones y conjuntos ordenados

Definición 6.8.1 *Si A es un conjunto que está ordenado mediante $\preceq$, B es otro conjunto ordenado mediante $\leq$ y $f : A \longrightarrow B$ es una aplicación, decimos que f es creciente o también que es un morfismo de orden (estrictamente creciente) si cualesquiera que sean $x, y \in A$ verificando que $x \prec y$, entonces $f(x) \leq f(y)$ $(f(x) < f(y))$.*

Diremos que f es decreciente (estrictamente decreciente) si cualesquiera que sean $x, y \in A$ verificando que $x \prec y$, entonces $f(x) \geq f(y)$ $(f(x) > f(y))$.

Hemos de aclarar que mediante $\leq$ se está indicando un orden cualquiera y que $a < b$ indica que a es estrictamente anterior a b; es decir, que $a \leq b$ y $a \neq b$. De la misma manera hemos de recordar que $x \prec y$ significa que x es estrictamente anterior a y; es decir que $x \preceq y$ y $x \neq y$.

Definición 6.8.2 *Si A es un conjunto que está ordenado mediante $\preceq$, B es otro conjunto ordenado mediante $\leq$ y $f : A \longrightarrow B$ es una aplicación, decimos que f es monótona (estrictamente monótona) si f es creciente o decreciente (estrictamente creciente o estrictamente decreciente).*

Si f es un morfismo de orden biyectivo entonces f^{-1} es una aplicación biyectiva, pero en general no es un morfismo de orden de B en A.

Ejemplo 6.8.3 Sea $A = \{a, b\}$ y sean las relaciones de orden en A: $\preceq$, dada por $\{(a, a), (b, b)\}$, y $\leq$, dada por $\{(a, a), (b, b), (a, b)\}$.

Sea $f : A \longrightarrow A$, considerando el conjunto inicial ordenado mediante $\preceq$ y el conjunto final ordenado mediante $\leq$, y definida por $f(a) = a$ y $f(b) = b$.

Es claro que f es una aplicación biyectiva y que además es un morfismo de orden. Desde luego f^{-1} es también una aplicación biyectiva, pero sin embargo, ahora, no es un morfismo de orden pues $a \leq b$ y en cambio $a \not\preceq b$. □

Vemos ahora una condición suficiente para que la inversa de un morfismo biyectivo sea un morfismo.

Proposición 6.8.4 *Si A está totalmente ordenado, mediante $\preceq$, B está ordenado mediante $\leq$ y f es un morfismo biyectivo de A en B, entonces f^{-1} es un morfismo biyectivo de B en A.*

Demostración. Basta probar que f^{-1} es un morfismo de orden de B en A. Supongamos que no lo es; por lo que existirán $y, y' \in B$ tales que $y < y'$ y $f^{-1}(y) = x \not\preceq f^{-1}(y') = x'$. Ahora bien, A está totalmente ordenado, por tanto $f^{-1}(y') = x' \prec x = f^{-1}(y)$. Pero f es un morfismo, por lo que $f(x') \leq f(x)$ y de aquí que $y' \leq y$, contradiciendo que $y < y'$.

■

Definición 6.8.5 *Si A es un conjunto que está ordenado mediante $\preceq$, B es otro conjunto ordenado mediante $\leq$ y $f : A \longrightarrow B$ es una aplicación, decimos que f es un isomorfismo de orden de A en B, si es un morfismo de orden biyectivo y f^{-1} también es un morfismo de orden biyectivo. En esta circunstancia decimos que A, con el orden $\preceq$, y B, con el orden $\leq$, son conjuntos isomorfos.*

Se sigue inmediatamente, de la proposición 6.8.4, que si A y B son conjuntos totalmente ordenados, entonces un morfismo de orden es isomorfismo de orden si y sólo si la aplicación es biyectiva.

Si A es un conjunto ordenado mediante $\preceq$ y B lo es mediante $\leq$, se deduce inmediatamente, de las definiciones anteriores, que:

1. Toda aplicación estrictamente creciente (estrictamente decreciente) es creciente (decreciente).

2. Toda aplicación estrictamente monótona es monótona.

3. Toda aplicación creciente (decreciente) e inyectiva es estrictamente creciente (estrictamente decreciente).

   Hemos de resaltar que sin embargo una aplicación estrictamente creciente o estrictamente decreciente entre conjuntos ordenados no tiene porqué ser inyectiva. Es inyectiva si y sólo si el conjunto original de la aplicación es totalmente ordenado.

4. La condición necesaria y suficiente para que una aplicación biyectiva f entre dos conjuntos ordenados A y B sea un isomorfismo de orden es que cualesquiera que sean $x, y \in A$, entonces $x \preceq y$ si y sólo si $f(x) \leq f(y)$.

5. Si A es totalmente ordenado y B es parcialmente ordenado, entonces f es un isomorfismo de orden si y sólo si f es sobreyectiva y estrictamente creciente.

Veamos finalmente que la existencia de un orden $\preceq$ en un conjunto A, permite ordenar otro conjunto B si existe una aplicación biyectiva $f : A \longrightarrow B$, de forma que f resulta ser un isomorfismo de orden.

Proposición 6.8.6 *Sea A un conjunto ordenado, mediante $\preceq$, y f una aplicación biyectiva entre A y un conjunto B. Entonces, la relación definida en B por: "cualesquiera que sean $y, y' \in B$, $y \leq y'$ si y sólo si $f^{-1}(y) \preceq f^{-1}(y')$" es un orden sobre B y f es un isomorfismo de orden entre los conjuntos ordenados A y B. Si el orden de A es total, entonces el de B también lo será.*

Demostración. Como $f^{-1}(y) \preceq f^{-1}(y)$ se sigue $y \leq y$. Luego $\leq$ es reflexiva.

Si $y, y' \in B$ verifican que $y \leq y'$ e $y' \leq y$, entonces $f^{-1}(y) \preceq f^{-1}(y')$ y $f^{-1}(y') \preceq f^{-1}(y)$, de donde $f^{-1}(y) = f^{-1}(y')$ y de aquí que $y = y'$, toda vez que f es biyectiva, resultando que $\leq$ es antisimétrica.

Si $y, y', y'' \in B$ son tales que $y \leq y'$ e $y' \leq y''$, entonces $f^{-1}(y) \preceq f^{-1}(y')$ y $f^{-1}(y') \preceq f^{-1}(y'')$, por tanto $f^{-1}(y) \preceq f^{-1}(y'')$, luego $y \leq y''$, resultando que $\leq$ es transitiva.

Por otra parte, si $y, y' \in B$ son tales que $y < y'$, entonces, por la definición del orden en B, se tiene que $f^{-1}(y) \preceq f^{-1}(y')$ y, como f es biyectiva, f^{-1} es también una aplicación y además biyectiva. Tenemos que f^{-1} es un morfismo de orden biyectivo. Además si $x \prec x'$, entonces $f(x) \leq f(x')$, pues de lo contrario $y' < y$ (siendo $f(x') = y'$ y $f(x) = y$) y al ser f biyectiva tendremos que $x' \prec x$, lo que es absurdo; así, pues, f es un morfismo biyectivo. Concluimos que f es un isomorfismo de orden.

Finalmente, supongamos que A es totalmente ordenado. Sean $y, y' \in B$, entonces $f^{-1}(y), f^{-1}(y') \in A$, por lo tanto se tendrá que $f^{-1}(y) \preceq f^{-1}(y')$ o bien $f^{-1}(y') \preceq f^{-1}(y)$, pero entonces $y \leq y'$ o bien $y' \leq y$, resultando que B está totalmente ordenado mediante $\leq$.

■

Ejercicios

1. Demostrar que si A es un conjunto totalmente ordenado, B es un conjunto ordenado y A y B son isomorfos, entonces B está totalmente ordenado.

2. Sea E un conjunto ordenado mediante una relación que denotaremos por $\leq$. *Una parte X de E se dice* **libre** *si no es vacía y si dos elementos*

distintos cualesquiera de X son no comparables . Sea L el conjunto de las partes libres de E. Se define en L la relación de orden $\mathcal{R}$ dada por $X \mathcal{R} Y$ *si y sólo si para todo* $x \in X$ *existe un* $y \in Y$ *tal que* $x \leq y$. Demostrar que:

(a) La aplicación $f : E \to L$ dada por $f(x) = \{x\}$, es un isomorfismo de E en una parte de L.

(b) Si E es totalmente ordenado, entonces f es un isomorfismo.

3. Sean Y un conjunto no vacío, $(\mathbb{N}, \leq)$ el conjunto ordenado de los números naturales con el orden usual y $f : X \to \mathbb{N}$ una aplicación. Se define en Y la siguiente relación:

$$x \preceq y \iff f(x) \leq f(y).$$

Demostrar que:

(a) La relación $\preceq$ no es en general una relación de orden.

(b) La relación $\preceq$ es una relación de orden si f es una aplicación inyectiva.

4. Probar que si f es un isomorfismo de orden entre $(A, \preceq)$ y $(B, \leq)$ y g es otro isomorfismo de orden entre $(B, \leq)$ y $(C, \ll)$, entonces $g \circ f$ es un isomorfismo de orden entre $(A, \preceq)$ y $(C, \ll)$.

Capítulo 7

Inducción

7.1 Introducción

En el segundo capítulo hemos visto algunos métodos de demostración de teoremas y ahora estamos en condiciones de abordar una técnica más: *la inducción matemática*; que es especialmente adecuada para probar proposiciones relativas al conjunto de los números naturales. Así, si quisiéramos demostrar que $\sum_{i=0}^{n} 3^i = \frac{1}{2}(3^{n+1}-1)$, cualquiera que sea $n \in \mathbb{N}$, lo que estamos diciendo es que deseamos probar la anterior expresión para cada valor natural: $0, 1, 2, 3, 4, \ldots$.

Cuando se nos presentan situaciones en las que es preciso demostrar que para cada número natural se verifica una cierta propiedad P, no podemos obviamente probar cada caso particular $P(0)$, $P(1)$, $P(2)$, etc., pretendiendo agotar el universo de los naturales, por lo que se hace preciso buscar un procedimiento "finito" que nos garantice que la propiedad P se verifica para cada $n \in \mathbb{N}$.

Supongamos que probamos:

1. La propiedad P para $n = 0$.

2. Que cada vez que aumentemos en 1 el valor de n, si para n se verifica la propiedad P, entonces para $n+1$ también se verifica.

En estas condiciones habremos probado que se verifica la propiedad P para cada valor de n, pues: si es cierto $P(0)$, también lo será $P(1)$ (por 2.), pero al ser $P(1)$ cierta, entonces también lo será $P(2)$ (nuevamente en virtud de 2.), y así sucesivamente. En esto consiste el proceso de inducción, en probar:

1. $P(0)$.

2. Para cada $n \in \mathbb{N}$, $P(n)$ implica $P(n+1)$.

Ejemplo 7.1.1 Demostremos que $\sum_{i=0}^{n} 3^i = \frac{1}{2}(3^{n+1} - 1)$.

Tenemos una propiedad P que se afirma para cada valor de $n \in \mathbb{N}$, que es:

$$\text{“}3^0 + 3^1 + 3^2 + \ldots + 3^n = \frac{1}{2}(3^{n+1} - 1)\text{”}.$$

Si $n = 0$ entonces $3^0 = \frac{1}{2}(3^1 - 1) = 1$.

Por otra parte, hemos de probar que si P es cierta para n, entonces P también se verifica para $n + 1$, siendo $n \in \mathbb{N}$ arbitrario. Veámoslo.

Sea $n \in \mathbb{N}$ un número natural cualquiera y supongamos que para él se verifica que $\sum_{i=0}^{n} 3^i = \frac{1}{2}(3^{n+1} - 1)$. De aquí hemos de deducir que para el natural siguiente $n + 1$, la propiedad se verifica; es decir, que:

$$\sum_{i=0}^{n+1} 3^i = \frac{1}{2}(3^{n+2} - 1).$$

Ahora bien,

$$\begin{aligned}
\textstyle\sum_{i=0}^{n+1} 3^i &= \textstyle\sum_{i=0}^{n} 3^i + 3^{n+1} \\
&= \tfrac{1}{2}(3^{n+1} - 1) + 3^{n+1} && \text{(por hipótesis)} \\
&= \tfrac{1}{2}3^{n+1} - \tfrac{1}{2} + 3^{n+1} = \tfrac{3}{2}3^{n+1} - \tfrac{1}{2} \\
&= \tfrac{1}{2}3^{n+2} - \tfrac{1}{2} = \tfrac{1}{2}(3^{n+2} - 1).
\end{aligned}$$

□

No debiéramos tener duda alguna en aceptar este procedimiento de demostración, del mismo modo que no la albergamos de las leyes de inferencia de la lógica. El principio de inducción se basa en el hecho de que después de cada número natural n hay uno que lo sigue $n + 1$, y que todo natural m puede ser alcanzado mediante un número finito de pasos, a partir del 0.

7.2 Conjuntos inductivos

Desde nuestro enfoque de la teoría de conjuntos no debiera haber objeción alguna a emplear el concepto de número natural con la despreocupación con que lo hacemos. Al fin y al cabo, la existencia de éstos podría integrar nuestro punto de partida, ¿hay acaso algo más *natural* que los números naturales? No obstante, vamos a efectuar algunas disgresiones en torno a este asunto, mostrando que desde la teoría axiomática de conjuntos pueden construirse los números naturales y evidenciando de paso la necesidad de algún postulado más de la axiomática de Zermelo–Fraenkel.

Para cada conjunto X definimos un nuevo conjunto que tenga como elementos los de X y al propio X, que denominaremos *sucesor* de X y que denotaremos mediante X^+. Así pues,

$$X^+ = X \cup \{X\}.$$

Ejemplo 7.2.1 Consideremos el conjunto vacío $\emptyset$, entonces

$$\emptyset^+ = \emptyset \cup \{\emptyset\} = \{\emptyset\}.$$

Ahora tendremos que

$$\{\emptyset\}^+ = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}.$$

Podemos obtener a continuación el sucesor de este último conjunto, resultando

$$\{\emptyset, \{\emptyset\}\}^+ = \{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}.$$

□

Desde una perspectiva intuitiva parece claro que un cierto número natural, por ejemplo 1, "se debiera corresponder de alguna manera" con un conjunto que tuviera exactamente un elemento. Y el 2 se debiera corresponder con un conjunto que tuviese exactamente dos elementos. Ahora bien, supuesto que hemos sido capaces de definir el 1, el 2 se podría construir fácilmente formando el conjunto de dos elementos consistente en el elemento que tenía el conjunto 1 y añadiéndole el propio conjunto 1; es decir 2 sería el sucesor de 1. Si repetimos este proceso podemos ir construyendo números sobre los construidos anteriormente.

Para nuestros propósitos es conveniente comenzar con el número 0, como un conjunto que no tiene elementos, por tanto $0 = \emptyset$. Ahora definimos el 1 como el sucesor de 0 y tendremos

$$1 = \emptyset^+ = \emptyset \cup \{\emptyset\} = \{\emptyset\}.$$

Definimos el 2 como el sucesor del 1,

$$2 = 1^+ = \{\emptyset\}^+ = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} = \{0, 1\}.$$

Definimos el tres como el sucesor del 2

$$3 = 2^+ = \{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\}.$$

Y así sucesivamente. ¿Hasta cuándo? Desde los axiomas que conocemos no podemos garantizar la construcción de todos los números naturales por tratarse de un proceso "infinito". Necesitamos una nueva herramienta:

Axioma del infinito:
Existe un conjunto que contiene al 0 *y al sucesor de cada uno de sus elementos.*

Definición 7.2.2 *Un conjunto A se dice inductivo si se verifica que:*

1. $\emptyset \in A$.
2. *Para cada* $x \in A$, *se tiene que* $x^+ \in A$.

En términos de esta última definición, el *axioma del infinito* afirma que existe un conjunto A inductivo.

Si B y C son inductivos, claramente $B \cap C$ es inductivo. De forma general, la intersección de cualquier familia no vacía de conjuntos inductivos es también un conjunto inductivo.

Veamos cómo esta propiedad puede usarse para demostrar que existe un único conjunto inductivo que está contenido en todos los demás.

Sea A el conjunto inductivo cuya existencia queda garantizada por el *axioma del infinito*. Si existen otros conjuntos inductivos contenidos en A, tiene sentido considerar la intersección de todos ellos, que será también inductivo y, a su vez, el "menor" (en el sentido de la inclusión) conjunto inductivo contenido en A, llamémosle provisionalmente N. Este "menor" conjunto inductivo N contenido en A es realmente el "menor" conjunto inductivo, pues si B también es un conjunto inductivo $A \cap B \neq \emptyset$, $A \cap B$ es inductivo y además $A \cap B \subseteq A$, por lo que $N \subseteq A \cap B$ y consecuentemente $N \subseteq B$.

Esta propiedad de ser el "menor" conjunto inductivo (un conjunto inductivo que es subconjunto de cualquier conjunto inductivo) caracteriza al conjunto N de forma única. El axioma de extensión garantiza su unicidad. Este conjunto inductivo "mínimo" recibe el nombre de conjunto de los números naturales y en adelante lo denotaremos por $\mathbb{N}$.

$$\mathbb{N} = \{X \in A : \ X \in B \text{ para cada conjunto inductivo } B\}.$$

Un número natural es, por definición, un elemento de $\mathbb{N}$.

También podemos expresar la propiedad de "minimalidad" de $\mathbb{N}$, como conjunto inductivo, de esta otra manera, que se conoce como:

Principio de inducción matemática:
Si $M \subseteq \mathbb{N}$ *es tal que:*

1. $0 \in M$.
2. *Para cada* $n \in M$, *se verifica que* $n^+ \in M$.

entonces, $M = \mathbb{N}$.

Seguidamente se recogen las propiedades más importantes acerca del conjunto $\mathbb{N}$ de los números naturales:

1. $0 \in \mathbb{N}$.

2. Si $n \in \mathbb{N}$, entonces $n^+ \in \mathbb{N}$.

3. Para cada $n \in \mathbb{N}$ se verifica que $n^+ \neq 0$.

4. Si $n, m \in \mathbb{N}$ son tales que $n^+ = m^+$, entonces $n = m$.

5. Se verifica el principio de inducción matemática.

Todas son inmediatas, partiendo de la axiomática de Zermelo–Fraenkel, a excepción de la 4., pero no nos detendremos en su demostración por apartarse del propósito de este capítulo. Existen excelentes libros (algunos de ellos citados en la bibliografía) que tratan la construcción de los naturales y a los que el lector puede acudir si está interesado en aquella[1].

Estas cinco propiedades de los números naturales se pueden también utilizar como punto de partida para la definición de los mismos. Así, podemos enunciar: "*Existe un conjunto* $\mathbb{N}$ *con las propiedades* 1., 2., 3., 4. *y* 5. *anteriores, y que denominaremos conjunto de los números naturales*". Esta es la introducción *axiomática* de los números naturales, efectuada por Peano (1858–1932).

