2

Cálculo I

Números reales

Departamento de Matemáticas
Universidad de Extremadura

06 · 10 · 2023

En este capítulo se estudian los números reales. Se verán propiedades elementales y otras no tan elementales. Por ejemplo, $|x+y| \leq |x|+|y|$, que es una propiedad que cumplen todos estos números. Se denotará mediante $\mathbb{R}$ al conjunto de los números reales.

Es posible demostrar la existencia de $\mathbb{R}$ como (el único) cuerpo ordenado y completo. Hay varias pruebas de esta existencia. Una de ellas comienza con la construcción de los números racionales para llegar, a partir de las sucesiones de números racionales, a los números reales.

En este curso se asumirá la existencia de $\mathbb{R}$ como un cuerpo ordenado que cumple una serie de axiomas (propiedades que se suponen ciertas para los números reales) iniciales. A partir de ellos se demostrarán nuevas propiedades (teoremas) que irán apareciendo a medida que avance el capítulo. Se estudiarán además ciertos subconjuntos de los números reales, como los números naturales $\mathbb{N}$, los enteros $\mathbb{Z}$, los racionales $\mathbb{Q}$, y algunos más.

Axiomas para $\mathbb{R}$

El conjunto de números reales $\mathbb{R}$ tiene dos operaciones, suma y producto,

$$(x,y) \in \mathbb{R} \times \mathbb{R} \longrightarrow x+y \in \mathbb{R}, \qquad (x,y) \in \mathbb{R} \times \mathbb{R} \longrightarrow x\,y = x \cdot y \in \mathbb{R},$$

que verifican

Axioma I. Ambas operaciones son conmutativas, es decir,

$$x+y = y+x, \qquad x \cdot y = y \cdot x,$$

para cada $x, y \in \mathbb{R}$.

Axioma II. Propiedad asociativa de las dos operaciones:

$$x+(y+z) = (x+y)+z, \qquad x \cdot (y \cdot z) = (x \cdot y) \cdot z,$$

para $x, y, z \in \mathbb{R}$.

Departamento de Matemáticas
Universidad de Extremadura

Departamento de Matemáticas
Universidad de Extremadura

Axioma III. El producto es distributivo con respecto a la suma, es decir,

$$x\,(y+z) = x\,y + x\,z$$

para $x, y, z \in \mathbb{R}$.

Axioma IV. Existen dos elementos distintos 0 y 1 en $\mathbb{R}$ que cumplen

$$x + 0 = x, \qquad x \cdot 1 = x,$$

para cada $x \in \mathbb{R}$. Estos elementos son únicos. De haber dos elementos neutros de la suma 0 y $0'$ se tendría $0 = 0 + 0' = 0'$. Lo mismo ocurre con el elemento unidad 1, sólo puede haber uno.

Axioma V. Existencia de elemento opuesto (para la suma) y de elemento inverso (para el producto):

a) Si $x \in \mathbb{R}$, existe un único elemento $-x \in \mathbb{R}$ (que se llama opuesto de x) que verifica $x + (-x) = 0$, y

b) Si $x \in \mathbb{R}$ y $x \neq 0$, existe un único elemento $x^{-1} \in \mathbb{R}$ (se llama inverso de x) que cumple $x\,x^{-1} = 1$.

Se llama cuerpo conmutativo a cualquier conjunto que tenga dos operaciones verificando estos cinco axiomas. El conjunto $\mathbb{R}$ de números reales es un cuerpo conmutativo.

A partir de estos axiomas ya vistos se pueden obtener nuevos resultados. Son consecuencias de ellos y se llaman *teoremas*. Como regla general, cada teorema va acompañado de una *demostración*.

Teorema (leyes de cancelación). *Dados* $x, y, z, w \in \mathbb{R}$, *con* $w \neq 0$, *se tiene*

a) $x + z = y + z \implies x = y$.

b) $x\,w = y\,w \implies x = y$.

Demostración. a) Si $x + z = y + z$ entonces $x = x + z + (-z) = y + z + (-z) = y$. De la misma forma se demuestra b), ya que si $x\,w = y\,w$ entonces $x = x\,w\,w^{-1} = y\,w\,w^{-1} = y$. □

Teorema. *Si* $x, y, z, w \in \mathbb{R}$, *con* $z \neq 0 \neq w$, *entonces*

a) $x \cdot 0 = 0$, (*como consecuencia, los elementos unidad del axioma IV deben ser distintos, ya que* $x \cdot 1 = x$ *pero* $x \cdot 0 = 0$),

b) $-(-x) = x$,

c) $\left(w^{-1}\right)^{-1} = w$,

d) $(-1) \cdot x = -x$,

e) $x(-y) = -(xy) = (-x)y$,

f) $(-x) + (-y) = -(x + y)$,

g) $(-x)(-y) = xy$,

h) $(x/z)(y/w) = (xy)/(zw)$, *donde* a/b *significa* $a\,b^{-1}$,

i) $(x/z) + (y/w) = (xw + yz)/(zw)$.

Demostración. a) Como $x \cdot 0 + x \cdot 0 = x \cdot (0+0) = x \cdot 0 = 0 + x \cdot 0$, aplicando la ley de cancelación se tiene $x \cdot 0 = 0$. Para probar b), basta escribir $x + (-x) = 0 = (-x) + [-(-x)] = -(-x) + (-x)$ y de nuevo se llega a que $x = -(-x)$. El resto de la demostración es sencilla y se deja como ejercicio. $\square$

Axiomas del orden. $\mathbb{R}$ contiene un subconjunto P (que se llama parte positiva de $\mathbb{R}$) que induce un orden en los números reales, tal y como se explica a continuación.

Axioma VI. Los conjuntos $\{0\}$, P y $-P = \{x \in \mathbb{R} : -x \in P\}$ son disjuntos dos a dos y la unión de ellos es $\mathbb{R}$.

Axioma VII. Si $x, y \in P$ entonces $x + y \in P$ y $xy \in P$.

Definición (orden en $\mathbb{R}$). Los elementos de P se llaman *números positivos* y los de $-P$ se llaman *números negativos*. Para $x, y \in \mathbb{R}$ se dice que $x < y$ (o que $y > x$) si $y - x \in P$ (la expresión $y - x$ denota $y + (-x)$). También se escribe $x \leq y$ (o $y \geq x$) si $y - x \in P$ o bien $y = x$. Por ejemplo, $x > 0$ significa que $x = x - 0 \in P$.

Del axioma anterior, puede comprobarse fácilmente que la suma de dos números negativos es un número negativo, el producto de dos números negativos es un número positivo, y el producto de un número positivo por uno negativo es un número negativo. En particular, para cada $x \in \mathbb{R}$ se tiene que $x^2 = x \cdot x \geq 0$. Por ejemplo, $1 = 1^2 > 0$.

Teorema. *Para $x, y, z \in \mathbb{R}$ se tiene*

a) $x < y,\ y < z \Rightarrow x < z$, (*propiedad transitiva*)
b) *exactamente una de las tres relaciones $x < y$, $x = y$ o $x > y$ es cierta*,
c) $x < y \Rightarrow x + z < y + z$ (*el orden es compatible con la suma*),
d) $x < y,\ z > 0 \Rightarrow xz < yz$ (*el orden es compatible con el producto*),
e) $x < y,\ z < 0 \Rightarrow xz > yz$,
f) $-1 < 0 < 1$,
g) $z > 0 \Rightarrow 1/z > 0$,
h) $0 < x < y \Rightarrow 0 < 1/y < 1/x$.

