1. Números reales

Análisis de Variable Real

2014–2015

Resumen

Explicamos las propiedades de las diferentes clases de números reales. También realizamos una presentación axiomática de las propiedades de los números reales. De los axiomas de partida, incidimos especialmente en el llamado *Propiedad del Supremo*, que diferencia a la clase de los números reales de todas las demás, y que contiene en esencia el concepto de límite, central en Análisis Matemático.

Índice

1. Sistemas numéricos

1.1. Números naturales. Principio de Inducción

¿Qué son los números naturales?

Los números $1, 2, 3, \ldots$, reciben el nombre de *números naturales*. Con ellos se realizan dos operaciones: la *suma* de números naturales y el *producto* de números naturales, que dan como resultado otro número natural perfectamente definido. Para dos números naturales cualesquiera m y n, su suma suele representarse por $m + n$ y su producto por $m \cdot n$ o mn (si no hay lugar a confusión). Si denotamos con $\mathbb{N}$ el conjunto de todos los números naturales, podemos pensar en la suma y el producto como aplicaciones del producto cartesiano $\mathbb{N} \times \mathbb{N}$ en $\mathbb{N}$:

$$\begin{aligned} +\colon \mathbb{N} \times \mathbb{N} &\longrightarrow \mathbb{N} \\ (m,n) &\longmapsto m+n, \end{aligned} \qquad \begin{aligned} \cdot\colon \mathbb{N} \times \mathbb{N} &\longrightarrow \mathbb{N} \\ (m,n) &\longmapsto m\cdot n. \end{aligned}$$

Propiedades algebraicas de los naturales

A continuación describimos las propiedades fundamentales de estas operaciones (m, n, p representan números naturales cualesquiera):

- Propiedad *asociativa* de la suma: $(m + n) + p = m + (n + p)$.
- Propiedad *conmutativa* de la suma: $m + n = n + m$.
- Propiedad *asociativa* del producto: $(mn)p = m(np)$.
- Propiedad *conmutativa* del producto: $mn = nm$.
- Elemento *neutro* (o *unidad*) del producto: Hay un número natural, que denotamos por 1, tal que $n \cdot 1 = n$, cualquiera que sea n.
- Propiedad *distributiva* del producto respecto de la suma: $m(n+p) = mn + mp$.

Orden de los naturales

Se puede asimismo comparar el tamaño de dos números naturales cualesquiera y establecer de esta manera una relación de orden en $\mathbb{N}$. Suele escribirse $m \leqslant n$ para indicar que m es *menor o igual* que n (o, lo que es lo mismo, que n es *mayor o igual* que m, lo que también se escribe $n \geqslant m$).

Orden estricto

Definición 1.1. m es *estrictamente menor* (o simplemente *menor*) que n si $m \leqslant n$ y $m \neq n$. Lo denotamos $m < n$.

- Esto es lo mismo que decir que $n > m$, que se lee "n es *estrictamente mayor* (o simplemente *mayor*) que m."

Propiedades del orden

Esta relación de orden cumple las siguientes propiedades (m, n, p representan números naturales cualesquiera):

- Propiedad *reflexiva*: $m \leqslant m$.
- Propiedad *antisimétrica*: Si $m \leqslant n$ y $n \leqslant m$, entonces $m = n$.
- Propiedad *transitiva*: Si $m \leqslant n$ y $n \leqslant p$, entonces $m \leqslant p$.
- Propiedad de *orden total*: Siempre es $m \leqslant n$ o $n \leqslant m$.

Observación. La ordenación de $\mathbb{N}$ no es independiente de la suma y el producto. Podemos encontrar la siguiente relación: Para dos números naturales m, n se tiene $m > n$ si y solo si $m = n+p$ para algún número natural p. En este caso, al número p se le denomina *resta* o *diferencia* de m y n y se denota $p = m - n$.

Buena ordenación

Una propiedad, fundamental como veremos, que diferencia a los números naturales de los demás conjuntos de números, es la siguiente:

Teorema 1.2 (Principio de Buena Ordenación)**.** *Todo conjunto no vacío de números naturales posee un elemento mínimo, es decir, dado $S \subset \mathbb{N}$ no vacío, existe un elemento n_0 en S tal que $n_0 \leqslant n$ para todo $n \in S$.*

Ejemplos.

- El conjunto $\{3, 5, 7\}$ tiene por primer elemento el 3. No es demasiado sorprendente, ya que se trata de un conjunto finito. También tiene por último elemento al 7.
- El conjunto $\{\, n \in \mathbb{N} \mid n \text{ es par} \,\}$, que es infinito, tiene por primer elemento el 2, pero no tiene último elemento.