7.3 Principio de inducción

Retomamos nuestro discurso inicial, pensando que, después de todo, la disgresión anterior le será de utilidad al lector, tanto porque conocerá algo más acerca de los números naturales, como porque ayudará a una adecuada comprensión del principio de inducción, como método de demostración de proposiciones que contemplan una sucesión natural infinita de casos.

Principio de inducción: *Sea P una propiedad que deseamos probar que se verifica para cada número natural n. Indicamos por $P(n)$ la proposición correspondiente a la propiedad P para el valor $n \in \mathbb{N}$. Si se verifica que:*

1. *$P(0)$ es verdadera,*
2. *De ser $P(n)$ verdadera, con $n \in \mathbb{N}$, se deduce que $P(n^+)$ también lo es,*

entonces $P(n)$ es verdadera para cada $n \in \mathbb{N}$.

Demostración:
En efecto. Sea S el conjunto de los números naturales para los que $P(n)$ es verdadera:

$$S = \{n \in \mathbb{N} : \ P(n) \text{ es verdadera}\}.$$

[1] En particular, puede consultar el libro de A. Aizpuru: "Dominios Algebraicos Numéricos".

Es obvio que $0 \in S$ y que, para cada $n \in \mathbb{N}$, si $n \in S$ entonces $n^+ \in S$. En virtud del *principio de inducción matemática* (o axioma V de Peano) se sigue que $S = \mathbb{N}$. Es decir, $P(n)$ es verdadera para cada natural n.

■

El método de inducción consta de dos pasos. El primero requiere probar que la propiedad P se verifica para $n = 0$, es lo que se denomina *caso particular*. El segundo, que se denomina *paso de inducción*, consiste en "suponer" que la propiedad P se verifica para un valor n arbitrario, lo que llamaremos *la hipótesis de inducción* (h.i.), y a partir de ello se trata de demostrar que la propiedad también se verifica para el valor $n + 1$.

Ejemplo 7.3.1 Para cada $n \in \mathbb{N}$ se verifica que $3|(n^3 - n)$.

En efecto. Si $n = 0$ entonces $3|0$ evidentemente. Hagamos ahora la hipótesis de inducción: sea $n \in \mathbb{N}$ arbitrario y supongamos que para él se verifica que $3|(n^3 - n)$. En tal caso se tiene que existe $k \in \mathbb{N}$ tal que $n^3 - n = 3k$. Por tanto:

$$\begin{aligned}(n+1)^3 - (n+1) &= n^3 + 3n^2 + 3n + 1 - n - 1 \\ &= n^3 - n + 3n^2 + 3n \\ &= 3k + 3(n^2 + n) \qquad \text{(por h.i.)} \\ &= 3(k + n^2 + n),\end{aligned}$$

por lo que $3|[(n+1)^3 - (n+1)]$. En virtud del principio de inducción obtenemos la tesis deseada. □

Naturalmente el caso particular no tiene porqué ser necesariamente $n = 0$, bastaría efectuar una mínima alteración en la definición de conjunto inductivo, tomando como punto de partida en lugar de $\emptyset$ cualquier otro conjunto que definiera a un cierto natural k. El resto del razonamiento seguiría siendo válido y obtendríamos que, bajo las dos hipótesis de inducción (alterada la primera en la forma $P(k)$ es verdadera), se tendría que $P(n)$ es verdadera para cada $n \geq k$.

Otra forma de probar la validez de este principio cuando el caso particular es cualquier número natural k, es teniendo en cuenta que $\mathbb{N}$ está bien ordenado mediante el orden usual $\leq$.

Proposición 7.3.2 *Sea $P(n)$ una proposición que se afirma para cada $n \in \mathbb{N}$. Y sean $k \in \mathbb{N}$ y $N = \{n \in \mathbb{N} : n \geq k\}$. Si se verifica que:*

1. *$P(k)$ es verdadera,*
2. *De ser $P(n)$ verdadera, con $n \in N$, se deduce que $P(n+1)$ también lo es,*

entonces $P(n)$ es verdadera para cada $n \in N$.

Demostración. Supongamos que el conjunto

$$B = \{n \in N : \ P(n) \text{ es falsa}\} \subseteq N$$

no es vacío.

Como $\mathbb{N}$ está bien ordenado, mediante $\leq$, entonces N también está bien ordenado, mediante la misma relación. Por tanto existirá $b \in N$ tal que b es el primer elemento de B, de donde

$$P(b) \quad \text{es falsa.} \tag{7.1}$$

Como $P(k)$ es verdadero, se tiene que $k \neq b$ y ha de ser $b > k$, por lo que $b - 1 \geq k$, luego $b - 1 \in N$. Al ser b el primer elemento de B, se tiene que $P(b-1)$ es verdadero, entonces por la segunda hipótesis se tiene que

$$P(b) \quad \text{es verdadero.} \tag{7.2}$$

(7.1) y (7.2) se contradicen, por lo que $B = \emptyset$ y consecuentemente $P(n)$ es verdadera para cada $n \geq k$.

■

Ejemplo 7.3.3

1. Para cada $n \geq 5$, se tiene que $2^n > n^2$.

   Sea $n = 5$, entonces $2^5 = 32 > 5^2 = 25$. Supongamos que es cierto para n arbitrario (hipótesis de inducción). Veamos que también lo es para $n + 1$.

$$\begin{array}{rcll} 2^{n+1} & = & 2 \cdot 2^n & \\ & > & 2n^2 & \text{(por h.i.)} \\ & = & n^2 + n^2 & \\ & \geq & n^2 + 5n = n^2 + 2n + 3n & \text{(ya que } n \geq 5) \\ & > & n^2 + 2n + 1 = (n+1)^2. & \end{array}$$

   En virtud del principio de inducción obtenemos la conclusión deseada.

2. La suma de los primeros n números impares positivos es n^2.

   Para $n = 1$ tendremos el caso particular, que aquí podemos enunciar como "la suma del primer impar es 1^2", lo que evidentemente es cierto.

   Supongamos ahora que $1 + 3 + 5 + \ldots + (2n-1) = n^2$ (que es la hipótesis de inducción) y veamos que también se verifica para los $n + 1$ primeros impares.

$$\begin{array}{rcl} 1 + \ldots + (2n-1) + (2n+1) & = & (1 + \ldots + (2n-1)) + (2n+1) \\ & = & n^2 + (2n+1) \quad \text{(por h.i.)} \\ & = & (n+1)^2. \end{array}$$

3. Para cada $n \in \mathbb{N}$, $n \geq 4$, se tiene que $n! > 2^n$.

   Caso particular: cuando $n = 4$. Se tiene que $4! = 24 > 16 = 2^4$. Supongamos que se verifica que para n arbitrario $n! > 2^n$ (hipótesis de inducción). Veamos que también es cierto para $n + 1$.

$$\begin{aligned} (n+1)! &= (n+1) \cdot n! \\ &> (n+1) \cdot 2^n \quad \text{(por h.i.)} \\ &> 2 \cdot 2^n = 2^{n+1} \quad \text{(pues } n \geq 4\text{)}. \end{aligned}$$

   Concluyendo así con la demostración.

□

Hemos de hacer notar que el caso particular es de vital importancia, una mala elección del mismo nos puede arrastrar a conclusiones erróneas.

Una variante del principio de inducción consiste en suponer, en el paso de inducción, que se verifican $P(0)$, $P(1)$, ..., $P(n-1)$ y que de la verdad de ellos se deduce que $P(n)$ también es verdadera. Es la segunda versión del principio de inducción, que usualmente se conoce como:

Inducción fuerte:
Sea P una propiedad tal que, cualquiera que sea $n \in \mathbb{N}$, de ser verdadera $P(k)$ para cada $k \in \mathbb{N}$ con $k < n$, se deduce que $P(n)$ es también verdadera. Entonces $P(n)$ es verdadera para todo $n \in \mathbb{N}$.

Es decir, para demostrar $P(n)$, para todo $n \in \mathbb{N}$, es suficiente demostrar $P(n)$, para cada $n \in \mathbb{N}$, suponiendo que se verifica $P(k)$, para cada $k \in \mathbb{N}$ con $k < n$.

Expresada como una regla de inferencia la inducción fuerte tiene la forma:

$$\forall n[(\forall k < n\, P(k)) \longrightarrow P(n)] \longrightarrow \forall n P(n),$$

mientras que la primera formulación del principio de inducción tiene la forma:

$$[P(0) \wedge \forall n(P(n) \longrightarrow P(n+1))] \longrightarrow \forall n P(n).$$

Realmente no se trata de un principio diferente a la primera versión, pues ambos son equivalentes. Es decir, cada uno puede ser demostrado como un método de demostración válido, suponiendo el otro.

Proposición 7.3.4 *Los principios de inducción e inducción fuerte son equivalentes.*

Demostración. Admitamos el principio de inducción y supongamos que:

si $P(k)$ es verdadero para todo $k < n$, entonces $P(n)$ es verdadero. (7.3)

Sea $Q(n)$ la propiedad "$P(k)$ se verifica para cada $k < n$". Desde luego $Q(0)$ se verifica ya que no existe k natural y $k < 0$.

Si $Q(n)$ se verifica; es decir, si $P(k)$ es verdadero para cada $k < n$, entonces $P(n)$ se verifica, en virtud de (7.3). Luego $P(k)$ se verifica para todo $k < n+1$ y de esta forma $Q(n+1)$ se verifica.

Al verificar $Q(n)$ los requisitos del principio de inducción, se tiene que $Q(n)$ es verdadera para todo $n \in \mathbb{N}$. Luego $P(n)$ se verifica para todo $n \in \mathbb{N}$.

Dejamos como ejercicio para el lector probar la implicación recíproca.

■

No obstante la equivalencia existente entre ambas formulaciones del principio de inducción, a veces es más adecuado utilizar la segunda, como ponemos de manifiesto en los siguientes ejemplos.

Ejemplo 7.3.5

1. Probemos que cualquier entero mayor que 1 puede descomponerse en el producto de factores primos (Teorema Fundamental de la Aritmética).

   Sea $P(n)$ la proposición "n se puede descomponer en factores primos". Desde luego $P(2)$ es verdadero. Supongamos que $P(k)$ es verdadero para cada $k \in \mathbb{N}$, con $k \leq n$. Debemos probar que $P(n+1)$ es verdadero.

   Si $n+1$ es primo, tenemos de inmediato que $P(n+1)$ es verdadero. Si $n+1$ es compuesto, entonces se tiene que $n+1 = p \cdot q$, siendo $2 \leq p \leq q < n+1$. Por hipótesis de inducción, tanto p como q se pueden escribir como el producto de primos, por lo que $n+1$ se puede expresar como producto de primos y $P(n+1)$ es verdadera.

   Concluimos que $P(n)$ es verdadera cualquiera que sea $n \in \mathbb{N}$, $n > 1$.

2. Veamos que $\mathbb{N}$, con el orden usual $\leq$, se trata de un conjunto bien ordenado.

   Supongamos que $A \subseteq \mathbb{N}$, pero que no tiene primer elemento. Probaremos que cualquiera que sea $n \in \mathbb{N}$ se tiene que $n \notin A$, de donde $A = \emptyset$; por lo que, si $A \subseteq \mathbb{N}$ es tal que $A \neq \emptyset$, entonces necesariamente tiene un primer elemento. Concluyendo que $\mathbb{N}$ está bien ordenado.

   Usaremos el método de inducción fuerte para demostrar que cualquiera que sea $n \in \mathbb{N}$ se tiene que $n \notin A$.

   Supongamos que $n \in \mathbb{N}$ y que para cada $k < n$ se tiene que $k \notin A$. En este caso, si $n \in A$ se sigue que n sería el primer elemento de A, lo que contradice el hecho de que A no tiene primer elemento, por lo tanto ha de ser $n \notin A$. En consecuencia $n \notin A$, cualquiera que sea $n \in \mathbb{N}$.

□

Ejercicios

1. Demostrar por inducción que $\sum_{i=1}^{n} 2^i = 2^{n+1} - 2$ cualquiera que sea $n \in \mathbb{N}$.

2. Demostrar por inducción que si $x \in \{x \in \mathbb{R} : 0 < |x| < 1\}$, cualquiera que sea $n \in \mathbb{N}$, $n > 1$, se verifica que $(1+x)^n \geq 1 + nx$.

3. Probar por inducción que si A es un conjunto con n elementos, entonces $\mathcal{P}(A)$ tiene 2^n elementos.

4. Demostrar que:

$$1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \ldots + \frac{1}{\sqrt{n}} > 2(\sqrt{n+1} - 1).$$

5. Demostrar, por inducción, que si $p | a_1 a_2 \ldots a_n$, siendo p primo y $a_i \in \mathbb{N}$, para cada $i \in \{1, \ldots, n\}$, entonces $p | a_i$, para algún $i \in \{1, \ldots, n\}$.

6. Sea el siguiente enunciado:

   Si en una ciudad hay un millonario, entonces todos los habitantes son millonarios.

   cuya *"demostración"* por inducción se acompaña:

   Procedemos por inducción sobre n, siendo éste el número de personas de un conjunto G_n, donde siempre habrá una millonaria.

   (a) Comprobamos el caso particular: sea G_1 el grupo formado por el "millonario conocido", luego se verifica trivialmente.

   (b) Hipótesis de inducción: supongamos el resultado válido para n personas. Veamos que también lo es para $n+1$.
   Sea G_{n+1} un grupo de $n+1$ personas en el que hay un millonario. Si prescindimos de una de las personas del grupo, que no sea el millonario, tendremos un grupo de n personas donde una es millonaria, por hipótesis de inducción todas son millonarias. De este último grupo sacamos a una persona (que ya sabemos que es millonaria) y reintegramos a la persona que se sacó en primer lugar; nuevamente tenemos un grupo de n personas en la que hay un millonario (realmente $n-1$), por tanto, por hipótesis de inducción nuevamente, tendremos que los n son millonarios. Luego las $n+1$ personas del grupo G_{n+1} son millonarias.

   (c) Concluimos por el principio de inducción completa que la afirmación inicial es cierta cualquiera que sea el número de personas en el que se encuentre el millonario identificado (esto demuestra la irreconciliable separación de las clases sociales).

¿Dónde está el error de la supuesta demostración?

7. Demostrar por inducción sobre $n \in \mathbb{N}$ que:
   (a) $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.
   (b) $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$.
   (c) $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$.
   (d) $1 + 6\sum_{i=0}^{n} 7^i = 7^{n+1}$.
   (e) $2^{n+2} + 3^{2n+1}$ es divisible por 7.

8. Demostrar por inducción la expresión del *binomio de Newton.*

9. ¿Es cierto que el cubo de un cierto número natural n está acotado superiormente por 3^n?

10. La sucesión de Fibonacci satisface la ecuación

$$a_0 = 0,\ a_1 = 1,\ a_{n+2} = a_n + a_{n+1}.$$

Probar por inducción que $a_{n+2} \geq \left(\frac{3}{2}\right)^n$, cualquiera que sea $n \in \mathbb{N}$, con $n \geq 0$.

11. Demostrar por inducción que $2^n \geq 3n^2 + 5$, para $n \geq 8$.

12. Los números armónicos H_k, con $k \in \mathbb{N}$, vienen definidos mediante:

$$H_k = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{k}.$$

Probar por inducción que $H_{2^n} \geq 1 + \frac{n}{2}$.

7.4 Principio de inducción transfinita

En general, para conjuntos bien ordenados podemos establecer un proceso de demostración parecido al *principio de inducción matemática.*

Definición 7.4.1 *Si $a \in A$ y A es un conjunto ordenado, mediante la relación $\preceq$, denominamos* **segmento inicial** *determinado por a y lo denotamos por $s(a)$, al conjunto:*

$$s(a) = \{x \in A :\ x \prec a\}.$$

Principio de inducción transfinita:
Sea A un conjunto bien ordenado y $S \subseteq A$ tal que para cada $a \in A$ verificando que $s(a) \subseteq S$, se deduce que $a \in S$. Entonces $S = A$.

Es decir, el principio de inducción transfinita afirma que: si A está bien ordenado y $S \subseteq A$ es tal que siempre que el conjunto de todos los predecesores estrictos de un elemento cualquiera de A está incluido en S implica que el propio elemento pertenece a S, entonces S debe contener a todo A.

Análogamente a la inducción matemática, se denomina *paso de inducción* al aserto: "si $a \in A$ verifica que $s(a) \subseteq S$, entonces $a \in S$" e *hipótesis de inducción* a la premisa.

La demostración del *principio de inducción transfinita* es la siguiente:

Demostración:
Si $S \neq A$, entonces $A \setminus S \neq \emptyset$ y $A \setminus S \subseteq A$, por lo que tendrá un primer elemento, sea éste

$$b \in A \setminus S. \tag{7.4}$$

Ahora bien, al ser b el primer elemento de $A \setminus S$ todos sus predecesores estrictos pertenecerán a S, por lo que $s(b) \subseteq S$, de donde, por verificarse la hipótesis de inducción, se tiene que

$$b \in S. \tag{7.5}$$

(7.4) y (7.5) se contradicen, por tanto $S = A$.

■

El principio de inducción transfinita difiere del de inducción matemática en dos cuestiones:

1. En el principio de inducción transfinita no hay ninguna suposición acerca de un elemento inicial, como el 0 en la inducción matemática.

   En este caso la diferencia es más lingüística que de fondo. En efecto, como A está bien ordenado ha de tener un primer elemento, sea éste a_0, entonces, obviamente, $s(a_0) = \emptyset$, por lo que $s(a_0) \subseteq S$. Para que pueda aplicarse el principio de inducción transfinita es necesario que $a_0 \in S$.

2. La hipótesis de inducción es diferente. En la inducción matemática se pasa a cada elemento a partir de su predecesor, mientras que en la inducción transfinita se pasa a cada elemento a partir del conjunto de todos sus predecesores, lo que guarda relación con la inducción fuerte, anteriormente vista.

   Esta diferencia es sustancial. En $\mathbb{N}$ cada elemento tiene un predecesor inmediato, pero en un conjunto bien ordenado cualquiera, ésto no tiene porqué ser así.

   Si aplicamos el principio de inducción transfinita a $\mathbb{N}$ el resultado es equivalente al principio de inducción matemática, de hecho estaríamos ante el principio de inducción fuerte. Pero si se aplica el principio de inducción

matemática a un conjunto bien ordenado arbitrario, no es equivalente a la inducción transfinita. Por tanto, la equivalencia de los dos principios en $\mathbb{N}$ es un caso especial.