Demostración. a) Como $y - x, z - y \in P$, basta sumarlos (aplicando el axioma VII) para obtener $z - x \in P$, es decir, $x < z$. El apartado b) se sigue directamente del axioma VI. Los apartados c), d) y e) son triviales, y f) ya se ha visto. El apartado g) es fácil: como $z(1/z) = 1 > 0$, entonces z y $1/z$ tienen el mismo signo. Por último, para ver h), basta multiplicar por $1/(xy)$ en la desigualdad $0 < x < y$, ya que entonces se tiene $0 < 1/y < 1/x$. $\square$

El mismo teorema se puede reformular cambiando algunos $<$ por $\leq$. En particular, se tiene

Teorema. *Si $x, y, a, b \in \mathbb{R}$, entonces $x \leq y,\ a \leq b \Rightarrow x + a \leq y + b$.*

Demostración. Basta aplicar el partado c) del teorema anterior: $x + a \leq y + a \leq y + b$. $\square$

Este resultado puede escribirse como:

$$\left.\begin{array}{rcl} x & \leq & y \\ a & \leq & b \end{array}\right\} \Rightarrow x + a \leq y + b.$$

Se dice que las desigualdades se pueden *sumar* ordenadamente y se tienen otras desigualdades.

Departamento de Matemáticas
Universidad de Extremadura

Definición (valor absoluto). Para cada $x \in \mathbb{R}$ se define el *valor absoluto* de x como

$$|x| = \begin{cases} -x & \text{si} \quad x \leq 0, \\ x & \text{si} \quad x \geq 0. \end{cases}$$

De la definición es fácil deducir que $|x|$ es el mayor valor posible de x y $-x$. También es fácil comprobar que $|x| = |-x|$.

Lema. *Si* $x, a \in \mathbb{R}$, $a \geq 0$, *entonces*

$$|x| \leq a \iff -a \leq x \leq a.$$

Por ejemplo, $|x| \leq 1$ es lo mismo que decir $-1 \leq x \leq 1$.

Demostración. Las desigualdades $-a \leq x \leq a$ se pueden escribir de varias formas equivalentes:

$$\begin{cases} x \leq a \\ -a \leq x \end{cases} \iff \begin{cases} x \leq a \\ -x \leq a \end{cases} \iff |x| \leq a,$$

(en la última se utiliza que $|x|$ es el mayor de los dos valores x y $-x$). □

Teorema. *Para* $x, y \in \mathbb{R}$ *se tiene*

a) $|xy| = |x| \cdot |y|$,

b) $|x + y| \leq |x| + |y|$ *(conocida como desigualdad triangular)*,

c) $\big||x| - |y|\big| \leq |x - y|$.

Demostración. a) Basta aplicar la definición en los casos $x \leq 0$, $x \geq 0$, $y \leq 0$, $y \geq 0$.

Para ver b), se escribe $-|x| \leq x \leq |x|$, $-|y| \leq y \leq |y|$, y se suman (utilizando propiedades ya conocidas):

$$-(|x| + |y|) \leq x + y \leq |x| + |y|.$$

Por el lema anterior se termina la prueba.

Para ver c), se puede aplicar el apartado anterior, y se obtiene

$$|x| = |x - y + y| \leq |x - y| + |y|,$$

es decir

$$|x| - |y| \leq |x - y|.$$

Razonando de forma simétrica (intercambiando los papeles de x e y) se llega a

$$|y| - |x| \leq |y - x| = |x - y|.$$

En total,

$$\big||x| - |y|\big| \leq |x - y|,$$

que termina la demostración. □

Con todas estas propiedades se tienen consecuencias del tipo

$$|a + b + c - d| \leq |a + b| + |c - d|, \qquad |x - y| = |y - x|, \qquad \left|\frac{x}{y}\right| = \frac{|x|}{|y|}$$

Departamento de Matemáticas
Universidad de Extremadura

o similares, que suelen utilizarse con cierta frecuencia.

Estos siete axiomas definen un cuerpo ordenado con las operaciones compatibles con la suma y el producto. Sin embargo, el conjunto de números reales no es el único cuerpo que verifica estos axiomas anteriores. Por ejemplo, ya se verá que los números racionales forman un cuerpo que cumplen estos mismos axiomas. Y hay otros cuerpos que también los verifican (por ejemplo `https://en.wikipedia.org/wiki/Ordered_field`).

Lo que distingue a los números reales del resto de cuerpos ordenados es la completitud, que recoge el último axioma.

Axioma VIII (de completitud de Dedekind [matemático alemán, 1831–1916]). Si A y B son subconjuntos no vacíos de $\mathbb{R}$ que verifican $a < b$ para cada $a \in A$ y $b \in B$, entonces existe algún número $c \in \mathbb{R}$ que cumple

$$a \leq c \leq b$$

para todo $a \in A$ y $b \in B$.

Se puede utilizar también una variante equivalente de este axioma:

Axioma VIII'. Sean A y B subconjuntos de $\mathbb{R}$ que verifican

a) ambos son no vacíos, es decir, $A \neq \emptyset$ y $B \neq \emptyset$,
b) entre ambos rellenan todo $\mathbb{R}$, es decir, $A \cup B = \mathbb{R}$,
c) si $a \in A$ y $b \in B$ entonces $a < b$ (cualquier elemento de A es menor que cualquier elemento de B). En particular, deben ser disjuntos, es decir, $A \cap B = \emptyset$.

Entonces existe un único elemento $c \in \mathbb{R}$ que verifica

d) si $x \in \mathbb{R}$ y $x < c$ entonces $x \in A$, y
e) si $x \in \mathbb{R}$ y $c < x$ entonces $x \in B$.

Claramente ese elemento c debe estar en A o en B, pero no en ambos. Por tanto debe darse una de las dos alternativas: o bien $A = \{x \in \mathbb{R} : x \leq c\}$ y $B = \mathbb{R} \setminus A$, o bien $A = \{x \in \mathbb{R} : x < c\}$ y $B = \mathbb{R} \setminus A$.

Este axioma VIII' proviene del texto original de Dedekind, donde habla de la *continuidad de la recta real*: «Si todos los puntos de la recta se descomponen en dos clases tales que todo punto de la primera clase está a la izquierda de cada punto de la segunda clase, entonces existe un y sólo un punto que produce esta partición de todos los puntos en dos clases, este corte de la recta en dos partes».

Se admite la existencia de un conjunto $\mathbb{R}$ que verifica los axiomas I–VIII. En él son ciertas además todas las consecuencias de dichos axiomas.

Es posible también probar la existencia de un conjunto $\mathbb{R}$ verificando todas estas propiedades. Así lo hacen algunos autores y se pueden encontrar distintos libros que lo hacen de esta forma. Se parte de los números naturales, se construyen nuevos números, como los enteros, racionales,... Después se llega, mediante otro tipo de objetos –como sucesiones, por ejemplo–, a una clase más amplia de números, que son los números reales. Se demuestra que estos números verifican todas los axiomas I–VIII y sus consecuencias.

En este curso se verá que los números racionales $\mathbb{Q}$ y los números complejos $\mathbb{C}$ son cuerpos que cumplen sólo algunos de los axiomas anteriores. En la siguiente tabla se muestra un resumen de cuál es la situación.

	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
Axiomas I,...,V (cuerpo)	✓	✓	✓
Axiomas VI y VII	✓	✓	×
Axioma VIII (o VIII')	×	✓	×

Teorema fundamental del orden en $\mathbb{R}$ (el principio del supremo)

En este apartado se demostrará un resultado esencial de los números reales. Es el punto de partida de otras muchas propiedades de $\mathbb{R}$ que se obtienen como consecuencia.

Definición. Sea $E \neq \emptyset$ un subconjunto de $\mathbb{R}$. Se dice que $b \in \mathbb{R}$ es una *cota superior* de E si $x \leq b$ para todo $x \in E$. De forma simétrica, se dice que $c \in \mathbb{R}$ es una *cota inferior* de E si $c \leq x$ para todo $x \in E$.

Hay conjuntos, como $\mathbb{R}$, que no tienen cota superior ni cota inferior.

Se dice que E está acotado superiormente (resp. inferiormente) si tiene alguna cota superior (resp. inferior). En este caso tiene infinitas cotas superiores (resp. inferiores).

Definición. Si E es un conjunto acotado superiormente, se llama *supremo* de E a la menor de las cotas superiores. Se escribe $s = \sup E$, y verifica

a) s es cota superior de E, y
b) si b es otra cota superior de E, entonces $s \leq b$.

Es evidente E puede tener como mucho un supremo: en caso de tener varios deben coincidir por la definición, ya que solo uno de ellos será la menor cota superior.

El supremo de E puede entonces expresarse como el único número que cumple

x	$\leq$	s	$\leq$	b
elementos de E				cotas superiores de E

es decir, s es una cota superior de E y es menor o igual que todas las demás cotas superiores.

El *ínfimo* de un conjunto E se define similarmente como la mayor de las cotas inferiores. Se denota $\inf E$.

Si un conjunto está acotado superior e inferiormente, se dice que es un conjunto acotado.

Ejemplos: a) $E = \{x \in \mathbb{R} : x \geq 1\}$ tiene como cotas inferiores cualquier número menor o igual que 1. Su ínfimo es 1. No está acotado superiormente, y por tanto no tiene supremo.
b) $E = \{x \in \mathbb{R} : 0 < x \leq 1\}$ está acotado. Además $0 = \inf E$ y $1 = \sup E$. Tanto el ínfimo como el supremo pueden pertenecer o no al conjunto.

La existencia del supremo de cada conjunto acotado superiormente es una propiedad que tiene $\mathbb{R}$. Sin embargo, ya se verá que hay otro tipo de números, como los números racionales $\mathbb{Q}$, en los que ocurren hechos como estos:

a) $E = \{x \in \mathbb{Q} : x^2 < 2\}$ está acotado superiomente en $\mathbb{Q}$ pero no tiene supremo (en $\mathbb{Q}$), y

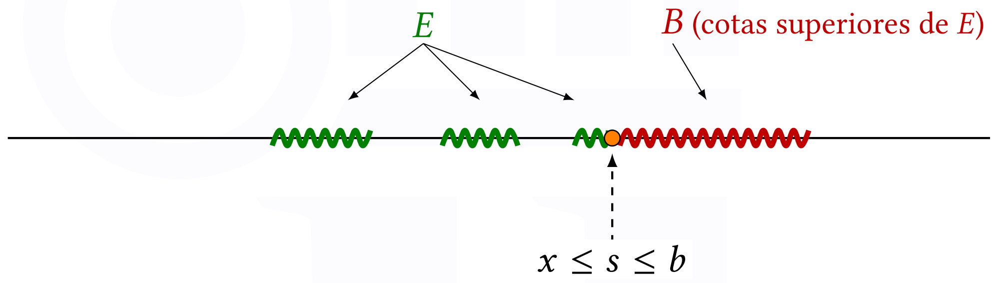
Departamento de Matemáticas
Universidad de Extremadura

b) $E = \left\{ \left(1 + \dfrac{1}{n}\right)^n \ : \ n = 1, 2, 3 \ldots \right\}$ está acotado superiomente en $\mathbb{Q}$ pero no tiene supremo (en $\mathbb{Q}$).

Teorema (fundamental del orden o principio del supremo). *Todo conjunto no vacío y acotado superiormente de números reales tiene supremo en* $\mathbb{R}$.

Este teorema dice que si $E \subset \mathbb{R}$, $E \neq \varnothing$ y E está acotado superiormente, entonces existe $\sup E \in \mathbb{R}$. No se garantiza que este supremo pertenezca a E. En algunos casos se tendrá $\sup E \in E$ y en otros no.

Demostración. Sea $E \subset \mathbb{R}$, $E \neq \varnothing$ y E acotado superiormente. Sea B el conjunto de las cotas superiores de E, que es no vacío por hipótesis. Si $x \in E$, $b \in B$, entonces $x \leq b$.



Se trata de ver que existe $s \in \mathbb{R}$ que verifica $x \leq s \leq b$ (para cada $x \in E$ y $b \in B$). Así se termina la demostración, ya que entonces s sería el supremo de E. Por supuesto, números que verifiquen $x \leq s \leq b$ (con $x \in E$ y $b \in B$) solo puede haber uno: si $x \leq s \leq b$ y $x \leq s' \leq b$, entonces ambos son cotas superiores de E, y así se tendría $s \leq s'$ y también $s' \leq s$.

Para probar la existencia de ese número s se hace lo siguiente:

a) Si $E \cap B \neq \varnothing$, entonces existe $s \in E \cap B$. Como $s \in B$ (es cota superior de E), entonces $x \leq s$ para todo $x \in E$. Como $s \in E$, se tiene $s \leq b$ para cada $b \in B$. En resumen, $x \leq s \leq b$ y por tanto $s = \sup E$.

b) Si $E \cap B = \varnothing$, entonces $x < b$ para todo $x \in E, b \in B$. El axioma VIII garantiza la existencia de un valor $s \in \mathbb{R}$ que verifica $x \leq s \leq b$ para $x \in E, b \in B$. La unicidad de este valor s ya se ha explicado más arriba. En consecuencia, $s = \sup E$. □

Ejemplos:

1) si $E = \{x \in \mathbb{R} : 0 < x < 1\} \cup \{2, 3\}$ entonces $B = \{x \in \mathbb{R} : 3 \leq x\}$ y $s = 3$.

2) si $E = \{\ldots, -9, -8, -7, -6\} \cup \{x \in \mathbb{R} : -5 < x < 1\}$ entonces $B = \{x \in \mathbb{R} : 1 \leq x\}$ y $s = 1$.

El mismo teorema puede enunciarse y demostrarse para la existencia de ínfimo de un conjunto acotado inferiormente. La demostración es idéntica (simétrica, más bien) haciendo los cambios oportunos de cota superior por inferior, supremo por ínfimo, …

Teorema. *Todo conjunto no vacío y acotado inferiormente de números reales tiene ínfimo en* $\mathbb{R}$.

A veces, probar que un número es el supremo de un conjunto (es decir, es cota superior y la menor de todas ellas) se puede simplificar utilizando un criterio muy útil, que recoge el siguiente resultado (y otro análogo para el ínfimo de un conjunto que se deja como ejercicio).