Ejemplo 7.4.2 Sea $A = \mathbb{N}^+ = \mathbb{N} \cup \{\mathbb{N}\}$, con el siguiente orden, que denotaremos por $\preceq$: *"si $n, m \in A$ son naturales, entonces $n \preceq m$ si y sólo si $n \leq m$ y $n \prec \mathbb{N}$ para cada $n \in \mathbb{N}$".*

Claramente A está bien ordenado mediante $\preceq$. Ahora bien, si aplicamos las hipótesis del principio de inducción a A, tendremos que podemos encontrar conjuntos $S \subseteq A$ para los que aún verificándose que:

(a) $0 \in S$,

(b) Para cada $n \in S$, se tiene que $n + 1 \in S$,

no podemos asegurar que $S = A$. Así si $S = \mathbb{N}$, se verifican las hipótesis y sin embargo $\mathbb{N} \subsetneq A$, por lo que no es equivalente al principio de inducción transfinita. □

Podemos enunciar:

Proposición 7.4.3 *Sea A un conjunto bien ordenado mediante $\preceq$ y $P(a)$ una proposición que se enuncia cualquiera que sea $a \in A$ y tal que: para cada $a \in A$, si $P(x)$ es verdadera con $x \in A$ verificando que $x \prec a$, implica que $P(a)$ es verdadera. Entonces $P(x)$ es verdadera cualquiera que sea $x \in A$.*

Demostración. Basta poner $S = \{x \in A : P(x) \text{ es verdadera}\}$ y aplicar el principio de inducción transfinita.

■

Capítulo 8

Conjuntos infinitos

8.1 Generalización del producto cartesiano

En el capítulo 4 se definió el producto cartesiano de dos conjuntos, A y B, como el conjunto de los pares ordenados (a, b), con $a \in A$ y $b \in B$.

Es natural plantearse cómo generalizar este concepto a un número n cualquiera de conjuntos:

$$A_1 \times A_2 \times \ldots \times A_n,$$

e incluso si tiene sentido el producto cartesiano de una familia arbitraria de conjuntos.

Sea $\{x, y\}$ un par no ordenado tal que $x \neq y$. Una familia σ que tuviese por conjunto de índices a $\{x, y\}$ podríamos denotarla (ver sección 6.4) en la forma $\{\sigma_x, \sigma_y\}$. De todas las familias indexadas por $\{x, y\}$ podemos considerar aquellas que verifican que $\sigma_x = \sigma(x) \in A$ y $\sigma_y = \sigma(y) \in B$. Pues bien, al conjunto de todas estas familias lo vamos a representar por Φ; así pues, que $\varphi \in \Phi$, quiere decir que φ es una familia cuyo conjunto de índices es $\{x, y\}$ y tal que $\varphi(x) = \varphi_x \in A$ y $\varphi(y) = \varphi_y \in B$.

Definamos ahora una aplicación $f : \Phi \longrightarrow A \times B$, de la manera siguiente:

$$f(\varphi) = (\varphi_x, \varphi_y).$$

Desde luego f es una aplicación y además es biyectiva, ya que:

1. Es inyectiva, pues si $f(\varphi) = f(\sigma)$, entonces $(\varphi_x, \varphi_y) = (\sigma_x, \sigma_y)$, de donde

   $$\varphi_x = \sigma_x \qquad \text{y} \qquad \varphi_y = \sigma_y,$$

   por lo que $\varphi = \sigma$.

2. Es sobreyectiva, pues cualquiera que sea $(a, b) \in A \times B$ existe $\varphi \in \Phi$ tal que $\varphi_x = a$ y $\varphi_y = b$, por lo que $f(\varphi) = (a, b)$.

Permítasenos la licencia de decir que "en algún sentido" se pueden identificar Φ y $A \times B$, pues la diferencia entre uno y otro conjunto es una cuestión de notación.

Esta identificación es la que nos va a permitir generalizar el producto cartesiano de dos conjuntos.

Si $A_1, A_2, \ldots, A_n$ son conjuntos, el producto cartesiano de ellos es el conjunto de familias φ indexadas por $\{1, 2, \ldots, n\}$ y tales que $\varphi(i) = \varphi_i \in A_i$, para cada $i \in \{1, 2, \ldots, n\}$.

Análogamente podemos hablar de producto cartesiano de una familia arbitraria de conjuntos.

Definición 8.1.1 *Si $\{A_i\}_{i\in\mathcal{I}}$ es una familia indexada de conjuntos, llamamos producto cartesiano de la misma y lo denotamos por $X_{i\in\mathcal{I}}A_i$, al conjunto de todas las familias indexadas $\{x_i\}_{i\in\mathcal{I}}$ tales que $x_i \in A_i$, para cada $i \in \mathcal{I}$.*

Cuando los A_i son todos iguales al mismo conjunto A, el producto cartesiano es el conjunto de todas las aplicaciones de $\mathcal{I}$ en A, $A^{\mathcal{I}}$. Cuando $\mathcal{I} = \mathbb{N}$, éste es el conjunto de todas las sucesiones en A.

Las ternas ordenadas pueden definirse como familias cuyos conjuntos de índices son ternas no ordenadas. Análogamente para las cuaternas, etc.

8.2 Necesidad de un nuevo axioma

8.2.1 Haciendo infinitas elecciones sucesivas

A finales del siglo XIX, los matemáticos se dieron cuenta de que las operaciones con conjuntos, comúnmente admitidas, no resultaban suficientes para fundamentar razonamientos matemáticos del análisis.

Así, por ejemplo, consideremos la siguiente situación:

> *Sea $A \subseteq \mathbb{R}$ y $a \notin A$, tal que cualquier intervalo abierto de centro a contenga al menos un punto de A. Deseamos probar que existe una sucesión $(a_n)_{n\in\mathbb{N}}$ de puntos de A, cuyo límite es precisamente a.*
>
> Veámoslo:
>
> Sea $I_n = (a - \frac{1}{n}, a + \frac{1}{n})$ un intervalo abierto de centro a y radio $\frac{1}{n}$. Por hipótesis para $I_1 = (a - 1, a + 1)$ existe un punto $a_1 \in A \cap I_1$, para $I_2 = (a - \frac{1}{2}, a + \frac{1}{2})$ existe $a_2 \in A \cap I_2$, para I_3 existe $a_3 \in A \cap I_3$, y, en general, dado $n \in \mathbb{N}$ existe $a_n \in (a - \frac{1}{n}, a + \frac{1}{n})$. Formamos así una sucesión $(a_n)_{n\in\mathbb{N}}$, y veamos que $a_n \longrightarrow a$, cuando $n \longrightarrow \infty$. En efecto, cualquiera que sea $\varepsilon > 0$ existe un natural n_0 tal que $n_0\varepsilon > 1$, por lo que cualquiera que sea $n \geq n_0$ se tendrá que $\frac{1}{n} \leq \frac{1}{n_0} < \varepsilon$ y, además, $|a - a_n| < \frac{1}{n} < \varepsilon$. Por tanto $(a_n)_{n\in\mathbb{N}}$ es la sucesión buscada.

Examinemos qué es lo que hemos hecho. Hemos construido una sucesión $(A_n)_{n\in\mathbb{N}}$ de subconjuntos de A, de la forma $A_n = A \cap I_n$, que son no vacíos, y hemos "deducido" que existe una aplicación

$$\begin{array}{rccc} f: & \mathbb{N}\setminus\{0\} & \longrightarrow & A \\ & n & \longmapsto & f(n) = a_n \in A_n. \end{array}$$

Esto puede parecer absolutamente natural, pero hay un problema: para cada $n \in \mathbb{N}$ el elemento a_n no está determinado de manera única en A_n. Por tanto "hay que elegir" un a_n en A_n y ello para cada natural n; es decir, hay que hacer un número infinito de elecciones sucesivas.

Con este procedimiento estamos dando por buena la siguiente afirmación:

> *"Dada una colección no vacía de conjuntos no vacíos (en nuestro caso $\{A_i\}_{i\in\mathbb{N}}$), existe un conjunto (en el ejemplo $\{a_i\}_{i\in\mathbb{N}}$), que contiene un elemento de cada uno de los conjuntos de la colección",*

y que vamos a denominar provisionalmente (AE).

La controversia, a principios del siglo XX, fue mucha, tanta como los trabajos dedicados a probar que tal proceder era legítimo y que podía deducirse de los postulados de la teoría de conjuntos. En 1963 Paul J. Cohen demostró que el aserto (AE) era independiente de los axiomas de Zermelo–Fraenkel y, por tanto, que su legitimación no podía provenir de aquellos. Así, lo que parece un proceder natural no lo es tanto sin la ayuda de una nueva herramienta: formular un nuevo axioma que consista expresamente en la propiedad enunciada en (AE), y que denominaremos como *axioma de elección*.

8.2.2 El axioma de elección

Procederemos ahora a presentar otras formulaciones equivalentes del axioma de elección. Al contemplarlo desde varias perspectivas, esperamos que el lector adquiera una adecuada comprensión de su significado.

Sabemos que si A y B son dos conjuntos no vacíos, entonces $A \times B$ es no vacío y, recíprocamente, que si el producto cartesiano de A y B es no vacío, entonces tanto uno como otro son no vacíos.

Este hecho puede generalizarse, de forma que podemos afirmar que para n conjuntos $\{A_i\}_{1\leq i\leq n}$ *el producto cartesiano es no vacío si y sólo si cada uno de los conjuntos A_i no es vacío.* Puede demostrarse por inducción y se deja al lector como ejercicio.

Deseamos generalizar este resultado al caso de una familia arbitraria de conjuntos.

Si uno de los conjuntos de la familia es vacía, entonces el producto cartesiano es vacío, pero la otra implicación necesita de un nuevo axioma.

Axioma de elección:
El producto cartesiano de una familia no vacía de conjuntos no vacíos es no vacío.

Es decir, si $\{A_i\}_{i\in\mathcal{I}}$ es una familia de conjuntos no vacíos, cuyo conjunto de índices $\mathcal{I}$ es no vacío, entonces existe una familia $\{a_i\}_{i\in\mathcal{I}}$ tal que $a_i \in A_i$, para cada $i \in \mathcal{I}$.

Vamos a interpretar este axioma en términos de una colección $\mathcal{C}$ no vacía de conjuntos no vacíos.

Como sabemos, una tal colección se puede considerar como una familia donde tanto el conjunto indexado como el conjunto de índices es $\mathcal{C}$:

$$\begin{array}{rccc} i: & \mathcal{C} & \longrightarrow & \mathcal{C} \\ & X & \longmapsto & i(X) = X_X. \end{array}$$

El axioma de elección nos asegura entonces que el producto cartesiano de los elementos de $\mathcal{C}$ tiene al menos un elemento. Ahora bien, un elemento de tal producto cartesiano es, por definición, una aplicación f cuyo dominio es el conjunto de índices $\mathcal{C}$ y de forma que si $X \in \mathcal{C}$, entonces $f(X) \in X$.

Supongamos ahora que $\mathcal{C}$ es la colección de todos los subconjuntos no vacíos de un cierto conjunto A.

El axioma de elección nos asegura que:
Existe una aplicación f cuyo dominio es $\mathcal{P}(A)\backslash\{\emptyset\}$, tal que si $X \subseteq A$ y $X \neq \emptyset$, entonces $f(X) \in X$.

¿Qué es lo que hace la función f?, pues, para cada conjunto no vacío X, "elige" un elemento suyo $f(X) \in X$. De aquí el nombre del axioma y el de la función f, conocida como *función de elección.*

Cuando la colección de conjuntos es finita la "elección simultánea" de un elemento de cada subconjunto no vacío no tiene ningún problema y puede hacerse sin necesidad de introducir ningún axioma nuevo. Pero, lamentablemente, para casos infinitos es necesario introducir este nuevo axioma.

Existen diversas proposiciones que son **equivalentes** al axioma de elección. Entre ellas citaremos dos:

Lema de Zorn:
Si A es un conjunto ordenado, tal que cada cadena en A tiene una cota superior, entonces A tiene elemento máximo.

Principio del buen orden:
Cualquiera que sea un conjunto A, existe una relación de orden en él tal que A, con esta relación, está bien ordenado.

No entraremos en la demostración de estas equivalencias por apartarse por completo de nuestro propósito. No obstante, el lector interesado puede acudir a la bibliografía, donde encontrará excelentes libros que abordan esta cuestión.

8.3 Conjuntos equipotentes

En diversas ocasiones hemos utilizado la expresión "infinito" apelando a su significado intuitivo. Vimos que el axioma del infinito nos permite construir el conjunto de los naturales $\mathbb{N}$ y, en alguna medida, es lógico que tengamos una cierta identificación entre "el infinito" y el conjunto de los naturales.

En este capítulo queremos profundizar en el concepto del infinito matemático: ¿qué debemos entender por un conjunto infinito?, e incluso (informalmente hablando)"¿son todos los conjuntos infinitos del mismo tamaño?"

Empezamos precisando qué es un conjunto finito y qué es un conjunto infinito. Posteriormente nos preocuparemos de la "comparación" de conjuntos infinitos.

Si tenemos un conjunto arbitrario con cuatro elementos, podemos establecer una biyección entre él y el conjunto $\{1,2,3,4\}$. Análogamente para cualquier conjunto que tenga n elementos podemos establecer una biyección entre él y el conjunto $\{1,\ldots,n\}$ y, de esta manera, afirmamos que es posible establecer una biyección entre dos conjuntos cualesquiera que tengan n elementos cada uno.

Este procedimiento para "identificar" conjuntos por su "tamaño", sugiere la siguiente definición.

Definición 8.3.1 *Decimos que dos conjuntos, A y B, son equipotentes y lo denotamos por $A \sim B$, si se puede establecer entre ellos una biyección.*

Para subconjuntos de un conjunto U, la equipotencia es una relación de equivalencia en $\mathcal{P}(U)$. En efecto:

1. Es reflexiva, pues la identidad es una biyección.

2. Es simétrica, pues si $A \sim B$, entonces existe $f : A \longrightarrow B$ aplicación biyectiva, de donde $f^{-1} : B \longrightarrow A$ es también biyectiva y, consecuentemente, $B \sim A$.

3. Es transitiva, pues la composición de dos aplicaciones biyectivas es una aplicación biyectiva. Así si $f : A \longrightarrow B$ es la biyección que establece la equipotencia de A y B, y $g : B \longrightarrow C$ la correspondiente biyección entre B y C, tendremos que $g \circ f : A \longrightarrow C$ es también una biyección.

No deja de ser sorprendente que existan conjuntos que son equipotentes a subconjuntos propios de sí mismos, por ejemplo, si a cada número natural le

hacemos corresponder su doble obtenemos que $\mathbb{N}$ y el conjunto de los números pares son equipotentes. Afortunadamente cada número natural se comporta de manera más sensata. Recordemos, previamente, que un número natural n se construye como el conjunto $\{0, \ldots, n-1\}$.

Proposición 8.3.2 *Si $n \in \mathbb{N}$, entonces no existe subconjunto propio alguno de n que sea equipotente a n.*

Demostración. Veámoslo por inducción. Si $n = 0$, entonces se verifica de forma evidente la proposición.

Supongamos que es cierta para n; es decir, que si $A \subsetneq n$, entonces A no es equipotente a n.

Por el contrario supongamos que existe una biyección $f : n^+ \longrightarrow A \subsetneq n^+$. Si $n \notin A$ entonces la restricción $f|_n$ de f a n es una biyección entre n y un subconjunto propio de n, lo que contradice la hipótesis de inducción. Si $n \in A$, entonces n ha de ser equipotente a $A \setminus \{n\}$, de donde se tiene, en virtud de la hipótesis de inducción, que $n = A \setminus \{n\}$ y de aquí que $A = n^+$, contradiciendo que A es un subconjunto propio de n^+.

■

Esta diferencia justifica la siguiente definición:

Definición 8.3.3 *Un conjunto A se dice que es finito si es equipotente a algún número natural. En otro caso se dice que es infinito.*

Desde luego si A es finito entonces A es equipotente *a uno y sólo un* número natural, pues de lo contrario tendremos que existen dos números naturales distintos que son equipotentes, sean éstos m y n. Pero si $n \neq m$, entonces uno de ellos debe ser elemento y, consecuentemente, subconjunto propio del otro, resultando que tenemos un número natural que es equipotente a un subconjunto propio suyo, lo que contradice la proposición 8.3.2.

De lo anterior se deduce que un conjunto finito nunca es equipotente a un subconjunto propio suyo.

Como $\mathbb{N}$ es equipotente a algún subconjunto propio suyo (por ejemplo, los números pares), es claro que no puede ser finito, por lo que es infinito. Este es el ejemplo más sencillo de conjunto infinito.

Por otra parte, ya que todo subconjunto de un número natural es equipotente a un número natural (el lector debería detenerse en su demostración), se sigue que todo subconjunto de un conjunto finito es también finito.

Proposición 8.3.4 *Si un conjunto A es infinito, entonces tiene un subconjunto equipotente con $\mathbb{N}$.*

Demostración. Si A es infinito, en particular $A \neq \emptyset$, por lo que existe $a_0 \in A$. Por ser A infinito, no puede ser que A sea equipotente con 1 y de aquí que $A \setminus \{a_0\}$ no puede ser equipotente con 0, por lo que $A \setminus \{a_0\}$ es no vacío.

Sea $a_1 \in A \setminus \{a_0\}$. Al no ser A equipotente con 2 se sigue que $A \setminus \{a_0, a_1\}$ no puede ser vacío, por lo que existe $a_2 \in A \setminus \{a_0, a_1\}$. Repitiendo este procedimiento, podemos construir una sucesión $(a_n)_{n\in\mathbb{N}}$ tal que $a_i \in A$ para cada $i \in \mathbb{N}$ y $a_i \neq a_j$, cualesquiera que sean $i, j \in \mathbb{N}$ con $i \neq j$.

Ahora bien, es claro que $(a_n)_{n\in\mathbb{N}}$ es equipotente con $\mathbb{N}$, pues la aplicación

$$\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & (a_n)_{n\in\mathbb{N}} \subseteq A \\ & n & \longmapsto & f(n) = a_n \end{array}$$

es obviamente biyectiva.

■

Hemos de observar que en el razonamiento anterior está implícito el uso del axioma de elección. Una presentación formalizada de la demostración requeriría partir de una función de elección para A.

A continuación presentamos algunos resultados de interés.

Proposición 8.3.5 *Si A es equipotente con B y C es equipotente con D, entonces $A \times C$ es equipotente con $B \times D$.*

Demostración. Sean $f : A \longrightarrow B$ y $g : C \longrightarrow D$ biyectivas. Definimos ahora la aplicación $h : A \times C \longrightarrow B \times D$ tal que $h(a, c) = (f(a), g(c))$, donde $a \in A$ y $c \in C$. Veamos que es biyectiva.

Si $h(a, c) = h(a', c')$, entonces $f(a) = f(a')$ y $g(c) = g(c')$, de donde $a = a'$ y $c = c'$ y consecuentemente $(a, c) = (a', c')$. Concluimos que h es inyectiva.