Teorema. *Sea $E \subset \mathbb{R}$ no vacío y $s \in \mathbb{R}$. Entonces*

$$s = \sup E \iff \begin{cases} \textbf{a)} & x \le s \text{ para cada } x \in E, \text{ es decir, } s \text{ es cota superior de } E, \text{ y} \\ \textbf{b)} & \text{para cada } \varepsilon > 0 \text{ existe algún } x \in E \text{ verificando } x > s - \varepsilon. \end{cases}$$

(El apartado **b**) dice que $s - \varepsilon$ no puede ser cota superior de E, ya que s es la menor de todas ellas).

La demostración del teorema es sencilla. La idea que subyace es la siguiente: si $s = \sup E$, ¿hay elementos $x \in E$ que verifiquen $s - \varepsilon < x \le s$? Si la respuesta fuese negativa, entonces s no sería la menor de las cotas superiores de E.

Con este criterio el cálculo del supremo se simplifica bastante. Por ejemplo, es evidente que $\sup\{1, 2, 3\} = 3$ y $\sup\{x \in \mathbb{R} : 0 \le x < 1\} = 1$.

¿Qué números hay en $\mathbb{R}$?

Hasta ahora se ha admitido la existencia de un conjunto $\mathbb{R}$ de números que verifican ciertos axiomas (del I al VIII) y varias propiedades que se derivan de ellos, como el teorema fundamental del orden. Los números reales se pueden sumar, multiplicar, y hay también operaciones inversas. Cada $x \in \mathbb{R}$ tiene un opuesto $-x$ y un inverso x^{-1} (siempre que $x \neq 0$). En todo este proceso anterior, de axiomas y propiedades de los números reales, han aparecido algunos números, como el 0 y 1, los elementos neutro de la suma e identidad del producto.

A partir de éstos, realizando operaciones, se obtienen números nuevos, como por ejemplo $1 + 1$, $1+1+1$,... y sus inversos y opuestos, por ejemplo $-(1+1)$ y $1/(1+1+1)$. Y las sumas y productos que puedan hacerse entre ellos. ¿Se llega así a encontrar todos los números reales? La respuesta a esta cuestión es negativa, como ya se verá más adelante. Y entonces cabe preguntarse, ¿hay alguna forma de encontrar todos los números reales?

Números naturales

Los números 1, $1 + 1$, $1 + 1 + 1$... se llaman números naturales. Se suelen escribir como $1, 2, 3$... Está claro que no se repiten nunca, ya que $1 < 1 + 1 < 1 + 1 + 1 < \dots$ El conjunto de todos ellos se denota mediante

$$\mathbb{N} = \{1,\ 2,\ 3, \dots\}.$$

Es un subconjunto de $\mathbb{R}$, y por tanto, como ya se ha visto, sobre esos números hay definidas dos operaciones, suma y producto, que verifican ciertas propiedades. Las operaciones suma y producto son cerradas en $\mathbb{N}$, es decir,

$$a, b \in \mathbb{N} \Rightarrow \begin{cases} a + b & \in & \mathbb{N}, \\ a \cdot b & \in & \mathbb{N}. \end{cases}$$

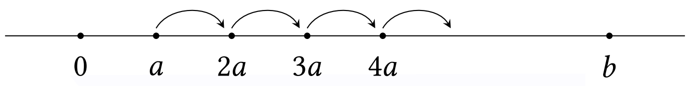
Sin embargo, los opuestos $-a$ de números naturales no son números naturales.

También hay un orden entre ellos, y se verifica la siguiente propiedad, conocida como propiedad arquimediana del orden.

Teorema (propiedad arquimediana). *Sean $a, b \in \mathbb{R}$ con $a > 0$. Entonces existe $n \in \mathbb{N}$ para el cual $na > b$. Equivalentemente, $\mathbb{N}$ no está acotado superiormente. O también, si $a, b > 0$, entonces para algún $n \in \mathbb{N}$ se tiene $a > b/n$.*

A veces este resultado se expresa en otro términos: para cualquier $a > 0$, el conjunto de sus múltiplos naturales $\{a, 2a, 3a, \dots\}$ no está acotado superiormente. Así, al elegir cualquier número b, debe haber uno de estos múltiplos de a que sea mayor: debe existir algún $na > b$.

Demostración. Se trata de ver que alguno de los números $a, 2a, 3a, 4a$... es mayor que b. Como muestra el dibujo, al ir dando pasos de tamaño a, en algún momento se sobrepasa a b.



Sea $E = \{na : n \in \mathbb{N}\}$, el conjunto de todos los múltiplos naturales de a. Se supone, por reducción al absurdo, que b es una cota superior de E, es decir, $na \leq b$ para todo $n \in \mathbb{N}$. Entonces se aplica el teorema fundamental del orden y existe $s = \sup E$. Un número que es cota superior de E y es la menor de todas ellas. Por ser el supremo, al considerar cualquier número menor que él, como por ejemplo $s - a$, debe existir $ma > s - a$. Por tanto $(m+1)a > s$ y se llega a un elemento de E mayor que s, lo que es imposible. □

Este teorema dice que dado cualquier número positivo $a \in \mathbb{R}$, sus múltiplos $a, 2a, 3a$... llegan a sobrepasar cualquier valor. En particular, tomando $a = 1$ se tiene que $\mathbb{N}$ no está acotado superiormente.

Números enteros

Los elementos del conjunto $\mathbb{Z} = \mathbb{N} \cup -\mathbb{N} \cup \{0\}$ se llaman números enteros. Es un conjunto de números reales formados por los números naturales, sus opuestos y el cero. Sobre ellos hay definidas operaciones suma y producto.

Puede comprobarse que si $a \in \mathbb{Z}$ entonces $-a \in \mathbb{Z}$. Además, las operaciones suma y producto son cerradas en $\mathbb{Z}$, es decir,

$$a, b \in \mathbb{Z} \Rightarrow \begin{cases} a + b & \in & \mathbb{Z}, \\ a \cdot b & \in & \mathbb{Z}. \end{cases}$$

[Por ejemplo, si $a, b \in \mathbb{Z}$ son ambos positivos, entonces $a+b \in \mathbb{Z}$ trivialmente. Y si $a \in \mathbb{N}, b \in -\mathbb{N}$ entonces $a, -b \in \mathbb{N}$ y $a + b = a - (-b)$ es diferencia de dos naturales: es un número natural o bien su opuesto lo es.]

Definición (potencias enteras de números reales). Sea $x \in \mathbb{R}$. Se definen

$$x^0 = 1, \; x^1 = x, \; x^2 = x \cdot x, \; x^3 = x \cdot x \cdot x, \; \dots$$

y en general $x^n = x \cdot \overset{n}{\ldots} \cdot x$ (producto de x repetidas unas n veces) para $n \in \mathbb{N}$. Suele escribirse también $x^{n+1} = x^n \cdot x$ para definir las potencias n-ésimas de x.

Para $x \neq 0$ y $n \in \mathbb{N}$ se define $x^{-n} = 1/x^n$. Con estas definiciones se tiene

Teorema. *Si $x, y \in \mathbb{R} \setminus \{0\}$ y $m, n \in \mathbb{Z}$, entonces*

a) $x^m x^n = x^{m+n}$,

b) $x^m y^m = (xy)^m$,

c) $(x^m)^n = x^{m \cdot n}$.

d) *Si $n > 0, x > 0, y > 0$, entonces* $\left[x < y \Leftrightarrow x^n < y^n\right]$.