Sea $(b, d) \in B \times D$. Por ser f y g sobreyectivas, existen $a \in A$ y $c \in C$ tales que $f(a) = b$ y $g(c) = d$, de donde $(b, d) = (f(a), g(c))$, y de aquí que existe (a, c) tal que $h(a, c) = (b, d)$, por lo que h es sobreyectiva.

■

Proposición 8.3.6 *Sean A equipotente con B y C equipotente con D, y tales que A y C son disjuntos, así como B y D, entonces $A \cup C$ es equipotente con $B \cup D$.*

Demostración. Sean las aplicaciones biyectivas $f : A \longrightarrow B$ y $g : C \longrightarrow D$, entonces la aplicación $h : A \cup C \longrightarrow B \cup D$, tal que $h(x) = f(x)$ si $x \in A$ y $h(x) = g(x)$ si $x \in C$, es biyectiva.

■

Ejercicios

1. Sean A y B dos conjuntos y B^A el conjunto de todas las aplicaciones de A en B. Si A, B y C son conjuntos cualesquiera, probar que $C^{A\times B}$ y $\left(C^B\right)^A$ son equipotentes.
2. Demostrar que si $A \sim B$ entonces $\mathcal{P}(A) \sim \mathcal{P}(B)$.
3. Demostrar que si $A\backslash B$ es equipotente con $B\backslash A$, entonces A es equipotente con B.

8.4 Cardinal de un conjunto

Definición 8.4.1 *Dado un conjunto finito A, el (único) número natural que es equipotente con A, se denomina el cardinal de A, lo denotaremos por $|A|$.*

Los números naturales son, así, el conjunto de cardinales de los conjuntos finitos.

La notación utilizada, $|A|$, se puede prestar a confusión, si se está denotando al conjunto con letras minúsculas ($|a|$). No obstante, según el contexto se pueden aclarar las posibles confusiones. También se utiliza para denotar el cardinal de A, $card(A)$.

Es claro que si dos conjuntos finitos son equipotentes, entonces tienen el mismo cardinal y recíprocamente, si tienen el mismo cardinal es que ambos son equipotentes al mismo número natural y, por tanto, son equipotentes entre sí. De esta manera el cardinal de A nos indica el "número de elementos de A".

A continuación, expondremos algunos resultados en relación con los cardinales infinitos, apelando a su significado intuitivo como generalización del concepto de número de elementos de un conjunto finito.

Hemos visto como el conjunto de los naturales y el de los pares son equipotentes. Más adelante veremos que es posible también establecer una biyección entre $\mathbb{N}$ y $\mathbb{Z}$ y entre $\mathbb{N}$ y $\mathbb{Q}$. Informalmente podríamos decir de todos estos conjuntos, que son equipotentes entre sí, tienen el mismo "número de elementos", puesto que cada elemento de uno de los conjuntos se puede poner en correspondencia con uno y sólo uno del otro conjunto y al revés.

Es decir, si dos conjuntos infinitos A y B son equipotentes, entre ellos hay una biyección f. Por cada elemento x de A hay uno y sólo uno en B, que es $f(a)$ y, al revés, por cada $b \in B$ hay un elemento y sólo uno $f^{-1}(b) = a$ en A. De esta manera, informal e intuitivamente hablando, podríamos decir que A y B "tienen el mismo número de elementos". También desde esta óptica, si dos conjuntos infinitos A y B "tienen el mismo número de elementos", se podrá establecer una biyección entre ellos, por lo que serán equipotentes.

Los conjuntos finitos equipotentes quedan caracterizados por un número, su cardinal. Con esta misma idea, queremos caracterizar los conjuntos infinitos que son equipotentes, aunque ahora no se trate de un número natural.

Diremos que dos conjuntos A y B (finitos o infinitos) son equipotentes si y sólo si tienen el mismo cardinal. El cardinal de A, lo denotaremos por $|A|$ o bien por $card(A)$. Así, $|A| = |B|$ si y sólo si $A \sim B$.

Si A y B son dos conjuntos tales que A es equipotente con algún subconjunto de B, entonces existe una aplicación $f : A \longrightarrow B$ que es inyectiva. A partir de aquí vamos a poder definir un orden en los cardinales (sean éstos finitos o infinitos).

Definición 8.4.2 *Dados dos conjuntos A y B, si existe una aplicación inyectiva de A en B, decimos que el cardinal de A es menor o igual que el cardinal de B y escribimos $|A| \leq |B|$.*

Cuando $|A| \leq |B|$ y $|A| \neq |B|$, decimos que el cardinal de A es estrictamente menor que el cardinal de B y escribimos $|A| < |B|$.

El conjunto de todos los pares ordenados (A, B) de subconjuntos de algún conjunto U para los que $|A| \leq |B|$, constituye una relación en $\mathcal{P}(U)$, conjunto potencia de U. Esta relación es de orden.

Desde luego $A \sim A$ y por tanto existe una aplicación inyectiva entre ellos, de donde $|A| \leq |A|$.

Si f es inyectiva de A en B, entonces es biyectiva de A en $f(A)$ y análogamente si g es inyectiva de B en C, entonces es biyectiva de B en $g(B)$. Por tanto $g|_{f(A)} \circ f$ es biyectiva entre A y $g(B)$, por lo que es inyectiva entre A y C, de donde $|A| \leq |C|$ si $|A| \leq |B|$ y $|B| \leq |C|$.

La verificación de la propiedad antisimétrica la garantiza el siguiente teorema.

Teorema 8.4.3 de Schröder–Bernstein *Si A y B son conjuntos tales que*

$$|A| \leq |B| \quad \text{y} \quad |B| \leq |A|,$$

entonces $|A| = |B|$.

Demostración. Podemos suponer que $A \cap B = \emptyset$. Si no fuese así, siempre podemos remitir a dos conjuntos disjuntos; si $A \cap B = C$, basta considerar $A \setminus C$ y $B \setminus C$, probarlo para ellos y a partir de aquí ya es inmediato.

Sean $f : A \longrightarrow B$ y $g : B \longrightarrow A$ inyectivas.

Para cada $a \in A$ se tiene que $f(a) \in B$, de donde $g(f(a)) \in A$, por lo que

$$f(g(f(a))) \in B, \ \ldots$$

Estos elementos, alternativamente de B y A, forman una sucesión infinita, para cada $a \in A$. Cada uno de los elementos de la sucesión es la imagen del elemento anterior por lo que vamos a decir que es un *descendiente* del mismo. Cada término de la sucesión es un descendiente de todos los que le preceden y también diremos que cada término de la sucesión es un *ancestro* de todos los que le siguen. Análogamente, para cada $b \in B$ tendremos una sucesión de descendientes:

$$g(b),\ f(g(b)),\ g(f(g(b))),\ \ldots$$

Para cada elemento, ya sea de A o de B, puede ocurrir una de estas tres cosas:

1. Que al buscar los ancestros del elemento tan anteriores a él como sea posible, suceda que lleguemos a un $a \in A$ que no tenga ancestro. Si esto ocurre es porque $a \in A \setminus g(B)$.
2. Que al buscar los ancestros del elemento tan anteriores a él como sea posible, suceda que lleguemos a un $b \in B$ que no tenga ancestro. Si ello ocurre es porque $b \in B \setminus f(A)$.
3. Que al buscar los ancestros del elemento tan anteriores a él como sea posible, suceda que el "*linaje*" se remonte al infinito.

Sea A_A el conjunto de aquellos elementos de A que se originan en A; es decir A_A se trata de la unión de $A \setminus g(B)$ con el conjunto formado por todos los descendientes en A de cada $a \in A \setminus g(B)$.

Sea A_B el conjunto de aquellos elementos de A que se originan en B; es decir A_B se trata del conjunto formado por todos los descendientes en A de cada $b \in B \setminus f(A)$.

Finalmente sea A_∞ el conjunto de aquellos elementos de A cuyo "linaje" se remonta al infinito. Análogamente podemos definir B_B, B_A y B_∞.

Si $a \in A_A$, entonces $f(a) \in B_A$ y la restricción $f|_{A_A} : A_A \longrightarrow B_A$ es biyectiva.

Si $a \in A_B$, entonces $a \in Dom\ g^{-1}$ y $g^{-1}(a) \in B_B$ y $g^{-1}|_{A_B} : A_B \longrightarrow B_B$ es biyectiva.

Si $a \in A_\infty$, entonces $f(a) \in B_\infty$ y $f|_{A_\infty} : A_\infty \longrightarrow B_\infty$. Sea ahora la aplicación $h : A \longrightarrow B$ tal que

$$h(a) = \begin{cases} f|_{A_A}(a) & \text{si } a \in A_A \\ g^{-1}|_{A_B}(a) & \text{si } a \in A_B \\ f|_{A_\infty}(a) & \text{si } a \in A_\infty, \end{cases}$$

que es biyectiva.

■

Veamos ahora que el recíproco de la proposición 8.3.4 también es cierto.

Proposición 8.4.4 *Si A es un conjunto que tiene un subconjunto equipotente con $\mathbb{N}$, entonces A es infinito.*

Demostración. En efecto, si A fuese finito tendríamos que existiría $n \in \mathbb{N}$ tal que $A \sim n$, de donde $|A| = n$, por lo que también $|A| \leq n$; por otra parte, por hipótesis, $|\mathbb{N}| \leq |A|$. Luego $|\mathbb{N}| \leq n$, pero $n \leq |\mathbb{N}|$. Del Teorema de Schröder–Berstein concluimos que $|\mathbb{N}| = n$ y, por tanto, que $\mathbb{N}$ es finito, lo que es absurdo.

■

Resulta ya inmediato que:

Corolario 8.4.5 *Un conjunto A es infinito si y sólo si algún subconjunto suyo es equipotente con $\mathbb{N}$.*

Proposición 8.4.6 *Un conjunto A es finito si y sólo si $|A| < |\mathbb{N}|$.*

Demostración. Si A es finito, entonces $A \sim n$, por lo que $|A| = n$. Como $n = \{0, \ldots, n-1\} \subsetneq \mathbb{N}$, se tiene que $n \leq |\mathbb{N}|$ y, por tanto, que $|A| \leq |\mathbb{N}|$. Ahora bien, claramente $|A| \neq |\mathbb{N}|$, pues siendo $\mathbb{N}$ infinito no es posible establecer una aplicación sobreyectiva de A en $\mathbb{N}$.

Recíprocamente, si $|A| < |\mathbb{N}|$ entonces A debe ser finito. De lo contrario existirá $B \subseteq A$ tal que $B \sim \mathbb{N}$, por lo que $|B| = |\mathbb{N}|$. Como $B \subseteq A$, resulta que $|B| \leq |A|$ y de esta forma tendremos que $|\mathbb{N}| \leq |A|$, pero por hipótesis $|A| < |\mathbb{N}|$. Concluimos que $|A| < |A|$, lo que es absurdo.

■

Ejercicios

1. Probar que el cardinal de un conjunto infinito no se altera si a éste le quitamos un número finito de elementos.
2. Si A y B son dos conjuntos finitos que tienen el mismo número de elementos y f es una aplicación de A en B. Demostrar que son equivalentes que:
   (a) f es inyectiva.
   (b) f es sobreyectiva.
   (c) f es biyectiva.
3. Sean A y B dos conjuntos finitos y disjuntos, tales que $A \sim m$ y $B \sim n$. Probar que $A \cup B \sim m + n$.
4. Sean A y B dos conjuntos finitos tales que $A \sim m$ y $B \sim n$. Probar que $A \times B \sim m \cdot n$.

8.5 El concepto de cardinal desde la perspectiva axiomática

Esta sección es más bien una digresión dentro del discurso general, ya que su contenido no afecta de forma fundamental al significado y uso de las secciones anteriores de este capítulo. Pretendemos exclusivamente informar al lector de los problemas que desde la perspectiva axiomática se nos plantearían en la introducción del concepto de cardinal.

Observemos que nuestra implícita definición de número cardinal nos remite a clases de equivalencia de conjuntos equipotentes, puesto que $|A| = |B|$ si y sólo si $A \sim B$. Es decir, todos los conjuntos que pertenecen a la misma clase de equipotencia tienen el mismo cardinal, pero no podemos demostrar (a partir de los axiomas hasta ahora conocidos) que existen las clases de equivalencia apropiadas. Por ello si quisiéramos ir más allá de un estudio intuitivo necesitaríamos en este momento introducir una nueva idea primitiva y un axioma especial para números cardinales.

Así, postulamos que con cada conjunto A está asociado un objeto $|A|$, el número cardinal de A, tal que a dos conjuntos equipotentes asociamos el mismo número cardinal. El nuevo axioma sería:

Axioma para cardinales: $|A| = |B|$ si y sólo si $A \sim B$.

Existen otras posibilidades para la introducción del concepto de cardinal.

Podríamos definir los números cardinales como cierto tipo de números ordinales. Esta definición requiere abordar el concepto de ordinal (que no entra dentro del propósito de este trabajo) y del axioma de elección para demostrar que todo conjunto tiene un número cardinal. Pero este procedimiento, en aras de la formalización, nos alejaría sustancialmente de nuestros objetivos. Otras posibilidades para la introducción de los cardinales no son menos costosas.

Sepa el lector simplemente que existen otros caminos, propios de un estudio de la *Teoría axiomática de conjuntos.* Aquél que desee ampliar horizontes sobre este tema (desde la opción señalada) encontrará en el libro de P. Suppes [18] un buen referente.

8.6 Conjuntos numerables

Definición 8.6.1 *Decimos que un conjunto A es numerable si es equipotente con $\mathbb{N}$ o con algún subconjunto suyo.*

Obsérvese que de la definición se deduce que A es numerable si es posible establecer una aplicación $f : A \longrightarrow \mathbb{N}$ inyectiva. También se deduce que si A

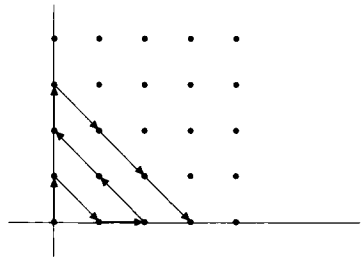


Figura 8.1: $\mathbb{N} \times \mathbb{N}$ es numerable

es numerable y $f : \mathbb{N} \longrightarrow A$ es la aplicación que determina la numerabilidad, necesariamente f ha de ser sobreyectiva.

Un conjunto numerable puede ser finito o infinito; en este último caso se dice que el conjunto es infinito numerable. Observemos que afirmar que A es numerable es tanto como decir que sus elementos se pueden disponer como una sucesión.

Veamos algunos conjuntos que son numerables.

Observando que es posible disponer los números enteros en la forma

$$\{0, 1, -1, 2, -2, 3, -3, \ldots\},$$

vemos que $\mathbb{Z}$ es numerable. Un procedimiento más formal es el siguiente.

Proposición 8.6.2 *$\mathbb{Z}$ es numerable.*

Demostración. La aplicación $f : \mathbb{N} \longrightarrow \mathbb{Z}$ tal que

$$f(n) = \begin{cases} 0 & \text{si} \quad n = 0 \\ \frac{n}{2} & \text{si} \quad n = \dot{2} \\ -\frac{n-1}{2} & \text{si} \quad n \neq \dot{2} \end{cases}$$

es claramente biyectiva.

■

Toda vez que, intuitiva e informalmente hablando, suele entenderse que dos conjuntos si son equipotentes "tienen el mismo número de elementos", el resultado precedente es ciertamente sorprendente.

Obsérvese la figura 8.1 y dispónganse los elementos de $\mathbb{N} \times \mathbb{N}$ como ella sugiere:

$$\{(0,0), (0,1), (1,0), (2,0), (1,1), (0,2), (0,3), (1,2), \ldots\}.$$

A la vista de ello podemos enunciar:

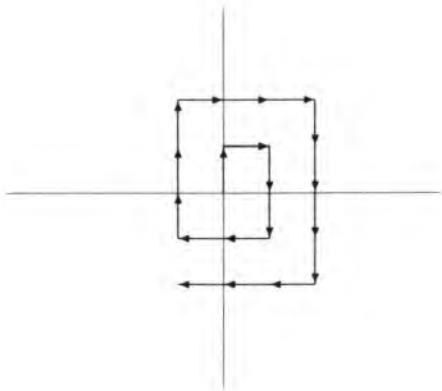


Figura 8.2: $\mathbb{Z} \times \mathbb{Z}$ es numerable

Proposición 8.6.3 $\mathbb{N} \times \mathbb{N}$ *es numerable.*

Si usted lector no es partidario de métodos tan heterodoxos, para justificar el "sorprendente" resultado que acabamos de enunciar, considere la aplicación biyectiva $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, dada por:

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

Pero aún más extraordinario resulta la próxima proposición, cuya justificación damos inmediatamente:

Consideremos la aplicación que se sugiere en la figura 8.2. Ella nos permite disponer los elementos de $\mathbb{Z} \times \mathbb{Z}$ como la sucesión

$$\{(0,0),(0,1),(1,1),(1,0),\ldots\}.$$

Proposición 8.6.4 $\mathbb{Z} \times \mathbb{Z}$ *es numerable.*

De hecho, el resultado anterior es un caso particular de este otro:

Proposición 8.6.5 *El producto cartesiano de dos conjuntos numerables es numerable.*

Demostración. Sean A y B numerables y $f : A \longrightarrow \mathbb{N}$ y $g : B \longrightarrow \mathbb{N}$ las inyecciones correspondientes. Consideremos la aplicación $h_1 : A \times B \longrightarrow \mathbb{N} \times \mathbb{N}$ dada por:

$$h_1(a,b) = (f(a), g(b)),$$

que claramente es inyectiva. Por otra parte, por la proposición 8.6.3, existe $h_2 : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ biyectiva. Concluimos que $h_2 \circ h_1 : A \times B \longrightarrow \mathbb{N}$ es inyectiva, por lo que $A \times B$ es numerable.

■

A continuación vamos a ver tres procedimientos distintos para probar la numerabilidad de $\mathbb{Q}$. Puede que el lector saque algún provecho adicional al ver que, comúnmente, hay diversas formas de llegar a un mismo resultado, así como de las diferentes técnicas utilizadas en cada caso.

Proposición 8.6.6 *$\mathbb{Q}$ es numerable.*

Demostración.

Primera forma:

Para una fracción irreducible $\frac{a}{b}$ vamos a llamar rango de la misma a $a + b$ y vamos a considerar que el rango de 0 es 0. Disponemos a continuación las fracciones por orden creciente de su rango, de manera que para aquellas que tienen el mismo rango, las ordenamos de menor a mayor, colocando tras cada fracción positiva, la misma con signo negativo, como indicamos a continuación:

$$\begin{array}{ll} \text{rango } 0: & 0 \\ \text{rango } 2: & \frac{1}{1}, -\frac{1}{1} \\ \text{rango } 3: & \frac{1}{2}, -\frac{1}{2}, \frac{2}{1}, -\frac{2}{1} \\ \quad \ldots & \quad \ldots \end{array}$$

Ello nos permite construir una biyección entre $\mathbb{N}$ y $\mathbb{Q}$.

Segunda forma:

También podíamos haber procedido a probar que los racionales positivos son numerables, teniendo en cuenta la siguiente indicación:

$$\begin{array}{ccccccccc} 1 & \rightarrow & \frac{1}{2} & & \frac{1}{3} & \rightarrow & \frac{1}{4} & \frac{1}{5} & \cdots \\ & \swarrow & & \nearrow & & \swarrow & & & \cdots \\ 2 & & \frac{2}{2} & & \frac{2}{3} & & \frac{2}{4} & \frac{2}{5} & \cdots \\ \downarrow & \nearrow & & \swarrow & & & & & \cdots \\ 3 & & \frac{3}{2} & & \frac{3}{3} & & \frac{3}{4} & \frac{3}{5} & \cdots \\ \\ \vdots & & \vdots & & \vdots & & \vdots & \vdots & \end{array}$$

Es claro que también será numerable los racionales negativos y, por tanto, la unión de ambos unión $\{0\}$ también será numerable (como en breve se precisará).

Tercera forma:

Consideremos ahora los números naturales escritos en base 11, donde los dígitos son: $0, 1, \ldots, /$. Si a cada fracción $\frac{a}{b}$ le hacemos corresponder el natural a/b,

tendremos una aplicación inyectiva de $\mathbb{Q}$ en $\mathbb{N}$ y que no es sobreyectiva (¿por qué?).

■

Un resultado de interés es el que hace referencia a la unión numerable de conjuntos numerables. Entre otras cosas puede servirnos para demostrar la numerabilidad de $\mathbb{Q}$, mediante otro procedimiento distinto a los anteriores (ver ejercicios).

Lema 8.6.7 *Existe una familia $\{A_n\}_{n\in\mathbb{N}}$ numerable de subconjuntos infinitos de $\mathbb{N}$, disjuntos dos a dos y cuya unión es $\mathbb{N}$.*

Demostración. Contémplese la disposición de los números naturales que se indica a continuación:

$$\begin{array}{cccccc} 0 & 1 & 3 & 6 & 10 & 15 & \ldots \\ 2 & 4 & 7 & 11 & 16 & \ldots & \\ 5 & 8 & 12 & 17 & \ldots & & \\ 9 & 13 & 18 & \ldots & & & \\ 14 & 19 & \ldots & & & & \\ 20 & \ldots & & & & & \end{array}$$

donde la distribución de los números naturales se hace siguiendo diagonales. Así, el primer número es el 0, luego la primera diagonal: $1, 2$, después la segunda diagonal $3, 4, 5$, a continuación la tercera diagonal $6, 7, 8, 9$, y así sucesivamente: $10, 11, 12, 13, 14$, etc. La diagonal primera se compone de dos números (el 1 y el 2), la diagonal k–ésima se compone de $k + 1$ números.

Al considerar las filas de la distribución anterior, es claro que:

1. Cada una de ellas constituye un subconjunto infinito de $\mathbb{N}$.
2. Son disjuntas entre sí.
3. La unión de todas ellas es $\mathbb{N}$.

■

Proposición 8.6.8 *La unión numerable de conjuntos infinitos numerables es numerable.*

Demostración. Sea $\{X_n\}_{n\in\mathbb{N}}$ la familia en cuestión. Para cada $n \in \mathbb{N}$, como X_n es infinito numerable y el conjunto A_n del lema anterior también lo es, se tiene que ambos son equipotentes y, por tanto, que existe una biyección $f_n : A_n \longrightarrow X_n$.

Sea la aplicación $f : \mathbb{N} \longrightarrow \bigcup_{n\in\mathbb{N}} X_n$ tal que $f(i) = f_n(i)$, si $i \in A_n$.

Si $x \in \bigcup_{n\in\mathbb{N}} X_n$, entonces $x \in X_n$ para algún $n \in \mathbb{N}$, por lo que existe $i \in A_n$ tal que $f_n(i) = x \in X_n$, al ser f_n biyectiva. Como $f(i) = f_n(i)$, se concluye que f es sobreyectiva y, en consecuencia, que $\bigcup_{n\in\mathbb{N}} X_n$ es numerable.

■

Es obvio que el resultado anterior sigue siendo válido si no todos los conjuntos de la familia $\{X_n\}_{n\in\mathbb{N}}$ son infinitos. Del mismo modo, si la familia no es infinita el resultado sigue siendo válido, en particular: la unión de dos conjuntos numerables es numerable.

Ejercicios

1. Demostrar, haciendo uso de la numerabilidad de la unión numerable de conjuntos numerables, que $\mathbb{Q}$ es numerable.
2. Sea $Z[x]$ el conjunto de todos los polinomios con coeficientes enteros. Probar que $Z[x]$ es numerable.
3. Se dice que un número es algebraico si es solución de alguna ecuación algebraica con coeficientes enteros:

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

siendo $n \in \mathbb{N}$ y $a_i \in \mathbb{Z}$ para cada $i \in \{0, \ldots, n\}$. Demostrar que el conjunto de los números algebraicos es numerable.

8.7 Conjuntos no numerables

De lo visto hasta ahora podríamos erróneamente sospechar que cualquier conjunto infinito es numerable. El próximo resultado evidencia que nada más lejos de la realidad.

Teorema 8.7.1 (de Cantor) *Cualquiera que sea el conjunto A se tiene que*

$$|A| < |\mathcal{P}(A)|.$$

Demostración. Sea la aplicación $f : A \longrightarrow \mathcal{P}(A)$ tal que para cada $a \in A$, $f(a) = \{a\}$ que es claramente inyectiva, pues si $f(a) = f(b)$, entonces $\{a\} = \{b\}$, de donde $a = b$. Por tanto $|A| \leq |\mathcal{P}(A)|$.

Además, $|A| \neq |\mathcal{P}(A)|$, de lo contrario existirá $g : A \longrightarrow \mathcal{P}(A)$ biyectiva. Como $g(a) \subseteq A$, tiene sentido considerar $B = \{a \in A : a \notin g(a)\} \subseteq A$. Al ser g sobreyectiva, para B existirá $b \in A$ tal que $g(b) = B$.

Ahora bien, puede ocurrir que $b \in B$ o que $b \notin B$. Si $b \in B$, por la definición de B se tiene que $b \notin g(b) = B$ y si $b \notin B$ se concluye que $b \in g(b) = B$. En cualquier caso llegamos a contradicción.

Concluimos que efectivamente $|A| \neq |\mathcal{P}(A)|$.

■

Si $A = \mathbb{N}$, el Teorema de Cantor nos dice que existen conjuntos con cardinal mayor al de $\mathbb{N}$, es decir conjuntos *no numerables*. Y además que los cardinales de conjuntos infinitos constituyen una sucesión "creciente" ilimitada: por grande que sea $|A|$, existe otro conjunto $\mathcal{P}(A)$ con cardinal estrictamente superior. A los cardinales de los conjuntos infinitos se les denominan *números transfinitos*; por tanto, existe una infinidad de números transfinitos mayores que $|\mathbb{N}|$.

Definición 8.7.2 *Un conjunto A se dice que es no numerable si su cardinal es estrictamente mayor que el de $\mathbb{N}$; es decir, si $|\mathbb{N}| < |A|$.*

Un caso de conjunto no numerable es el intervalo $(0, 1)$.

Proposición 8.7.3 *El intervalo abierto $(0, 1)$ es un conjunto no numerable.*

Demostración. Consideremos la expresión decimal de los elementos de $(0, 1)$. Supongamos que $(0, 1)$ es numerable, en ese caso podemos disponer sus elementos en una sucesión, en la forma $a_1, a_2, a_3, \ldots, a_n, \ldots$ cuyas expresiones decimales son:

$$\begin{aligned} &0.a_{11}a_{12}a_{13}a_{14}\ldots \\ &0.a_{21}a_{22}a_{23}a_{24}\ldots \\ &0.a_{31}a_{32}a_{33}a_{34}\ldots \\ &\ldots\ldots\ldots \end{aligned}$$

Sea ahora el número $b = 0.b_1b_2b_3b_4\ldots$, tal que $b_i \neq a_{ii}$ para cada $i \in \mathbb{Z}^+$. Es claro que b no puede estar en la sucesión anterior, toda vez que se diferencia de cada uno de los números en al menos una cifra, precisamente a_{ii}. Por otra parte es obvio que $b \in (0, 1)$, consecuentemente se obtiene la conclusión deseada.

■

El siguiente resultado es "sorprendente", pues nos pone de manifiesto, informalmente hablando, que "hay tantos puntos en un cubo como en cualquiera de sus lados".

Proposición 8.7.4 *El conjunto de puntos del interior de un cubo de arista 1 es equipotente con $(0, 1)$:*

$$(0, 1) \times (0, 1) \times (0, 1) \sim (0, 1).$$

Demostración. Si consideramos el cubo sobre un sistema de referencia cartesiano, como se indica en la figura 8.3, a cada punto del cubo le corresponde tres

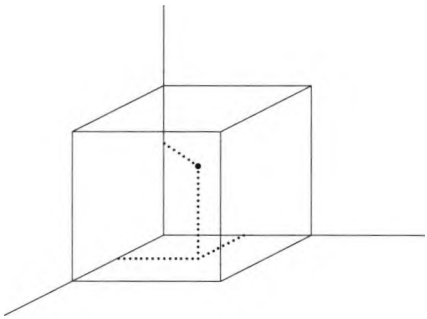


Figura 8.3: Cardinal del interior de un cubo

coordenadas que serán tres números decimales comprendidos entre 0 y 1. Por tanto, para cada punto P del cubo, sus coordenadas (x, y, z) son de la forma:

$$x = 0.a_1a_2a_3a_4\ldots$$
$$y = 0.b_1b_2b_3b_4\ldots$$
$$z = 0.c_1c_2c_3c_4\ldots$$

A este punto le corresponde de forma inequívoca el número decimal comprendido entre 0 y 1: $d = 0.a_1b_1c_1a_2b_2c_2a_3b_3c_3a_4b_4c_4\ldots$ Hemos establecido una biyección entre $(0,1)\times(0,1)\times(0,1)$ y $(0,1)$, por lo que ambos son equipotentes.

■

Ahora el lector no tendrá dificultad en probar un caso más sencillo:

$$|(0,1)| = |(0,1)\times(0,1)|.$$

Proposición 8.7.5 *El conjunto $\mathbb{R}$ de los números reales no es numerable.*

Demostración. Es evidente, pues $(0,1)\subseteq\mathbb{R}$.

■

Proposición 8.7.6 *El conjunto $\mathbb{R}$ de los números reales es equipotente con el intervalo $(0,1)$.*

Demostración. Consideremos las siguientes aplicaciones:

$$\begin{array}{rccl} f: & (0,1) & \longrightarrow & (-1,1) \\ & x & \longmapsto & f(x) = -1+2x \end{array}$$

$$\begin{array}{rccl} & & & y \\ g: & (-1,1) & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & g(x) = \begin{cases} \frac{-x}{1+x} & \text{si} \quad x\in(-1,0] \\ \frac{x}{x-1} & \text{si} \quad x\in(0,1). \end{cases} \end{array}$$

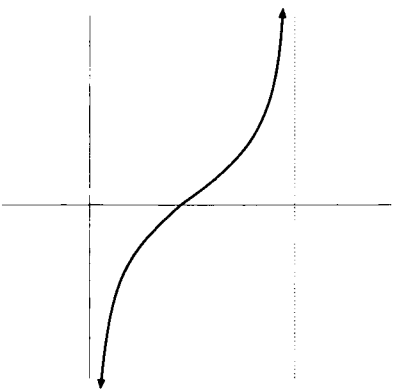


Figura 8.4: Biyección $g \circ f : (0,1) \longrightarrow \mathbb{R}$

que son biyectivas. Por tanto,

$$\begin{array}{rccl} g \circ f: & (0,1) & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & g \circ f(x) = \begin{cases} \frac{1-2x}{2x} & \text{si} \quad x \in (0, \frac{1}{2}] \\ \frac{-1+2x}{2x-2} & \text{si} \quad x \in (\frac{1}{2}, 1) \end{cases} \end{array}$$

es también biyectiva y consecuentemente $(0,1) \sim \mathbb{R}$.

■

Un razonamiento intuitivo para probar la proposición anterior es:

> El conjunto de todos los números reales x verificando que $0 < x < 1$, se pueden poner en biyección con los puntos de un segmento rectilíneo AB de longitud 1, excluyendo los extremos A y B. El conjunto de todos los números reales se pueden poner en biyección con los puntos de una recta.
>
> Si doblamos el segmento AB por la mitad, en ángulo recto, como se indica en la figura 8.5, y consideramos una proyección central de centro z, queda establecida una biyección entre el segmento AB y la recta. Consecuentemente $\mathbb{R}$ es equipotente con $(0,1)$.

Es obvio, a partir de las tres últimas proposiciones y de la proposición 8.3.5 que $|\mathbb{R}| = |(0,1)| = |(0,1) \times (0,1)| = |(0,1) \times (0,1) \times (0,1)| = |\mathbb{R}^2| = |\mathbb{R}^3|$.

De forma general, se tendrá que, para cada $n \in \mathbb{N}$, $|\mathbb{R}| = |\mathbb{R}^n|$ y por tanto que aún siendo $n \neq m$, se tiene que $|\mathbb{R}^n| = |\mathbb{R}^m|$.

Desde la época de la Grecia clásica se entendían como profundamente diferentes objetos matemáticos de 1, de 2 o de 3 dimensiones, así que resultados como los anteriores parecían atentar contra las más firmes convicciones

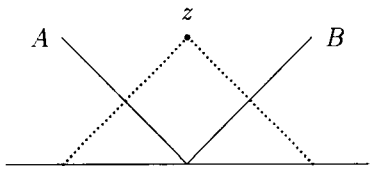


Figura 8.5: $\mathbb{R}$ es equipotente con $(0,1)$

geométricas. Dedekind observó que tales hechos no entraban en contradicción con los conceptos de la matemática clásica. La noción de dimensión hace intervenir no sólo la cardinalidad de $\mathbb{R}^n$, sino también su *topología*, pero este es un tema de considerable envergadura que requiere un tratamiento independiente, alejado por completo de nuestros objetivos. Para el lector con curiosidad y para aquél que haya entrado en contacto con conceptos de la topología, hemos de hacer observar que las biyecciones que hemos establecido entre $\mathbb{R}$ y $\mathbb{R}^n$ o entre $\mathbb{R}^n$ y $\mathbb{R}^m$ no son continuas. El propio Dedekind conjeturó y Brouwer (1881–1966) demostró en 1911, que no existe biyección alguna f entre $\mathbb{R}^n$ y $\mathbb{R}^m$, con $n \neq m$, que sea bicontinua (continua f y f^{-1}); es decir, si $n \neq m$ los espacios no pueden ser *homeomorfos*.

Abusando del tratamiento informal hemos venido diciendo cosas como que "tal conjunto tiene tantos elementos como tal otro". Así "un cubo y su arista" o "$\mathbb{Q}$ y $\mathbb{N}$". Esta forma de hablar busca, la sorpresa del lector abusando de la incorrecta intuición que se supone que tiene del infinito. Conviene hacer algunas precisiones.

"¿Quién tiene más elementos: $\mathbb{Q}$ o $\mathbb{N}$?". Puesto que $\mathbb{N} \subsetneq \mathbb{Q}$, la respuesta obviamente es que hay más racionales que números naturales. Pero si consideramos los números naturales escritos en base 11, donde los dígitos son $0, 1, \ldots, 9, /$ y a cada fracción $\frac{a}{b}$ le hacemos corresponder el número natural, en base 11, a/b, es claro que hay más naturales que racionales. Esta "paradójica" situación nos indica que es incorrecto hablar, para dos conjuntos infinitos, de "cuál de ellos es más grande". Sólo tiene sentido comparar sus tamaños mediante su cardinal y debemos hablar de si ambos tienen el mismo cardinal o uno de ellos tiene cardinal mayor que el otro.

Ejercicios

1. Probar que cualquier intervalo abierto (a, b) de la recta real es equipotente con $\mathbb{R}$.

2. Demostrar que el intervalo cerrado $[0, 1]$ de $\mathbb{R}$ no es numerable.

3. Estudiar la numerabilidad del conjunto $A = (0,1) \setminus S$, siendo $(0,1)$ un intervalo abierto de $\mathbb{R}$ y $S = \{\frac{1}{n} : n \in \mathbb{N} \text{ y } n \geq 2\}$.

4. Demostrar que el conjunto $10^{\mathbb{N}}$, de todas las aplicaciones definidas en $\mathbb{N}$ y con valores en $10 = \{0, 1, 2, \ldots, 9\}$, es equipotente con $\mathbb{R}$.

5. Demostrar que el conjunto $\mathcal{P}_F(\mathbb{N})$ de todos los subconjuntos finitos de $\mathbb{N}$ es numerable y que $\mathcal{P}(\mathbb{N}) \setminus \mathcal{P}_F(\mathbb{N}) \sim \mathbb{R}$.

6. Probar que el conjunto de todas las aplicaciones de $\mathbb{N}$ en $\mathbb{N}$ no es numerable.

7. Demostrar que cualquiera que sea el conjunto A, existe algún subconjunto B, de A, tal que $B \notin A$.

8. Demostrar que el conjunto de los números irracionales no es numerable.

9. Un número real que no es algebraico se dice que es trascendente (por ejemplo π o la base de los logaritmos neperianos e). Demostrar que el conjunto de los números trascendentes es equipotente con $\mathbb{R}$.

8.8 Aritmética cardinal

Se pueden definir operaciones entre los *cardinales de conjuntos infinitos*, por analogía con la aritmética usual, pero que presentan diferencias notables respecto de ésta.

En las líneas siguientes se presenta muy someramente en qué consisten estas operaciones, sin entrar en el estudio de las mismas. Nuestra intención es fundamentalmente tener una referencia del significado de la potencia $2^{|A|}$, donde A es un conjunto.

Si A y B son conjuntos (finitos o infinitos) con cardinales respectivos $|A| = m$ y $|B| = n$ y tales que $A \cap B = \emptyset$, se define la suma de ambos $m + n$ como el cardinal de la unión: $m + n = |A \cup B|$. Si los conjuntos no fueran disjuntos se sustituyen por otros equipotentes $A' \sim A$ y $B' \sim B$ tales que $A' \cap B' = \emptyset$ y entonces la suma es $m + n = |A' \cup B'|$.

La suma es conmutativa y asociativa, sin embargo si m es infinito se verifica que $m + m = m$ (piénsese en $|\mathbb{R}| + |\mathbb{R}| = |(0,1)| + |[1,2)| = |(0,1)| = |\mathbb{R}|$).

Se define el producto $m \cdot n$ como el cardinal del producto cartesiano, es decir: $m \cdot n = |A \times B|$. El producto es conmutativo, asociativo y distributivo respecto de la suma. Si embargo, si m es infinito se verifica que $m \cdot m = m$ (piénsese, por ejemplo, en $|\mathbb{R}| \cdot |\mathbb{R}| = |(0,1)| \cdot |(0,1)| = |(0,1) \times (0,1)| = |\mathbb{R}|$).