Demostración. Es sencilla y basta aplicar la definición. Por ejemplo, en el apartado a), si m y n son ambos positivos se tiene

$$x^m x^n = (x \cdot \overset{m}{\smile\ldots} \cdot x) \cdot (x \cdot \overset{n}{\smile\ldots} \cdot x) = x \cdot \overset{m+n}{\smile\ldots} \cdot x = x^{m+n}.$$

Además,

$$x^m x^{-n} = x \cdot \overset{m}{\smile\ldots} \cdot x \cdot \frac{1}{x \cdot \overset{n}{\smile\ldots} \cdot x} = x \cdot \overset{m-n}{\smile\ldots} \cdot x = x^{m-n}.$$

Para los apartados b) y c) es similar. Para el apartado d) se puede hacer por ejemplo

$$\begin{aligned} x < y &\Rightarrow x^2 = xx < xy < yy = y^2 && \text{(y así } x^2 < y^2\text{)} \\ &\Rightarrow x^3 = xx^2 < xy^2 < yy^2 = y^3 && \text{(y así } x^3 < y^3\text{)} \\ &\Rightarrow \ldots \Rightarrow x^n < y^n \end{aligned}$$

para $n \in \mathbb{N}$. De la misma forma se demuestra que $x > y \Rightarrow x^n > y^n$ (el orden que tengan x e y es el que tienen todas sus potencias). □

Números racionales e irracionales

Se define el conjunto de números racionales como $\mathbb{Q} = \{p/q \ : \ p, q \in \mathbb{Z},\ q \neq 0\}$. Por ejemplo, en este conjunto se encuentran números como 4, ya que $4 = 4/1$, y también $-1/3$. Los números reales que no son racionales se llaman irracionales. Se denota mediante $\mathbb{I}$ al conjunto de tales números, es decir, $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$. También se puede expresar esto diciendo que $\mathbb{I}$ y $\mathbb{Q}$ son subconjuntos disjuntos de $\mathbb{R}$ que cumplen $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$ (cada número real es racional o irracional, pero no ambas cosas a la vez).

Ya se ha visto anteriormente que

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Como consecuencia,

$$a/b,\ c/d \in \mathbb{Q} \ \Rightarrow \begin{cases} \dfrac{a}{b} + \dfrac{c}{d} \in \mathbb{Q} \\ \dfrac{a}{b} \cdot \dfrac{c}{d} \in \mathbb{Q} \end{cases}$$

Además, si $a/b \in \mathbb{Q}$ es no nulo, entonces tiene inverso: $(a/b)^{-1} = b/a \in \mathbb{Q}$. Las operaciones suma y producto son cerradas en $\mathbb{Q}$ y verifican los axiomas I, II..., V. Se dice que $\mathbb{Q}$ es un (sub)cuerpo dentro de $\mathbb{R}$. Sin embargo, como se verá más adelante, hay números irracionales $x \in \mathbb{I}$ que verifican $x \cdot x \notin \mathbb{I}$. Esto dice que $\mathbb{I}$ no es un cuerpo.

Cada número racional puede escribirse de varias formas (es una consecuencia de las propiedades ya vistas). Por ejemplo,

$$\frac{2}{3} = \frac{2 \cdot 5}{3 \cdot 5} = \frac{10}{15} = \frac{4}{6} = \frac{-2}{-3} = \ldots,$$

y en general

$$\frac{a}{b} = \frac{a \cdot m}{b \cdot m}$$

para $m \in \mathbb{Z}$ no nulo. Esta propiedad tan simple permite comparar números racionales y establecer cómo es el orden entre ellos. Dados $a/b,\ c/d \in \mathbb{Q}$, se escribe

$$\frac{a}{b} = \frac{ad}{bd}, \qquad \frac{c}{d} = \frac{cb}{bd}$$

y así

$$\frac{a}{b} \leq \frac{c}{d} \Leftrightarrow \frac{ad}{bd} \leq \frac{cb}{bd} \Leftrightarrow \frac{ad-bc}{bd} \leq 0.$$

En particular,

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc.$$

El orden en el cuerpo $\mathbb{Q}$ de los números racionales es total: todos los números son comparables. Estos elementos se representan en una recta

Además, si $x, y \in \mathbb{Q}$ y $x < y$, entonces $(x+y)/2 \in \mathbb{Q}$ y se tiene

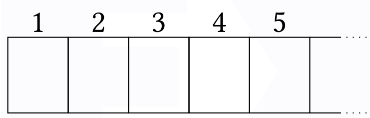
$$x < \frac{x+y}{2} < y.$$

Este razonamiento se puede repetir indefinidamente con cada pareja de números racionales: entre ellos siempre hay otro número racional. Todo esto da una ideal del tamaño que tiene $\mathbb{Q}$. Todos los conjuntos $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$ se representan en una recta. Una recta que aparentemente se rellena al ir colocando todos los números en ella. ¿Los números racionales ocupan la totalidad de la recta? La respuesta, que se verá más abajo, es no. Hay huecos en esa recta: nuevos números que no son racionales, aunque sí son reales.

El tamaño del conjunto de los números racionales puede resultar algo engañoso. Por definición, se llama *cardinal* de un conjunto al número de elementos que tiene. A finales del siglo XIX, el matemático G. Cantor amplió esta definición a conjuntos infinitos. Dos conjuntos tienen el mismo cardinal si existe una aplicación biyectiva entre ellos. Se llama conjunto numerable a cualquier conjunto con el mismo cardinal que $\mathbb{N}$, que se escribe $\operatorname{card}(\mathbb{N}) = \aleph_0$ ($\aleph$ es la letra «alef» o «aleph» hebrea, `http://es.wikipedia.org/wiki/Alef`). Un conjunto A es numerable si existe una aplicación biyectiva $f : \mathbb{N} \longrightarrow A$. Por ejemplo, el conjunto de números pares $A = \{2, 4, 6, \dots\} = \{2n : n \in \mathbb{N}\}$ es numerable, se escribe $\operatorname{card}(A) = \aleph_0$, y una aplicación biyectiva es

$$\begin{array}{rcl} f : \mathbb{N} & \longrightarrow & A \\ n & \rightsquigarrow & 2n. \end{array}$$

Un conjunto es numerable si sus elementos se pueden colocar en una fila infinita y numerada: hay elemento 1, un elemento 2, un elemento 3,…Los elementos de un conjunto numerable se pueden ir colocando de uno en uno dentro de las casillas del esquema siguiente:

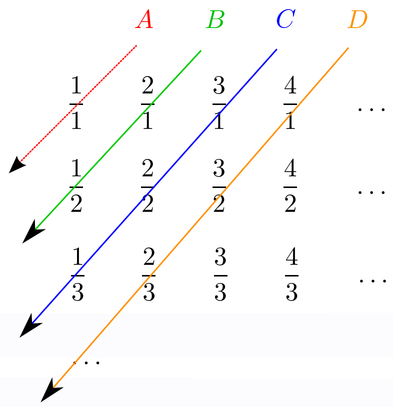


Una construcción así se conoce como «hotel de Hilbert», un hotel con infinitas habitaciones, la habitación nº 1, la nº 2...