Se define la potencia de base m y exponente n como el cardinal del conjunto A^B de todas las aplicaciones de B en A; es decir $m^n = |A^B|$. En particular $|2^A| = 2^{|A|}$, donde $2 = \{0, 1\}$.

Ejercicios

1. Demostrar que si $|A| = a$ y $|B| = b$ son finitos, entonces:

$$|A \cup B| + |A \cap B| = a + b.$$

2. Aplicando el ejercicio anterior demostrar que para tres conjuntos finitos cualesquiera A, B y C, se tiene que:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

3. Se tiene un conjunto con n elementos y tres subconjuntos suyos A, B y C tales que hay una tercera parte de elementos que pertenecen a cada uno de los conjuntos A, B y C, además la quinta parte del total pertenece a cada par de ellos y la décima parte a los tres. Determinar el número de elementos que no pertenecen a ninguno de los conjuntos A, B y C.

4. En Matemáticas hay matriculados 160 alumnos, de los cuales 130 se han matriculado en Análisis I, 118 en Topología y 110 en Álgebra. Se sabe también que en Análisis I y Topología hay 105, en Topología y Álgebra 98 y en Análisis y Álgebra 102. ¿Cuántos alumnos hay matriculados a la vez en Análisis I, Topología y Álgebra?

5. Una agencia de publicidad busca 29 modelos: 13 con los ojos azules, 13 morenos y 15 que sean mayores de 25 años. Además 6 tienen que ser morenos con los ojos azules, 4 morenos y mayores de 25 años y 5 con los ojos azules y mayores de 25 años. Determinar:

   (a) ¿Cuántos tienen que ser las tres cosas a la vez?

   (b) ¿A cuántas personas que sólo tengan los ojos azules se necesitan?

   (c) ¿Cuántas personas se necesitan que sean mayores de 25 años y con los ojos azules pero que no sean morenos?

6. En el conjunto de los números enteros positivos menores que 1000 determinar cuántos no son múltiplos ni de 3, ni de 5 ni de 7.

7. En una encuesta realizada a 1000 personas, sobre la audiencia de los informativos, se obtuvieron los siguientes datos: 420 veían TV1, 450 Antena 3, 400 Tele 5, 130 TV1 y Tele 5, 200 TV1 y Antena 3, 180 Antena 3 y Tele 5, 70 los tres. Determinar:

(a) ¿Cuántas personas no ven ningún informativo?

(b) ¿Cuántas personas ven únicamente los informativos de Tele 5?

(c) ¿Cuántas personas ven exclusivamente los informativos de una única cadena?

8. Demostrar que si a y b son cardinales tales que $a + b = a + a$, entonces $a \geq b$.

8.9 El cardinal de $\mathbb{R}$

El Teorema de Cantor nos indica que el cardinal de un conjunto es estrictamente menor que el cardinal del conjunto de sus partes. Pero, ¿cuál es el cardinal del conjunto potencia de un conjunto infinito? Para el caso finito vimos que si el cardinal de A es $|A| = n$ entonces $|\mathcal{P}(A)| = 2^n$, ahora probaremos que este resultado es generalizable para conjuntos infinitos.

Proposición 8.9.1 *Cualquiera que sea el conjunto A se verifica que*

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

Demostración. Basta probar que $\mathcal{P}(A) \sim 2^A$, donde 2^A es el conjunto de todas las aplicaciones $f : A \longrightarrow 2 = \{0, 1\}$.

Sea la aplicación $g : \mathcal{P}(A) \longrightarrow 2^A$ tal que a cada subconjunto B de A le hace corresponder su función característica χ_B, donde como sabemos

$$\chi_B : A \longrightarrow 2 = \{0, 1\},$$

es tal que:

$$\chi_B(x) = \begin{cases} 1 & \text{si} \quad x \in B \\ 0 & \text{si} \quad x \notin B \end{cases}$$

Es fácil comprobar que g es biyectiva, obteniendo la conclusión deseada.

■

Ya sabemos que $\mathbb{R}$ no es numerable. Veamos seguidamente que su cardinal es $2^{|\mathbb{N}|}$. Las demostraciones de este hecho usualmente necesitan de algunos conceptos del análisis y particularmente del uso de series. Puesto que estas páginas van dirigidas a un lector que aún no se ha familiarizado con aquellas, abordaremos el tema desde otra perspectiva y necesitaremos previamente del siguiente:

Lema 8.9.2 *Si a y b son números reales tales que $a < b$, entonces existe un número racional r tal que $a < r < b$.*

Demostración. Sea $n \in \mathbb{N}$ tal que $n > \frac{1}{b-a}$, por lo que

$$\frac{1}{n} < b - a. \tag{8.1}$$

Consideremos dos enteros positivos p y q tales que $p < a < q$.

Observemos que $q = p + \frac{n(q-p)}{n} > a$. Sea el conjunto $J = \{i \in \mathbb{N} : p + \frac{i}{n} > a\}$. J es no vacío ya que, al menos, $n(q-p) \in J$. Como $J \subseteq \mathbb{N}$ y $\mathbb{N}$ está bien ordenado mediante la relación $\leq$, se tiene que existe $j \in J$ primer elemento.

Ahora bien, $j > 0$, pues $p + \frac{0}{n} = p < a$, de donde $0 \notin J$. Por lo tanto $j - 1 \in \mathbb{N}$ y $j - 1 \notin J$, luego

$$p + \frac{j-1}{n} \leq a. \tag{8.2}$$

Sea $r = p + \frac{j}{n}$. Desde luego r es racional y puesto que $j \in J$ se sigue que

$$r > a. \tag{8.3}$$

Por otra parte, de (8.2) y (8.1) se tiene que

$$r = p + \frac{j}{n} = p + \frac{j-1}{n} + \frac{1}{n} < a + (b - a) = b. \tag{8.4}$$

Por (8.3) y (8.4) llegamos a la conclusión deseada. ∎

Proposición 8.9.3 *Se verifica que* $|\mathbb{R}| = 2^{|\mathbb{N}|}$.

Demostración. Veamos en primer lugar que $|\mathcal{P}(\mathbb{N})| \leq |\mathbb{R}|$.

Vamos a hacerle corresponde a cada subconjunto A de $\mathbb{N}$ un número real comprendido entre 0 y 1, de forma que el primer decimal sea 7 si $1 \in A$ o bien 3 si $1 \notin A$, de la misma forma el segundo decimal será 7 si $2 \in A$ o bien 3 si $2 \notin A$, y así sucesivamente si el n–ésimo decimal es d_n, entonces

$$d_n = \begin{cases} 7 & si \quad n \in A \\ 3 & si \quad n \notin A. \end{cases} \tag{8.5}$$

De esta forma podemos construir una aplicación[1]

$$\begin{array}{rccl} g: & \mathcal{P}(\mathbb{N}) & \longrightarrow & \mathbb{R} \\ & A & \longmapsto & g(A) = 0.d_1 d_2 d_3 \ldots \end{array}$$

tal que d_n viene dado por (8.5), para cada $n \in \mathbb{N}$.

[1] Por ejemplo, si A es el conjunto de los números impares, tendremos que $g(A) = 0.73737373\ldots$.

Desde luego g es inyectiva pues si $A \neq B$, entonces existirá al menos un natural n que pertenecerá a uno de los conjuntos pero no al otro, pero entonces para ese n la expresión del decimal d_n de $g(A)$ y de $g(B)$ será distinta, pues en un caso deberá ser 3 y en el otro 7. Por tanto, $g(A) \neq g(B)$, resultando que g es inyectiva y de aquí que

$$|\mathcal{P}(\mathbb{N})| \leq |\mathbb{R}|. \tag{8.6}$$

Veamos ahora la otra desigualdad. Sea $f : \mathbb{R} \longrightarrow \mathcal{P}(\mathbb{Q})$ tal que para cada $x \in \mathbb{R}$ es $f(x) = \{r \in \mathbb{Q} : r < x\}$. Veamos que f es inyectiva. En efecto, si $x \neq y$ son dos números reales, entonces ha de ocurrir que $x < y$ o bien que $y < x$.

Si $x < y$, por el lema 8.9.2 existe un racional r tal que $x < r < y$. Tenemos entonces que $r \in f(y)$ y que $r \notin f(x)$, por lo que $f(x) \neq f(y)$. Análogamente se puede probar que $f(x) \neq f(y)$ si $y < x$. De esta forma concluimos que f es inyectiva y que $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})|$.

Como $\mathbb{N} \sim \mathbb{Q}$ se sigue que $\mathcal{P}(\mathbb{N}) \sim \mathcal{P}(\mathbb{Q})$ (ver ejercicio 3 de la sección 8.3) y por tanto $|\mathcal{P}(\mathbb{N})| = |\mathcal{P}(\mathbb{Q})|$. Obtenemos finalmente que

$$|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})| = |\mathcal{P}(\mathbb{N})|. \tag{8.7}$$

Aplicando el Teorema de Schöreder–Bernstein a (8.6) y (8.7) obtenemos que

$$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$$

y, en virtud de la proposición 8.9.1, finalmente que $|\mathbb{R}| = |2^{\mathbb{N}}| = 2^{|\mathbb{N}|}$.

■

Hemos visto que existe una infinidad de cardinales transfinitos distintos. Al cardinal de $\mathbb{N}$ y por extensión de los conjuntos infinitos numerables se le denomina "álef cero" y se denota por $\aleph_0$; es decir $\aleph_0 = |\mathbb{N}|$. El cardinal de los conjuntos equipotentes con $\mathbb{R}$ es $|\mathbb{R}| = 2^{\aleph_0}$. El sucesor inmediato de $\aleph_0$ en el ordenamiento de los números cardinales se denota por $\aleph_1$ y se lee "álef uno".

Todo lo que sabemos hasta ahora es que $\aleph_o = |\mathbb{N}| < \aleph_1 \leq 2^{\aleph_0} = |\mathbb{R}|$. La relación entre $\aleph_0$ y $\aleph_1$ fue el objeto de un famoso problema acerca de los números cardinales: ¿es estricta la desigualdad entre $\aleph_1$ y $2^{\aleph_0}$? o por el contrario ¿existe un número cardinal transfinito estrictamente comprendido entre $\aleph_1$ y $2^{\aleph_0}$? Cantor conjeturó que no; es decir, que $\aleph_1 = 2^{\aleph_0}$. Esta suposición (entre $|\mathbb{N}|$ y $|\mathbb{R}|$ no hay ningún otro cardinal) se conoce como *Hipótesis del Continuo.*

Capítulo 9

Acerca del proceso de creación en matemáticas

El elemento de invención constructiva, de intuición directora, escapa a una simple formulación filosófica; sin embargo, continúa siendo el núcleo de todo resultado matemático, aun en los campos más abstractos.
(RICHARD COURANT, 1971, PG. 5)

9.1 Hacer matemáticas

Una cosa es cómo se crean las matemáticas y otra cómo se presentan una vez creadas. Ante un teorema y una escueta y elegante demostración pudiera pensar el lector que su autor llegó a ese resultado exactamente tal y como lo ha transcrito. Pero nada más alejado de la realidad. En la investigación matemática se empieza por afrontar un problema (en muchos casos autopropuesto) que suele empezar por una o varias preguntas del tipo: *¿qué pasaría si ...?, si se da tal condición, ¿será verdad que entonces ...?, y si no lo es, ¿de qué dependerá ...?, ¿ocurrirá en estas condiciones siempre A?, ¿nunca?, ¿a veces? y en este último caso ¿cuándo?, ¿por qué?,...*

El investigador no sólo no conoce las respuestas, tampoco el camino más adecuado para buscarlas e incluso, en ocasiones, si algunas de sus preguntas tienen respuesta, aunque espera que las técnicas y conocimientos que tiene sobre el tema le sirvan para llegar a buen puerto. El problema inicial puede derivar a otros y estos otros a otros tantos. El matemático, si la fortuna le sonríe, encontrará respuesta, a veces sólo parcial, a alguna de sus preguntas, otras quedarán en el cajón esperando que tras un oportuno tiempo de reposo se encienda

la luz que marque el sendero correcto para encontrar la solución. Cuando ha resuelto los problemas, o al menos cuando ha encontrado respuesta a una parte sustancial de sus preguntas, entonces reorganiza todo su trabajo, presentando los resultados obtenidos de forma coherente y concisa. Desgraciadamente en la papelera quedan los caminos que no condujeron a ninguna parte, los intentos infructuosos realizados, sin embargo, por senderos adecuados. Y desde que se propuso abordar el problema hasta que llegó a alguna conclusión pasaron semanas, incluso meses, tal vez años. En este proceso, el matemático ha profundizado en su conocimiento del campo de estudio, conoce más y mejor sobre los objetos matemáticos en cuestión, más y mejor sobre sus relaciones, tiene una idea más precisa sobre el alcance de diversas técnicas y sobre los límites de su propia ignorancia.

Hacer matemáticas consiste básicamente en resolver problemas. Identificar la estructura de los mismos, los conceptos subyacentes y las relaciones entre ellos, poner en marcha estrategias adecuadas, utilizar técnicas apropiadas, verificar el proceso seguido, interpretar la solución obtenida y cómo ésta amplía la profundización del conocimiento de los objetos matemáticos en cuestión y de sus relaciones entre ellos, etc. Es claro que algo tendrá que ver ésto con *el método matemático*; es más, esta es la parte esencial y la más difícil de explicar. A ello dedicaremos las líneas que siguen en este capítulo.

Por lo pronto, el lector deberá entender que por problema no nos estamos refiriendo a la realización de ejercicios. Resulta conveniente en este punto precisar la diferencia entre ambos.

Estaremos ante un ejercicio cuando, para su resolución, sólo se requiere la aplicación de ciertas técnicas y el conocimiento de ciertos conceptos previamente identificados y de ello el lector ha encontrado un amplio muestrario en este libro. La finalidad de los mismos es la adquisición de ciertos automatismos, el dominio de ciertas destrezas y el afianzamiento de ciertos hechos.

Estaremos ante un problema, cuando nos encontremos ante una situación para cuya resolución, de entrada, no existe un camino evidente. El problema podrá ser resuelto por el interesado si los conceptos subyacentes, sus relaciones y las técnicas precisas están a su alcance. La dificultad primera estriba en la identificación de tales cuestiones, la siguiente, en encontrar el camino adecuado que conduzca al éxito, la tercera, asegurarse de la corrección de los pasos dados, de las operaciones realizadas, de la adecuación de las técnicas y algoritmos utilizados, y la última, verificar la adecuación de la solución obtenida. Al final del primer capítulo propusimos algunos problemas que pretenden ilustrar estas ideas.

Cuando resolvemos problemas, decíamos antes, conocemos matemáticas más y mejor. Pero además sabemos también más sobre los procesos adecuados para abordar diversidad de problemas, aprendemos cómo determinadas estrategias de pensamiento son provechosas, cómo pueden ser aplicadas a problemas de naturaleza distinta, pero de estructura parecida, y aprendemos a superar situa-

ciones de bloqueo, a desconfiar razonablemente de lo que aparentemente pueda parecer a primera vista evidente; es decir, mejoramos nuestra capacidad para *hacer matemáticas*. Se puede mejorar la capacitación como resolutor de problemas, para lo que es conveniente examinar cuidadosamente el proceso seguido en la resolución de los mismos.

9.2 Análisis de un problema

En el primer capítulo propusimos un problema y proporcionamos la solución dada por un alumno nuestro. Volvamos a examinar aquél problema. Lo haremos en primera persona, de forma que el resolutor piense en voz alta.

> *¿Existe una infinidad de números primos que son de la forma múltiplo de cuatro más tres?*

Entender el problema

Hemos de hacernos una idea precisa de la situación. La cuestión es clara: o hay un número finito de números primos de la forma múltiplo de cuatro más tres, o hay un número infinito. Si hay infinitos números primos, ¿por qué no iba a haber infinitos primos de la forma múltiplo de cuatro más tres?

¿Qué es lo que se busca?, ¿entiendo bien los términos?, ¿hay alguna condición que se me escape? Vamos a examinar un poco la cuestión. Empecemos por ver algunos ejemplos y de esta forma nos familiarizaremos con el problema.

Desde luego, ya sabemos que existen primos múltiplos de cuatro más tres, por ejemplo: 3, 7, 11, 19. Y también que otros no lo son, por ejemplo: 5, 13, 17. Además, los que no son múltiplos de cuatro más tres, serán entonces múltiplos de cuatro más uno, a excepción del 2 claro está, pues son números impares, luego al dividirlos por cuatro sólo pueden dar de resto o tres, o uno.

Si examino de forma más cuidadosa las posibles situaciones, me haré una idea más precisa del problema que tengo entre manos. Se trata entonces de ver las distintas posibilidades que se pueden dar entre el número de primos impares de un tipo y el número de primos impares del otro:

1. Supongamos que hay un número finito de ambos. Esto es absurdo, pues sé que existe una infinidad de números primos.

2. Podría ser que hubiera un número finito de primos de la forma $4k + 1$ y una cantidad infinita de la forma $4k + 3$.

3. Pudiera ser que hubiera un número infinito de primos de la forma múltiplo de cuatro más uno y un número finito del tipo $4k + 3$.

4. Finalmente, pudiera ser que hubiese un número infinito de ambos.

Podríamos intentar probar que uno de los tipos es un conjunto finito y el otro, infinito. Pero si probamos que uno de los tipos constituye un conjunto infinito, nada podemos asegurar del otro. Parece pues razonable intentar probar que el número de primos de la forma $4k+3$ es infinito. Si la cosa no funciona siempre tendré ocasión de volver sobre mis pasos e intentar probar lo contrario.

Concebir un plan

¿Conozco un problema semejante?, ¿sé de algún teorema que me pueda ser útil? Sí, conozco el teorema de existencia de una infinidad de números primos. ¿Me será de utilidad el método allí empleado?, ¿necesitaré algún elemento auxiliar para poder utilizarlo?

Veamos: por analogía con el método del teorema, supondré que hay un conjunto finito de primos de la forma múltiplo de cuatro más tres e intentaré construir un número que sea primo, de la misma forma y que no esté en dicho conjunto. Si tengo éxito habré obtenido el resultado buscado mediante un proceso de reducción al absurdo.

Ejecución del plan

Sean $p_1, p_2, \ldots, p_m$ los únicos primos de la forma $4k+3$. He de construir un número n a partir de ellos que sea múltiplo de cuatro más tres, que sea primo y mayor que todos ellos. El número construido en el teorema $p_1 \cdots p_m + 1$ no nos vale ahora, pues aunque al suponer que es compuesto llegue a que tiene un divisor primo distinto de los p_i, éste, en principio, no tiene porqué ser múltiplo de cuatro más tres, podría ser (al menos mientras no probara lo contrario) múltiplo de cuatro más uno, no llegando de esta forma a contradicción alguna.