De forma sencilla se puede comprobar también que $\operatorname{card}(\mathbb{Z}) = \aleph_0$. Sorprendentemente, también se tiene

$$\operatorname{card}(\mathbb{Q}) = \operatorname{card}(\mathbb{Z}) = \operatorname{card}(\mathbb{N}) = \aleph_0.$$

A veces se enuncia este hecho como un teorema: «$\mathbb{Q}$ es numerable». Para probarlo es suficiente saber colocar los elementos (de momento sólo se tratan los positivos) de $\mathbb{Q}$ en una fila numerada $1, 2, 3, \dots$ así:



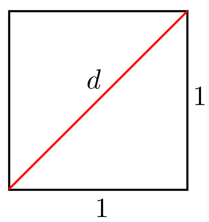
Según indica el dibujo, se van eligiendo los números de las diagonales $A, B, C, D, \ldots$ de forma ordenada

$$\frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \frac{2}{2}, \frac{1}{3}, \frac{4}{1}, \ldots$$

Los elementos de la diagonal A son las fracciones p/q con $p, q > 0$ y $p+q = 2$; los de la diagonal B son las fracciones p/q con $p, q > 0$ y $p + q = 3$, etcétera.

Este argumento de «diagonalización» (de Cantor) permite numerar conjuntos como $\mathbb{Q}$, aunque no es la única forma hacerlo. Para los números racionales negativos el mismo argumento muestra que se trata de un conjunto numerable. Por último, es fácil concluir que el conjunto $\mathbb{Q}$ de los números racionales, tanto los positivos como negativos, es numerable.

Sin embargo, a pesar que $\mathbb{Q}$ es infinito y que sus elementos están por todas partes al representarlos en la recta, su tamaño no es lo suficientemente grande como para rellenar esa recta completamente.



La diagonal de un cuadrado de lado 1 es un número que no puede escribirse como una fracción. Según el teorema de Pitágoras, $d^2 = 1^2 + 1^2 = 2$, es un número cuyo cuadrado es 2 y se escribe $d = \sqrt{2}$. Este número no es racional.

Teorema. *Si $p/q \in \mathbb{Q}$ entonces $(p/q)^2 \neq 2$. En otras palabras, no hay ningún número racional cuyo cuadrado sea 2. O tambien: $\sqrt{2}$ no es racional.*

Demostración. Por reducción al absurdo, se supone que d es racional, es decir, existen p, q enteros positivos tales que $d = p/q$ y cuyo cuadrado sea 2. Además, se elige la fracción p/q irreducible, es decir, p y q primos entre sí o también $\text{mcd}(p, q) = 1$.

Como $(p/q)^2 = 2$ entonces $2 = p^2/q^2$ y así $p^2 = 2q^2$ es un número par. Entonces p es par y entonces p^2 es múltiplo de 4. Luego $2q^2$ es múltiplo de 4 y así q^2 debe ser par, lo que obliga a que q sea par. Se llega a una contradicción: p y q son pares. □

Este número d no es racional. Es otro tipo de número. De él se conoce que verifica $d^2 = 2$, que suele escribirse como $d = \sqrt{2}$, y que no es una fracción. Se puede ir aproximando qué número debe ser sabiendo que su cuadrado es 2. Este proceso no es difícil. Se trata de ir comprobando qué cifras se pueden ir añadiendo para que al elevar al cuadrado salgan cantidades menores que 2 y cada vez más cercanas a 2. Se obtienen números

$$1 \quad 1.4 \quad 1.41 \quad 1.414 \quad 1.4142\ldots$$

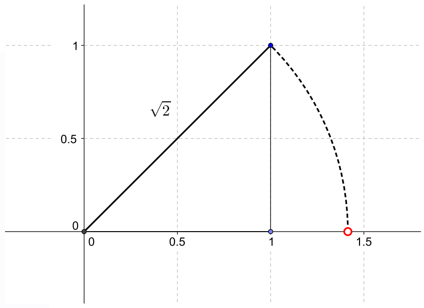
cuyos cuadrados son menores que 2, aunque cada vez se aproximan más a 2. Este proceso se puede hacer con el algoritmo de la raíz cuadrada. En el caso del cálculo de $\sqrt{2}$ es así:

$$
\begin{array}{r|l}
\sqrt{2} & \mathbf{1}.41 \\
-1 & \\
\hline
100 & 24 \times \mathbf{4} = 96 \\
-96 & \\
\hline
400 & 281 \times \mathbf{1} = 281 \\
-281 & \\
\hline
119 &
\end{array}
$$

y se van obteniendo los términos de la sucesión $(1, 1.4,\ 1.41,\ 1.414,\ 1.4142,\ \ldots)$ que representa (este concepto habrá que precisarlo más) a $\sqrt{2}$.

Ejercicio. Los conjuntos $A = \{x \in \mathbb{Q} : x \geq 0,\ x^2 < 2\}$ y $B = \{x \in \mathbb{Q} : x \geq 0,\ x^2 > 2\}$ verifican $a < b$ para cada $a \in A,\ b \in B$. Sin embargo no hay ningún elemento $c \in \mathbb{Q}$ que verifique $a \leq c \leq b$ para $a \in A,\ b \in B$. La idea es la siguiente: si fuera $c \in A$, entonces se puede encontrar $m \in \mathbb{N}$ que verifique $(c + 1/m)^2 < 2$, y así c no sería mayor que todos los elementos de A. El mismo razonamiento dice que c tampoco está en B. El teorema anterior descarta también la posibilidad de que $c^2 = 2$. Este número $c \in \mathbb{Q}$ no existe.

Esta cantidad $\sqrt{2}$ representa un «agujero» en el sistema de números racionales. Se habla de cantidades inconmensurables, como la diagonal del cuadrado y su lado.



Los números reales $\mathbb{R}$ se construirán a partir de los racionales como números que pueden ser aproximados en un sentido que se explicará más adelante. Esta idea de números que se consiguen mediante aproximación es el motivo por el que aparecen sucesiones de números racionales.

Otros números no racionales conocidos (y algunos no tan conocidos) son

- π, la constante descubierta por Euclides que indica la proporción entre la longitud de una circunferencia y su diámetro. Su valor es $\pi = 3.141593...$ y se conocen miles de millones de cifras decimales. La irracionalidad de π la probó J.H. Lambert en el siglo XVIII. Más tarde, en el siglo XIX, F. Lindemann demuestra que se trata de un número trascendente, es decir, que no es raíz de ningún polinomio con coeficientes enteros. Este último hallazgo se expresa como «la imposibilidad de cuadrar el círculo». Hay muchas expresiones cuyo resultado está relacionado con él, como por ejemplo

$$\frac{\pi^2}{6} = \sum_{n=1}^{\infty} \frac{1}{n^2}, \qquad \frac{\pi}{4} = \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} = 1 - \frac{1}{3} + \frac{1}{5} + \ldots$$

- e, la base de los logaritmos neperianos, cuyo valor es $e = 2.71828182...$ y que verifica

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} = \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n = 2.718281828459045\ldots$$

- $a = 0.10100100010000\ldots$, un número cuya expresión decimal ni es finita ni es periódica.
- $u = 0.123456789101112\ldots$, un número que contiene en su expresión decimal cualquier número natural. Por ejemplo, es este número aparecen todos los números de teléfono de todos los alumnos de esta universidad. Si se codifican las letras del alfabeto mediante

Departamento de Matemáticas
Universidad de Extremadura

números, por ejemplo, $a = 23, b = 24, \ldots, A = 70, B = 71, \ldots$, espacio $= 99, \ldots$, en la expresión de u aparece la palabra «Baba» (el apellido –sin tilde– del famoso personaje del cuento de los ladrones), y aparece infinitas veces. Esta palabra es, después de la codificación, 71232423.