El número que deseo construir ha de ser múltiplo de cuatro más tres, parece razonable pensar que sea de la forma $n = 4p_1 \cdots p_m + 3$, pero si uno de los p_i es tres, entonces obviamente $q = p_1 \cdots p_m = \dot{3}$, de donde $4q + 3 = \dot{3}$. Este resultado me indica que en el número que he de construir no puede figurar el 3 como factor en el primer sumando. Sea, por tanto, $n = 4p_2 \cdots p_m + 3$, siendo $p_2 = 7$ y $p_2 < p_3 < \ldots < p_m$, que es de la forma múltiplo de cuatro más tres.

Repaso y veo que está bien. ¿Me servirá para algo éste número n?, eso espero; creo que es el que ando buscando para llegar a una contradicción. Veamos.

Tengo que n no puede ser múltiplo de dos, pues es impar. Tampoco es múltiplo de 3, pues el primer sumando no es múltiplo de 3. Además cualquiera que sea p_i con $2 \leq i \leq m$, $n \neq \dot{p}_i$, pues el resto de la correspondiente división por p_i es obviamente 3. Tengo un primer resultado parcial:

Teorema 9.2.1 *Si $m-1$ números primos $p_2 = 7, \ldots, p_m$ son de la forma múltiplo de cuatro más tres, entonces $n = 4p_2 \cdots p_m + 3$ es primo con cualquiera de los números $2, 3, p_2, \ldots, p_m$.*

Ahora bien, si n así construido es compuesto, entonces tendrá un divisor primo, sea éste q. ¿Me servirá para algo el teorema que he obtenido? Que n tenga un divisor primo, no significa que éste sea múltiplo de cuatro más tres, podría ser múltiplo de cuatro más uno y en este caso no llegaré a contradicción alguna. El camino no me conduce a ninguna parte.

¿He comprobado todo lo que he hecho?, ¿he comprobado todos los razonamientos? Lo que yo tengo que conseguir es un factor de n que sea múltiplo de cuatro más tres, no que cualquier factor sea múltiplo de cuatro más tres.

Examinemos detenidamente esta cuestión. Ahora tengo otro problema (independiente del anterior): "Sea $n \neq \dot{3}$ compuesto y múltiplo de cuatro más tres, ¿tendrá algún divisor primo que sea múltiplo de cuatro más tres?"

Podemos descomponer n en factores primos. Desde luego si todos los factores de la descomposición fueran de la forma múltiplo de cuatro más uno, entonces n sería múltiplo de cuatro más uno, pues el producto de dos cualesquiera es múltiplo de cuatro más uno: $(4k+1)\cdot(4r+1) = 4(4kr+k+r)+1$, por lo tanto ha de existir un factor primo q de n que es múltiplo de cuatro más tres. Tengo otro pequeño teoremita:

Teorema 9.2.2 *Si $n \neq \dot{3}$ es un entero positivo, compuesto y múltiplo de cuatro más tres, entonces existe $q \in \mathbb{Z}^+$ primo, que es múltiplo de cuatro más tres y tal que $n = \dot{q}$.*

Volvamos a nuestro problema inicial. De ser $n = 4p_2 \cdots p_m + 3$ compuesto se sigue, del teorema 9.2.2, que tiene al menos un divisor primo q que es múltiplo de cuatro más tres, luego entonces, por nuestra hipótesis de partida, tendremos que $q \in \{p_1 = 3, p_2, \ldots, p_m\}$. Pero ello es imposible porque, por el teorema 9.2.1, sabemos que $n \neq \dot{3}$ y que además $n \neq \dot{p}_i$, con $p_i \in \{p_2 = 7, \ldots, p_m\}$. Consecuentemente n ha de ser primo. Y entonces $n = \dot{4} + 3 \notin \{p_1 = 3, p_2, \ldots, p_m\}$ es primo, contradiciendo la hipótesis de que éstos p_i eran todos los primos de la forma múltiplo de cuatro más tres. Podemos ya enunciar:

Teorema 9.2.3 *Existe una infinidad de primos que son de la forma múltiplo de cuatro más tres.*

Vuelta atrás

Confirmemos los resultados. Verifico el razonamiento: no he errado. ¿Puedo ver el resultado de una vez? La verdad es que sí, basta enunciar el teorema 9.2.3

y ordenar el razonamiento como se hizo en la demostración vista en el capítulo 1 (teorema 1.1.3).

¿Podemos extender el problema?, ¿podemos averiguar más cosas relativas a este tipo de problemas? Por ejemplo:

1. El número de primos de la forma múltiplo de cuatro más uno, ¿es también infinito?

2. Volvamos nuevamente a la sucesión inicial de nuestro problema:

$$3, 7, 11, 15, 19, 23, 27, 31, \ldots.$$

En ella hay infinitos primos. Pero esta sucesión no es más que una progresión aritmética de razón 4. ¿Ocurrirá lo mismo en cualquier otra progresión aritmética?, ¿en algunas sí y en otras no?, en su caso ¿de qué dependerá?

Tenemos nuevos problemas[1] ¿Valdrá el método para abordar, al menos, el primero de los dos problemas anteriores?

¿Podemos obtener el resultado de forma diferente? Creo que sí.

El "plan concebido" es el mismo que antes, pero voy a intentar variar su ejecución.

Nueva ejecución del plan

Veamos, sean $p_1, \ldots, p_m$ todos los primos de la forma múltiplo de cuatro más tres. Busco un múltiplo de cuatro más tres que no se encuentre entre los anteriores y que sea primo.

Considero el producto de los mismos $p = p_1 \cdots p_m$. ¿Cómo es p?, ¿es múltiplo de cuatro más tres? Es obvio que no necesariamente, pues: $3 \cdot 7 = 21 = 4 \cdot 5 + 1$, de la misma manera $7 \cdot 11 = 77 = 4 \cdot 19 + 1$, sin embargo $3 \cdot 7 \cdot 11 = 231 = 4 \cdot 57 + 3$. ¿De qué dependerá que sea múltiplo de cuatro más tres o múltiplo de cuatro más uno?

Si el número de factores m es par, entonces p es múltiplo de cuatro más uno, pues el producto de cada dos de ellos tiene esta forma. Si m es impar, entonces p es múltiplo de cuatro más tres.

Ahora bien, se trata de que pueda construir un número primo del tipo $4+3$ y que no esté entre los m considerados, pero no necesariamente tengo que buscar, como antes, un tal número válido cualquiera que sea el número m. Puedo buscar uno que me sirva, en el primer caso cuando m es par y otro cuando m es impar.

[1] En el segundo caso, aunque la formulación de la pregunta es clara y el problema tiene un enunciado simple, su dificultad resulta extremadamente elevada. Dirichlet (1805–1859) demostró que *"Si $a, a + r, a + 2r, a + 3r, \ldots$, es una progresión aritmética de razón r tal que a y r son primos entre sí, entonces en ella hay una infinidad de números primos.* Su demostración requiere el uso de recursos matemáticos superiores.

Para m par, sea $n = p + 2$. Este número es del tipo $\dot{4} + 3$ y, desde luego, es primo con cualquiera de los p_i.

Si m es impar, $p+2$ es de la forma $\dot{4}+1$, por lo que no vale. Sea $n = 3p+2$, que es múltiplo de cuatro más tres y tal que es primo con cada uno de los p_i.

Ahora bien, pudiera ocurrir, en uno y otro caso, que el número n elegido no fuera primo, por ser divisible por un primo de la forma $\dot{4} + 1$. Pero claro, después de haber resuelto el problema, ya sé que la clave está en que si n es compuesto y múltiplo de cuatro más tres, tenga un factor primo q de la forma $\dot{4} + 3$, que sé que existe (lo hemos probado antes).

En ambos casos (m par o impar) tenemos que si n es primo ya tengo una contradicción con la hipótesis de reducción al absurdo. De no ser n primo, también en ambos casos, entonces q es divisor de n. Ahora bien si n es primo con cada p_i, entonces q también es primo con cada p_i, por lo que q es primo, del tipo $\dot{4}+3$ y distinto de cada p_i, luego llego a contradicción con la suposición de que todos estaban en $\{p_1, \ldots, p_m\}$.

Bueno, pero ¿podría intentar resolver el problema de una forma sustancialmente diferente? Tal vez la cosa sea cambiar de perspectiva. Sigo "obsesionado" con el procedimiento de reducción al absurdo.

Me replanteo el problema. Es equivalente a este otro: *"Cualquiera que sea el entero positivo n, encontrar un primo p, de la forma múltiplo de cuatro más tres, y que sea mayor que n.*

El lector debiera animarse a resolverlo.

9.3 Sobre la resolución de problemas

Decía Descartes (1596–1650) en el *Discurso del Método* publicado en 1637: *mi propósito, pues, no es el de enseñar aquí el método que cada cual ha de seguir para dirigir bien su razón, sino sólo exponer el modo como yo he procurado conducir la mía* y en la descripción ponía de manifiesto su método, que él creía universal, para resolver problemas. Desgraciadamente no existe este ideal cartesiano, pero tal vez sea posible aprender pequeñas etapas hacia ese ideal inaccesible. Y aunque *existe una gran variedad de formas de aprender eficazmente a "pensar matemáticamente"*, hemos optado por seguir las indicaciones de G. Polya [14]. El análisis del problema anterior se ha efectuado siguiendo sus indicaciones. La lectura de algunas de sus obras, reseñadas en la bibliografía, así como la de otros autores, también reseñados, como M. de Guzmán [6], Mason - Burton y Stacey [11] y Schoenfeld [17] será especialmente provechosa, por lo que las recomendamos vivamente.

Si en la redacción de este capítulo hemos tenido presente las ideas de Polya, es porque establece un marco claro para la reflexión del resolutor de problemas. Otras aportaciones, como las ya indicadas, matizan el sentido dinámico de las

diversas etapas en que Polya divide la resolución de un problema, o bien analizan aspectos de índole "psicológica", como los bloqueos, o establecen una división más fina.

9.3.1 Fases en la resolución de un problema

Siguiendo a Polya, distinguiremos cuatro fases en la resolución de un problema, cada una de las cuales queda caracterizada por una serie de interrogantes que sirven a modo de orientaciones para la práctica y tipifican un heurístico o estrategia general para la resolución del problema.

Las estrategias generales son las operaciones mentales, independientes de cualquier contenido concreto, que se desarrollan en el proceso de resolución de un problema, orientando la elección de los conocimientos y destrezas que serán necesarios utilizar para tal fin.

El buen resolutor está familiarizado con estrategias como las de: estimar y aproximar, ensayo y error, hacer una figura o un diagrama, simplificar tareas difíciles mediante el estudio de casos sencillos, dividir el problema en subproblemas, particularizar, utilizar la analogía, generalizar, reconocer regularidades, razonar hacia atrás, buscar contraejemplos, proceder por reducción al absurdo, conjeturar y verificar, probar y refutar, etc.

Las fases en la resolución de un problema son:

1. Entender el problema:

   En esta fase se trataría de hacerse una idea clara de la situación. Se puede decir que el problema se ha entendido cuando se es capaz de interpretar y reformular el enunciado, identificando los datos, las condiciones y lo que se busca.

   Una adecuada comprensión puede tener lugar después de diversos intentos fallidos de resolución, siempre que el control, que es necesario que el resolutor ponga en juego sobre su propio proceso, lo haga sabiamente volver hacia atrás.

   Son preguntas distintivas de esta fase:

   ¿Qué se busca?, ¿cuáles son los datos?, ¿entiendo bien los términos?, ¿sería capaz de reformular el problema?, ¿cuál es la condición?, ...

   Estrategias propias de esta fase son:

   Organizar la información, Ejemplificar, ...

2. Concebir un plan:

   En esta fase el resolutor explora caminos, posibilidades, intenta algunos, tantea el terreno y toma una decisión final concibiendo un plan para atacar el problema.

   Son orientadoras las respuestas a interrogantes como éstos:

¿Recuerdo un problema semejante?, ¿recuerdo algún problema relacionado con éste?, ¿conozco algún resultado teórico que me pueda ser útil? ...

Tengo un problema relacionado con el mío ya resuelto: ¿puedo emplear su resultado?, ¿y su método?, ...

No puedo resolverlo: ¿y si considero un caso particular?, ¿y si añado una condición que no esté en los datos?, ¿y si elimino alguna condición y lo hago más general?, ¿y si considero este otro análogo?, ¿podría resolver una parte del problema?, ...

¿He empleado todos los datos?, ¿y todas las condiciones?, ¿y todas las nociones esenciales concernientes al problema?, ...

En esta fase se ponen en juego las distintas estrategias, apuntadas por las preguntas anteriores: Simplificar, Particularizar, Generalizar, Analogía, Subproblemas, Conjeturar y verificar, Probar y refutar, Estimar, Aproximar, Razonar hacia atrás, ...

3. Ejecución del plan:

   Tras concebir un plan; es decir tras haber optado por una estrategia concreta se trata de ponerla en práctica, haciendo uso, cuando sea necesario, de nuevos heurísticos, propios de la fase anterior, en el proceso de ejecución. Es importante llevarlo a la práctica con rigor:

   ¿He comprobado cada paso que he dado?, ¿he detallado cada operación que me ocupa?, ¿para qué me servirá este resultado parcial?, ...

   Son heurísticos típicos de esta fase:

   Comprobar, Organizar con claridad la ejecución, ...

4. Vuelta atrás:

   Se trata de reflexionar sobre lo hecho y sobre su utilidad posterior. Son orientadoras las respuestas a las preguntas:

   ¿Puedo verificar el resultado?, ¿y el razonamiento?, ¿puedo obtenerlo de forma diferente?, ¿puedo emplear el resultado o el método de resolución en algún otro problema?, ...

   Los heurísticos más característicos de esta fase son:

   Comprobar la solución, Concretar la solución para casos particulares, Simplificar la solución, Examinar los razonamientos efectuados, Verificar la corrección de los pasos, Examinar y valorar el método, Extrapolar la solución y el método, ...

El lector debiera, ahora, contrastar el análisis del problema efectuado en la sección anterior con lo que acabamos de exponer y también con el proceso por él seguido, cuando abordó los problemas que se propusieron en el primer capítulo, lo que sin duda será enriquecedor.

En la resolución de problemas hemos de procurar reflexionar sobre los conceptos implicados y sobre sus mutuas relaciones, sobre los heurísticos movilizados y sobre nuestro propio proceso de resolución. Esta última cuestión es fundamental para mejorar nuestra capacidad para *hacer matemáticas*.

9.3.2 El control en el proceso de resolución

Como hemos podido observar, dentro de cada fase, el resolutor debe estar en condición de *controlar* la acción de su pensamiento, desechando estrategias que resulten infructuosas, volviendo a una fase anterior si fuera preciso ante un reiterado fracaso, etc.; en definitiva, el resolutor debe desarrollar su capacidad de *control* sobre el desarrollo de sus decisiones, tomando otras que contribuyan a perfeccionar el proceso de resolución. El *control* marca un punto de inflexión en el proceso de resolución y sirve para replantear y observar tanto el proceso mismo como la calidad de lo que se está haciendo. La capacidad de control es esencial para adquirir una buena capacitación como resolutor de problemas. Periódicamente hay que cuestionarse el camino emprendido, su idoneidad.

Hay que tener presente que no sólo importa lo que se sabe, sino también lo que se usa y porqué se usa y que en múltiples instantes el resolutor ha de replantearse el *proceso* y la *calidad* de lo que está haciendo. Algunas preguntas idóneas para cuidar el control sobre el proceso son:

- ¿Qué es lo que estoy haciendo?, ¿para qué?
- ¿Qué voy a hacer con ello?, ¿de qué forma me ayuda?
- ¿Cómo encaja el resultado?
- Pienso en un caso sencillo, ¿es cierto?, ¿qué es lo que falla?, ¿por qué?
- ...

Epílogo

Hemos abordado aunque sólo sea someramente, entre otras, dos cuestiones de capital importancia en el estudio de las matemáticas:

1. ¿Cuándo un argumento matemático es correcto?

2. ¿Qué métodos podemos usar para construir argumentos matemáticos?

De lo estudiado en el epígrafe *Terminología matemática*, pudiera extraerse la conclusión aventurada de que las verdades matemáticas, de una determinada teoría, pueden deducirse a partir de la selección de un buen sistema de axiomas y que una demostración siempre es reducible a un encadenamiento finito de fórmulas, de cuyo análisis lógico puede determinarse sin error la corrección o no de la misma. Ya sabemos que desafortunadamente o tal vez afortunadamente (para la riqueza y complejidad de las matemáticas) las cosas no son así.

Un breve paseo por la historia de las matemáticas nos ayudará a situar adecuadamente el significado del método axiomático–deductivo y dónde se sitúa la intuición creadora.

1 Sobre el método axiomático–deductivo

A pesar del rigor del proceder del método axiomático–deductivo presente en los *Elementos* de Euclides (S. III a. C.), prácticamente desde su aparición, el quinto y último postulado despertó recelos ya que se pensaba que su formulación era demasiado complicada. Nadie dudaba de su veracidad, pero carecía de la cualidad de simplicidad y autoevidencia de los otros axiomas.

Desde entonces hasta aproximadamente 1800, se llevaron a cabo dos líneas de trabajos para eliminar las dudas acerca de este axioma. Uno fue reemplazarlo por otra formulación más autoevidente. El otro fue deducirlo a partir de los restantes axiomas. Lobachewsky (1793-1856) intentó mediante la negación de este postulado, manteniendo los restantes, llegar a una contradicción, pero en su lugar obtuvo una geometría perfectamente consistente y distinta de la de

Euclides, que dió a conocer en 1829. En 1868 se demostró que era imposible deducir el quinto postulado de los demás.

Desde la aparición de las geometrías no euclídeas, es evidente que distintas verdades matemáticas pueden obtenerse si se parte de axiomas diferentes, siendo todas ellas igualmente válidas.