De la misma forma, cualquier texto conocido, como «El Quijote» o «La Ilíada y la Odisea» aparecen en la expresión decimal de u. Y también cualquier variación suya, como por ejemplo alguna versión que tenga algunos errores de escritura, o la versión escrita al revés, las letras en orden inverso. También está cualquier periódico de mañana, los mensajes que se vayan a escribir en el móvil dentro de dos días,... Incluso se podría pensar en hallar todas estas cosas en alguna versión finita de u, ya que todos estos números de los que se ha hablado están acotados.

El escritor Borges, en su relato «La Biblioteca de Babel» hace un juego similar sobre una biblioteca un tanto especial y los libros que puede contener.

Aparecen nuevos problemas aparentemente simples como «¿qué número es $u+u$?», entendiendo que $2u$ no es la respuesta esperada.

Resulta curioso que no se sepa si números como la constante γ de Euler, $\pi + e$, π/e, o $\log \pi$ son racionales o irracionales.

Representación decimal de los números reales

Los números naturales $\mathbb{N} = \{1, 2, 3. \ldots\}$ se pueden escribir con diez signos $0, 1, 2, \ldots, 9$ utilizando la notación posicional. Si se añaden el 0 y los opuestos se obtienen los números enteros $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. Los números racionales son parejas p/q de números enteros. Para expresar una fracción como un número decimal se hace la división. Por ejemplo

$$\begin{array}{l|l} 11 & 8 \\ \cline{2-2} \;\;30 & 1.375 \\ \;\;\;\;60 & \\ \;\;\;\;\;\;40 & \\ \;\;\;\;\;\;\;\;0 & \end{array}$$

indica que $11/8 = 1.375$. Similarmente,

$$\begin{aligned} 1/3 &= 0.333\ldots = 0.\widehat{3} \\ 29/30 &= 0.9\widehat{6} \\ 4/7 &= 0.571428571428571428571\ldots = 0.\widehat{571428}. \end{aligned}$$

Cada número racional se escribe como un número decimal cuya expresión es finita o se repite a partir de un cierto lugar (se llaman estas últimas expresiones decimales periódicas). Esto es evidente, ya que al hacer la división, por ejemplo con 8 como divisor, se van obteniendo restos menores que 8. En el ejemplo anterior salen como restos 3, 6, 4, 0. Estos restos son todos números menores que 8, luego o bien alguno se repite o bien aparece el valor 0 en algún momento. En cualquier caso la división da como resultado un número decimal finito o periódico.

Y a la inversa, dada una expresión decimal periódica o finita, hay un número racional que coincide con ella. Por ejemplo, si $a = 9.83$ entonces $a = 983/100$ y si $a = 3.274747474\ldots = 3.2\widehat{74}$ entonces se puede hacer:

$$a = 3.2\widehat{74} \Rightarrow \left\{ \begin{aligned} 10a &= 32.\widehat{74} \\ 1000a &= 3274.\widehat{74} \end{aligned} \right\} \Rightarrow 990a = 3274 - 32 \Rightarrow a = \frac{3274-32}{990} = \frac{3242}{990}.$$

Hay una correspondencia biyectiva entre números racionales y expresiones decimales periódicas o finitas, entendiendo que hay expresiones que son iguales aunque se escriben de distinta forma: $1.2\widehat{9} = 1.3$ o también $4.1 = 4.0\widehat{9}$ y $1 = 0.\widehat{9}$.

Las expresiones decimales no periódicas no son números racionales, aunque se pueden aproximar por expresiones periódicas o finitas tanto como se quiera. Por ejemplo,

$$\begin{aligned} \sqrt{2} &= 1.4142135623730950488\ldots \\ \pi &= 3.14159265358979323846\ldots \end{aligned}$$

Un infinito «más grande». El cardinal de $\mathbb{R}$.

Ya se ha visto la definición de conjunto numerable: se dice que un conjunto es numerable si existe una aplicación biyectiva entre él y $\mathbb{N}$. En otras palabras, un conjunto es numerable si puede «numerarse», etiquetar sus elementos como primero, segundo, tercero,...

Los conjuntos $\mathbb{N}$, $P = \{2, 4, 6, 8, \ldots\}$, $\mathbb{Z}$, e incluso $\mathbb{Q}$, son numerables. Este último puede explicarse mediante el proceso diagonal de Cantor. Otra forma de expresar este proceso de diagonalización consiste en dividir $\mathbb{Q}^+$ (de momento sólo se consideran los racionales positivos) en conjuntos finitos e ir numerando sus elementos. Se consideran los conjuntos $A_n = \{p/q \in \mathbb{Q}^+ : p + q = n\}$, que recubren $\mathbb{Q}^+$ y se empiezan a numerar los elementos de A_1, los de A_2,... eliminando los elementos redundantes (las fracciones equivalentes como $3/4 \in A_7$ y $6/8 \in A_{14}$.

Teorema. $\mathbb{R}$ *no es numerable.*

Demostración. Por reducción al absurdo se supone que sí lo es: existe una aplicación biyectiva $\varphi : \mathbb{N} \longrightarrow \mathbb{R}$. Así, todos los elementos de $\mathbb{R}$ se pueden escribir como $\mathbb{R} = \{\varphi(1), \varphi(2), \varphi(3), \ldots\}$. Se escribe la expresión decimal de cada uno de ellos

$$\begin{array}{rcl} \varphi(1) & = & a\,.\,a_1\,a_2\,a_3\ldots \\ \varphi(2) & = & b\,.\,b_1\,b_2\,b_3\ldots \\ \varphi(3) & = & c\,.\,c_1\,c_2\,c_3\ldots \\ & \ldots & \end{array}$$

La idea de la demostración es encontrar un número real que no esté en esa lista. Esto es una contradicción, ya que en esa lista están *todos* los números reales.

Se define un nuevo número real con expresión decimal $\alpha.\alpha_1\,\alpha_2\,\alpha_3\ldots$ donde

– α es cualquier valor, por ejemplo $\alpha = 93$,

– su primera cifra decimal es distinta a la primera cifra decimal de $\varphi(1)$: $\alpha_1 \neq a_1$,

– su segunda cifra decimal es distinta a la segunda cifra decimal de $\varphi(2)$: $\alpha_2 \neq b_2$,

– su tercera cifra decimal es distinta a la tercera cifra decimal de $\varphi(3)$: $\alpha_3 \neq c_3$,

– etcétera

Se consigue entonces un número que no puede ser ninguno de la lista $\varphi(1), \varphi(2), \varphi(3), \ldots$ En efecto, no puede ser igual a $\varphi(1)$ por tener la primera cifra decimal distinta; no puede ser igual a $\varphi(2)$ por tener la segunda cifra decimal distinta, y así con todos los demás. Esto representa una contradicción. Luego $\mathbb{R}$ no es numerable. □

Departamento de Matemáticas
Universidad de Extremadura

Así $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$, aunque los tres primeros tienen el mismo cardinal, son numerables. El cardinal de $\mathbb{R}$ es estrictamente mayor: $\aleph_0 = \text{card}(\mathbb{N}) = \text{card}(\mathbb{Z}) = \text{card}(\mathbb{Q}) < \text{card}(\mathbb{R})$.

El cardinal de $\mathbb{R}$ es mucho más grande que el de los conjuntos numerables (puede verse en las hojas de ejemplos y ejercicios resultados sobre esta afirmación). Como $\text{card}(\mathbb{N}) < \text{card}(\mathbb{R})$ y la diferencia entre ambos cardinales es tan grande, cabe preguntarse si existe algún conjunto intermedio. ¿Es posible encontrar (o al menos probar su existencia) un conjunto D que verifique $\text{card}(\mathbb{N}) < \text{card}(D) < \text{card}(\mathbb{R})$?

El teorema de Gödel-Cohen prueba que esta cuestión es un *indecidible*: no hay un sí o un no como respuesta a este problema. Con otras palabras, es imposible probar la falsedad o verdad sobre la existencia de dicho conjunto D con cardinal intermedio entre el de $\mathbb{N}$ y el de $\mathbb{R}$.

Suponer que tal conjunto D no puede existir se llama «hipótesis del continuo», es decir, el primer cardinal no numerable es el de $\mathbb{R}$, un conjunto «continuo»: una recta sin agujeros.

Se puede probar sin dificultad que el producto finito de conjuntos numerables, como $\mathbb{Q} \times \mathbb{Q}$, es numerable. También es numerable la unión numerable de conjuntos numerables. En general, dos conjuntos tienen el mismo cardinal si existe una aplicación biyectiva entre ellos. Esto hace que todos los intervalos (abiertos o cerrados) en $\mathbb{R}$ tienen el mismo cardinal que el de $\mathbb{R}$. Además $\mathbb{R}$ y $\mathbb{R}^2$ tienen el mismo cardinal, que hizo expresar a Cantor esa frase «lo veo pero no lo creo».

Los números reales se pueden dividir además en algebraicos y trascendentes. Los algebraicos son aquellos que son raíz de algún polinomio con coeficientes enteros, como $\sqrt{2}$ que es raíz de $x^2 - 2$. Los que no son raíz de tales polinomios se llaman trascendentes. No es complicado probar que los números algebraicos forman un conjunto numerable. Esto quiere decir que la mayoría de números reales son trascendentes. Cuando se escribe

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{I} = \mathbb{A} \cup \mathbb{T}$$

se indica que los números reales son racionales o irracionales, algebraicos o trascendentes. La mayoría de ellos son irracionales y trascendentes.

Otras propiedades de $\mathbb{R}$

El teorema fundamental del orden es el origen de muchas propiedades sobre los números reales. Incluso hay resultados equivalentes a este teorema fundamental del orden. Quizás el hecho de que $\mathbb{R}$ es completo tiene especial importancia: toda sucesión de Cauchy en $\mathbb{R}$ es convergente, que se verá más adelante.

En el cuerpo $\mathbb{Q}$ de los números racionales hay números positivos que no tienen raíz cuadrada. Ya se ha visto que $2 \in \mathbb{Q}$ es uno de estos números. Sin embargo, en $\mathbb{R}$ esto no es posible para los números positivos. El resultado siguiente dice que cualquier número real positivo $a \in \mathbb{R}$ tiene (y es un número real positivo) raíz cuadrada positiva, raíz cúbica positiva,...

Otra cuestión son las raíces de números reales negativos. En $\mathbb{R}$ la ecuación $x^2 = -1$ no tiene solución, es decir, -1 no tiene una raíz cuadrada que sea un número real. Se necesitan conocer otros números para hablar de raíces de números reales negativos.

Lema. *Si* $n \in \mathbb{N}$ *y* $0 < \varepsilon < 1$, *entonces* $(1 + \varepsilon)^n < 1 + 3^n \varepsilon$.

Demostración (por inducción). Para $n = 1$ es evidente. Se supone que la desigualdad es cierta para n y entonces

$$\begin{aligned}(1+\varepsilon)^{n+1} &= (1+\varepsilon)(1+\varepsilon)^n < (1+\varepsilon)(1+3^n\varepsilon) = 1+\varepsilon(1+3^n+3^n\varepsilon) \\ &< 1+\varepsilon(3^n+3^n+3^n) = 1+3^{n+1}\varepsilon\end{aligned}$$

y se termina la prueba. □

Teorema. *Todo número real positivo tiene una única raíz real positiva de cualquier orden, es decir,*

$$\forall a \in \mathbb{R}^+,\ \forall n = 2,3,\ldots \quad \dot{\exists}\, d \in \mathbb{R}^+ \ :\ d^n = a.$$

Se dice que $d = \sqrt[n]{a}$, la raíz n-ésima de a. Con esta notación, el enunciado del teorema puede ser «para cada número real positivo a, existen $\sqrt{a}$, $\sqrt[3]{a}$, $\sqrt[4]{a}$ ...». En particular, $\sqrt{2}$ es un número real.

Demostración. Sean $a \in \mathbb{R}^+$ y $n \in \{2,3,4,\ldots\}$. Se trata de encontrar un número real d positivo que cumpla $d^n = a$. La unicidad de un número que cumpla $d^n = a$ es evidente: si $d^n = a$ y $f^n = a$, entonces $d^n = f^n$ y por tanto $d = f$.

El conjunto $A = \{x \in \mathbb{R} : x^n < a\}$ es no vacío pues $0 \in A$. Además está acotado superiormente: por la propiedad arquimediana se elige $m \in \mathbb{N}$ que verifique $a < m$. Así, para cada $x \in A$ se tiene $x^n < a < m < m^n$ y entonces $x < m$. Esto dice que m es una cota superior de A.

Por el teorema fundamental del orden existe $d = \sup(A)$. Como el orden en $\mathbb{R}$ es total, se tiene que dar uno de los tres casos: $d^n < a$, $d^n = a$ o bien $d^n > a$. Por reducción al absurdo se trata de probar que sólo el segundo caso puede ser posible.

Si se supone que $d^n < a$ entonces es posible encontrar un $\varepsilon > 0$ pequeño que verifique $d^n(1+\varepsilon)^n < a$. [Esto se consigue utilizando el lema anterior $d^n(1+\varepsilon)^n < d^n(1+3^n\varepsilon) < a$ si $\varepsilon < (a/d^n - 1)/3^n$.] Como $(d(1+\varepsilon))^n < a$, entonces $d(1+\varepsilon) \in A$, y es mayor que d, que no es posible.

Si fuera $d^n > a$, entonces se elige un $\varepsilon > 0$ pequeño que verifique $a < \big(d/(1+\varepsilon)\big)^n$. [Esto es posible utilizando el lema anterior $\big(d/(1+\varepsilon)\big)^n > d^n/(1+3^n\varepsilon) > a$ si $\varepsilon < (d^n/a-1)/3^n$.] Como $d/(1+\varepsilon) < d$ y $d = \sup(A)$, existe un elemento $x \in A$ que verifica $d/(1+\varepsilon) < x \leq d$. Por tanto $x^n > a$ y se llega a un absurdo.

En total, $d^n = a$. □

Como consecuencia del teorema se tiene además $\sqrt[n]{a}\ \sqrt[n]{b} = \sqrt[n]{a\,b}$ para $a, b \geq 0$. Esto es fácil de ver a partir de la igualdad

$$\left(\sqrt[n]{a}\ \sqrt[n]{b}\right)^n = \left(\sqrt[n]{a}\right)^n \left(\sqrt[n]{b}\right)^n = a\,b,$$

y de la unicidad de la raíz n-ésima.

Julius Wilhelm Richard **Dedekind** (Alemania, 1831–1916)
Georg Ferdinand Ludwig Philipp **Cantor** (Rusia, 1845–1918)
David **Hilbert** (Alemania, 1862–1943)