Por aquella época, alrededor de 1870, Cantor trabajando en teoría de series infinitas, inicia el desarrollo de la teoría de conjuntos. Su trabajo lo llevó a la consideración de conjuntos infinitos. En 1874 publicó una famosa demostración de que el conjunto de los números reales no puede ponerse en correspondencia biunívoca con el conjunto de los números naturales. En 1878 introdujo la noción fundamental de conjuntos equipotentes, como aquellos que pueden ponerse en correspondencia biunívoca; este concepto condujo, en el caso de los conjuntos infinitos, a una generalización del concepto de número natural, al de número cardinal infinito. La característica de los conjuntos infinitos, definidos por primera vez por Dedekind en 1872, resultó ciertamente chocante, ya que un conjunto es infinito si y sólo si es equipotente a un subconjunto propio suyo. Una gran aportación de Cantor fue la de demostrar que no todos los conjuntos infinitos tienen la misma cardinalidad. Otra gran contribución suya fue el desarrollo de la teoría general de los números transfinitos; puesto que tanto si un conjunto A es finito como si no lo es, su conjunto potencia no es equipotente con A, se obtiene entonces, como ya sabemos, una cadena ilimitada de conjuntos crecientes infinitos no equipotentes, al "más pequeño" de los cuales (el cardinal de los números naturales) lo llamó $\aleph_0$ y al de los números reales $2^{\aleph_0} = c$ (la potencia del continuo). La pregunta de si existirá algún conjunto infinito cuya cardinalidad sea intermedia entre $\aleph_0$ y c, o por el contrario $\aleph_1 = c$ fue contestada, como ya hemos indicado, por el propio Cantor, conjeturando que no; y como también hemos señalado esta conjetura recibe el nombre de *Hipótesis del Continuo.*

Ciertamente desde el inicio de la teoría de conjuntos infinitos se plantearon resultados si no tan paradójicos, al menos tan chocantes como la propia caracterización señalada, o como el hecho de que los números racionales y los naturales tuviesen la misma potencia, o que un segmento unidad tuviese la misma potencia que el cuadrado unidad; tanto es así, que hasta el propio Cantor le pidió mediante una carta a Dedekind, en 1877, que revisase cuidadosamente la demostración del último resultado aquí indicado. En el último cuarto del siglo XIX aparece una serie de paradojas[2] en la teoría de conjuntos como: la "del mayor ordinal" dada a conocer en 1887 por Burali-Forti (1861–1931), la "del mayor número cardinal" descubierta por el propio Cantor en 1899 (pero publicada en 1932) y la de Bertrand Russell, referida anteriormente en el capítulo 3. Todos estos hechos junto con problemas en la fundamentación del Análisis originaron una profunda crisis de fundamentos.

[2]Un análisis más detenido de estas y otras paradojas, así como de su distinción entre paradojas lógicas y lingüísticas o semánticas, puede verse en Patrick Suppes [18] o en: BETH, E. (1950). *Les Fondements logiques des mathématiques.* París, Gauthier-Villars.

Puesto que las entidades que se estudian en matemáticas pueden considerarse como ciertas clases particulares de conjuntos, formalmente las diversas ramas de las matemáticas pueden considerarse dentro de la teoría de conjuntos. Por tanto las preguntas fundamentales acerca de la naturaleza de las matemáticas se intentaron reducir a preguntas acerca de la teoría conjuntista. Así se intentó, a principios de este siglo, fundamentar las matemáticas sobre la noción de conjunto, para lo que era necesario establecer un sistema de axiomas que regulase qué cosa es un conjunto y qué cosa no lo es, evitando posibles paradojas. El sistema de axiomas debía fijar también qué tipo de manipulaciones pueden realizarse con los conjuntos para obtener nuevos conjuntos. A la vez era preciso levantar un entramado que permitiera expresar en lenguaje conjuntista todos los conceptos de las matemáticas.

La axiomática de Zermelo–Fraenkel más el axioma de elección (teoría axiomática de Zermelo–Fraenkel estándar) fue la respuesta. En ella se construyen los números naturales.

Como ya sabemos, en 1908 Zermelo funda la teoría axiomática de conjuntos al introducir el esquema axiomático de separación en lugar del de abstracción que había originado la paradoja de Russell, y cuatro años antes había formulado el axioma de elección. Aunque el primero, no es el único que intervino en la axiomatización de esta teoría, de hecho la contribución de Frankel (1891-1965) fue tan importante, que la actual axiomática lleva el nombre de teoría de conjuntos de Zermelo-Fraenkel, pues fue este último el que introdujo, en 1922, el esquema axiomático de sustitución necesario para la aritmética ordinal y al que luego nos referiremos.

Para Zermelo un conjunto es un objeto no definido que satisface a una lista de axiomas dados. No obstante hay que señalar que los axiomas no fueron elegidos arbitrariamente, sino de acuerdo con una noción intuitiva cuyas consecuencias paradójicas se querían evitar, vedando todo papel a la intuición en el desarrollo posterior.

1.1 Limitaciones de la fundamentación axiomática

En el Congreso de la *Unión Matemática Internacional* celebrado en París en 1900, Hilbert (1862–1943) presentó veintitrés problemas. En el segundo de ellos se preguntaba si se podría demostrar que los axiomas de la aritmética son consistentes, es decir, que un número finito de etapas lógicas basadas en ellos no puede conducir a resultados contradictorios. Gödel (1906–1978) demostró en 1931 que en un sistema axiomático $\mathcal{S}$ que contenga a la axiomática del número natural, pueden formularse infinitas proposiciones p que son indecidibles (de forma que nunca podrá probarse si p es verdadera o falsa; o lo que es lo mismo existen dentro del sistema ciertas afirmaciones bien definidas, que no pueden ser demostradas ni refutadas a partir de los axiomas). Equivalentemente, si el sistema $\mathcal{S}$ fuese consistente y se le añade p, el nuevo sistema sigue siendo consistente y si a $\mathcal{S}$ se le añade $\neg p$ también se obtiene un nuevo sistema consistente.

Pero esto no fue todo, también en 1931 Gödel demostró que no es posible garantizar la *consistencia* de cualquier sistema de axiomas que contenga a la axiomática del número natural (en particular la de Zermelo–Fraenkel). En otras palabras, no es posible garantizar que no pueda demostrarse un cierto teorema p y su contrario $\neg p$. Naturalmente no es "previsible" que pueda darse una situación tan profundamente caótica, al fin y al cabo el edificio que habitamos se observa sólido y robusto y nadie, en tales condiciones, piensa que la casa se le puede venir encima. No obstante, Gödel nos advirtió que un cataclismo siempre es posible.

1.2 Sobre la demostración

Si la fundamentación tiene estas notabilísimas limitaciones, la idea de demostración también tiene las suyas. Teóricamente un teorema debiera considerarse demostrado si se deduce a partir de los axiomas mediante una manipulación correcta de los símbolos. Pero esto convertiría a la matemática en absolutamente ilegible (piénsese que Russell y Whitehead en su obra *Principia Mathematica*, que fue un intento de sistematización lógica y formalizada de la matemática, sólo después de más de cuatrocientas páginas pudieron obtener que $1 + 1 = 2$). En la práctica se acepta como demostración aquello que podría escribirse en esa forma, si se tuviese tiempo ilimitado y paciencia infinita. Realmente una demostración se considera correcta cuando diversos especialistas del tema en cuestión de la comunidad matemática la aceptan como tal.

Naturalmente en el proceso de demostración se hace uso de reglas de inferencia correctas y se sigue un razonamiento lógico cuyas premisas han sido estudiadas en lo que antecede, pero de ninguna manera, como el lector habrá ya experimentado, se procede mediante una cadena deductiva paso a paso, según los esquemas de la lógica simbólica. Y aún más, el rigor en la demostración viene dirigido por la inspiración, por la intuición creadora del matemático, que busca intrincados caminos para responder preguntas nacidas de su inagotable curiosidad.

La comunidad matemática encajó aquellos resultados y ha continuado produciendo teorema tras teorema. Se ha continuado trabajando como siempre se hizo, apoyándose en la intuición y en métodos informales y heurísticos y semiformalizando los resultados una vez obtenidos.

2 Sobre el axioma de elección y la hipótesis del continuo

Por su importancia para la matemática actual no queremos dejar de referirnos al axioma de elección (AE) y a la hipótesis del continuo (HC).

Como ocurrió con la geometría euclídea, en la teoría de conjuntos de Zermelo-

Frankel había igualmente un axioma cuestionado, se trataba del axioma de elección. Su significado intuitivo es claro y en ese sentido plausible, pero, como indicamos en el capítulo 8, la remisión al infinito, a una colección infinita de conjuntos, impide que realmente se pueda elegir verdaderamente uno por uno los elementos en cada uno de los conjuntos miembros de la colección. Por otra parte, dentro de la axiomática estándar de Zermelo-Frankel (donde incluimos el axioma de elección) aparece como teorema la famosa "paradoja" de Banach-Tarski, resultado que nos permitiría a partir de una esfera sólida cualquiera en el espacio tridimensional descomponerla en un número finito de partes disjuntas, de tal manera que, a partir de un cierto número de ellas, podemos construir una esfera idéntica a la dada por medio de movimientos rígidos (sin deformación), y con las restantes otra esfera también idéntica a la inicial por el mismo procedimiento; resultado que choca frontalmente con nuestra intuición básica de que cualquier conjunto acotado del espacio tridimensional tiene un volumen perfectamente definido, sea positivo o nulo, e invariante por isometrías. Sin embargo la importancia que tiene este axioma es fundamental, pues sin el axioma de elección buena parte de la matemática actual no se sustentaría.

El hecho es que la comunidad matemática procuró utilizar este axioma lo menos posible. Sin embargo en 1938 Gödel clarificó el panorama, al obtener el siguiente resultado: si la teoría de Zermelo-Frankel restringida (sin el axioma de elección) es consistente, entonces también lo es con el axioma de elección (teoría estándar). Dicho de otra manera, el axioma de elección no es más peligroso que el resto de los axiomas y, por tanto, si hay una contradicción en la teoría de Zermelo-Frankel estándar es porque previamente existía una contradicción en la teoría restringida.

En 1963 Paul J. Cohen (1934) demostró que el axioma de elección es independiente de los restantes axiomas de la teoría de Zermelo-Frankel restringida, para lo que construyó una teoría no cantoriana de conjuntos, es decir, con los axiomas de la teoría restringida y como nuevo axioma la negación del axioma de elección y demostró que si la teoría restringida era consistente la nueva teoría no cantoriana también es consistente.

Por otra parte, Gödel en 1940 y Cohen (1934) en 1963 probaron que la Hipótesis del Continuo es consistente con los axiomas de la Teoría de Zermelo–Fraenkel, pero que no puede ni probarse ni refutarse (es indecidible). Aceptarla o rechazarla como un nuevo axioma conduce, desde la axiomática de Zermelo–Frankel, a dos teorías distintas sobre la concepción del infinito matemático.

3 Otras consideraciones sobre la axiomática de conjuntos

A lo largo de estas páginas hemos ido haciendo referencia a distintos axiomas necesarios para la presentación formal de los diversos conceptos que se han ido

introduciendo, con el propósito, como adelantábamos en el prólogo, de, por una parte, ilustrar el significado del método axiomático-deductivo y, por otro, de crear una base intuitiva sobre la que en un futuro, tal vez no demasiado lejano, el lector pueda iniciar el estudio de la teoría axiomática de conjuntos.

Es el momento de hacer referencia a dos axiomas de los que nada hemos comentado, con los que podemos completar una visión global de la axiomática de Zermelo-Fraenkel.

3.1 El axioma de regularidad

Parece razonable que evitemos la posibilidad formal de que un conjunto pudiera considerarse como elemento de sí mismo. Por ejemplo, el conjunto de todos los árboles no es un árbol y por tanto no es un elemento de sí mismo.

A este fin podríamos tomar como axioma $A \notin A$, pero ello no evitaría que puedan existir dos conjuntos distintos A y B tales que $A \in B$ y $B \in A$, lo que no deja de ser algo nada intuitivo. Aún tomando como axioma la imposibilidad de esta última situación, nos encontraríamos con la posibilidad de existencia de tres conjuntos distintos entre sí y tales que $A_1 \in A_2$, $A_2 \in A_3$ y $A_3 \in A_1$. Si nuestro axioma postulase expresamente la imposibilidad de esta última situación, nada impediría la existencia de cuatro conjuntos distintos con un comportamiento semejante a los anteriores. Y así sucesivamente. Para evitar la existencia de sucesiones "descendientes" de conjuntos $A_1, A_2, \ldots, A_i, A_{i+1}, \ldots$ tales que $A_{i+1} \in A_i$ consideraremos el siguiente axioma, introducido por Zermelo en 1930.

> **Axioma de regularidad:**
> Si A es un conjunto no vacío, entonces existe un elemento $x \in A$ tal que $x \cap A = \emptyset$.

Formalmente:

$$A \neq \emptyset \longrightarrow \exists x[x \in A \wedge \forall y(y \in x \longrightarrow y \notin A)].$$

Veamos que efectivamente este axioma evita que pueda darse que $A \in A$; es decir, cualquiera que sea el conjunto A se tiene que $A \notin A$:

> Supongamos por el contrario que existe un conjunto A tal que $A \in A$. Se tiene que $A \in \{A\} \neq \emptyset$. Luego $A \in \{A\} \cap A$.
>
> Por otra parte, por el axioma de regularidad, existe $x \in \{A\}$ tal que $\{A\} \cap x = \emptyset$. Pero como $\{A\}$ es unitario, se sigue que $x = A$, de donde $\{A\} \cap A = \emptyset$, llegando a una contradicción con $A \in \{A\} \cap A$.

De la misma manera, el axioma de regularidad nos garantiza que *no existen dos conjuntos distintos A y B tales que $A \in B$ y $B \in A$.*

En efecto:

Supongamos por el contrario que existen A y B tales que $A \in B$ y $B \in A$. Entonces $A, B \in \{A, B\} \neq \emptyset$. Se tiene que

$$A \in \{A, B\} \cap B \quad \text{y} \quad B \in \{A, B\} \cap A. \tag{1}$$

Por otra parte, por el axioma de regularidad, existe $x \in \{A, B\}$ tal que $\{A, B\} \cap x = \emptyset$.

Ya que $x \in \{A, B\}$, entonces se tiene que $x = A$ o bien $x = B$, de donde $\{A, B\} \cap A = \emptyset$ o bien $\{A, B\} \cap B = \emptyset$, lo que contradice (1).

3.2 El axioma de sustitución

El axioma de sustitución permite que cualquier cosa sensata que se pueda hacer a los elementos de un conjunto, produzca un conjunto. La idea intuitiva del axioma es que si tenemos un cierto predicado $P(x, y)$ con la propiedad de que para todo x en un conjunto A existe un único y tal que $P(x, y)$, entonces podamos asegurar que el conjunto de los y existe y "sustituir" A por ese nuevo conjunto.

Formalmente:

Axioma de sustitución:

$$\forall x\ \forall y\ \forall z\ (x \in A \wedge P(x, y) \wedge P(x, z) \longrightarrow y = z)$$
entonces
$$\exists B\ \forall y\ [y \in B \longleftrightarrow \exists x(x \in A) \wedge P(x, y)].$$

Este axioma permite prescindir del axioma de especificación, ya que éste se deduce de aquél. En efecto:

Si $P(x, y)$ es "$x = y \wedge p(y)$", tenemos entonces que

$$\exists B\ \forall y\ [y \in B \longleftrightarrow \exists x(x \in A) \wedge (x = y \wedge p(y))],$$

de donde resulta que

$$\exists B\ \forall y\ [y \in B \longleftrightarrow y \in A \wedge p(y)],$$

que es el axioma de especificación.

Por otra parte, el axioma de las parejas se sigue de los axiomas de las potencias y del de sustitución. En efecto:

Sea $A = \mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$. Sean C y D dos conjuntos cuyo conjunto pareja queremos formar. Sea $P(x, y)$:

$$\text{“}(x = \emptyset \wedge y = C) \vee (x = \{\emptyset\} \wedge y = D)\text{”}.$$

Para cada $x \in \mathcal{P}(\mathcal{P}(\emptyset))$ existe un único y tal que $P(x, y)$.

Por el axioma de sustitución

$$\exists B\ \forall y\ [y \in B \longleftrightarrow \exists x\,\{x \in \{\emptyset, \{\emptyset\}\} \wedge \\ ((x = \emptyset \wedge y = C) \vee (x = \{\emptyset\} \wedge y = D))\}].$$

Obtenemos precisamente que existe un conjunto B que tiene como elementos a C y a D; es decir:

$$\exists B\ \forall y\ [y \in B \longleftrightarrow y = C \vee y = D],$$

con lo que hemos obtenido que $B = \{C, D\}$.

Bibliografía

[1] **Aizpuru Tomás, A.** (1997). *Dominios algebraicos numéricos (Los Principios del Análisis Matemático).* Cádiz, Departamento de Matemáticas. Universidad de Cádiz.

[2] **Courant, R. y Robbins, H.** (1971). *¿Qué es la matemática?* Madrid, Ed. Aguilar.

[3] **Davis, P. – Hersh, R.** (1988). *Experiencia matemática.* Madrid, M.E.C. y Labor.

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

[5] **Garrido, M.** (1978). *Lógica Simbólica.* Madrid, Ed. Tecnos.

[6] **Guzmán, M. de.** (1991). *Para pensar mejor.* Madrid, Ed. Labor.

[7] **Halmos, P.** (1973). *Teoría intuitiva de conjuntos.* México, C.E.C.S.A.

[8] **Honsberger, R.** (1994). *El ingenio en las matemáticas.* Madrid, Ed. Euler.

[9] **Hrbacek, K. – Jech, T.** (1984). *Introduction to Set Theory.* New York, Marcel Dekker, Inc.

[10] **Kuratowski, K., Mostowski, A.** (1976). *Set Theory.* North–Holland.

[11] **Mason, J.** (1988).*Pensar matemáticamente.* Madrid, M.E.C. y Labor.

[12] **Pérez Jiménez, M. J.** (1988).*Teoría de clases y conjuntos.* Barcelona, Edunsa.

[13] **Pérez Fernández, J. et atl.** (1997). *Problemas de Teoría Elemental de Números.* Cádiz, Departamento de Matemáticas. Universidad de Cádiz.

[14] **Polya, G.** (1957).*Cómo plantear y resolver problemas.* México, Trillas.

[15] **Polya. G.** (1967). *La Découverte des Mathématiques.* Paris, Dunod.

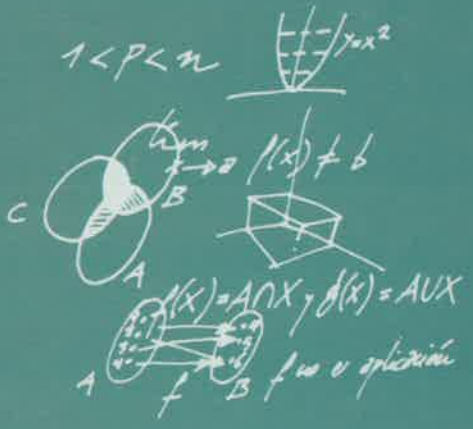
[16] **Rosen, K. H.** (1991). *Discrete Mathematics and its Applications.* New York, McGraw–Hill, Inc.

[17] **Shoenfeld, A.** (1985).*Mathematical problem solving.* San Diego, Academic Press.

[18] **Suppes, P.** (1968).*Teoría axiomática de conjuntos.* Cali, Editorial Norma.

[19] **Velleman, D.** (1994).*How to prove it.* New York, Cambridge University Press.

Indice de términos



SERVICIO•DE•PUBLICACIONES
UNIVERSIDAD•DE•CADIZ
1998

ISBN: 84-7786-509-4
9 788477 865094