Principio de Inducción Matemática

A partir de esta última propiedad, se puede demostrar la siguiente, que es un instrumento particularmente útil:

Teorema 1.3 (Principio de Inducción Matemática)**.** *Dado $S \subset \mathbb{N}$ tal que*

(I) $1 \in S$,

(II) $n + 1 \in S$, *siempre que* $n \in S$,

entonces $S = \mathbb{N}$.

Demostración. La estrategia de nuestro argumento será una demostración por reducción al absurdo. Supongamos que se cumplen las dos hipótesis del enunciado pero $S \neq \mathbb{N}$. Sea

$$S^c = \mathbb{N} \setminus S.$$

Entonces S^c no es vacío y el Principio de Buena Ordenación (Teorema 1.2) garantiza la existencia de un elemento $m \in S^c$ que es el primer elemento de S^c. Como, por (I), $1 \in S$, resulta que $1 \notin S^c$, de modo que $m > 1$. Se sigue que $m - 1$ es también un número natural, y como m es el mínimo elemento de S^c, tendremos que $m - 1 \notin S^c$.

Pero entonces deberá ser $m - 1 \in S$. Aplicamos ahora (II), con lo que se obtiene que $m \in S$. Pero esto implica que $m \notin S^c$, lo que contradice la definición de m. □

Enunciado práctico del P. de Inducción Matemática

El Principio de Inducción 1.3 admite una forma alternativa en que, en lugar de hablar de un subconjunto de números naturales, hacemos alusión a una propiedad P_n que puede ser cierta o falsa para cada número natural n.

Teorema 1.4 (Principio de Inducción Matemática)**.** *Dada una propiedad P_n tal que*

(I) *P_1 es cierta,*

(II) *P_{n+1} es cierta, siempre que P_n es cierta,*

entonces P_n es cierta para todo $n \in \mathbb{N}$.

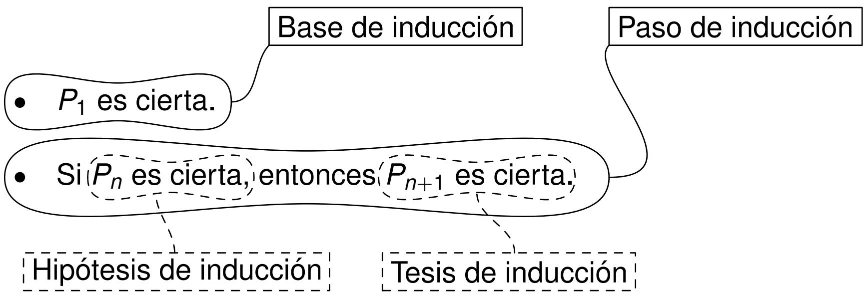
Dominó e inducción

Podemos comprender perfectamente el Principio de Inducción Matemática, si nos lo imaginamos de la manera siguiente: Supongamos que las propiedades P_1, P_2, P_3, etc., son unas fichas de dominó colocadas en fila, una detrás de otra, e imaginémonos que ocurren las dos siguientes cosas:

- Empujamos la primera ficha P_1, haciéndola caer.
- Las fichas están suficientemente cerca unas de otras, de forma que si una de ellas, P_n, cae, entonces lo hace sobre la siguiente P_{n+1}, derribándola también.

¿Qué podemos deducir en estas condiciones? Evidentemente, todas las fichas que hemos colocado en fila acaban por caer.

Partes de una demostración por inducción



En una demostración por inducción podemos distinguir dos partes, que tenemos que probar por separado:

- Primero probamos que "P_1 es cierta". Esta parte se denomina *base de inducción*.
- En segundo lugar probamos que "Si P_n es cierta, entonces P_{n+1} es cierta". Esta segunda parte se denomina *paso de inducción*. A su vez, aquí se pueden distinguir dos partes:
  - La suposición de que P_n es cierta es conocida como *hipótesis de inducción*.
  - La frase "P_{n+1} es cierta", que es a la que debemos llegar, se denomina *tesis de inducción*.

Ejemplos.

- Probar que $1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n+1)$ para todo $n \in \mathbb{N}$.

Solución. Sea P_n la proposición

$$1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n+1).$$

Entonces P_1 afirma que $1 = \frac{1}{2} \cdot 1(1+1)$, P_2 afirma que $1+2 = \frac{1}{2} \cdot 2(2+1)$, y así sucesivamente. En particular, vemos que P_1 es cierta, y esto establece la base de nuestra inducción.

Para verificar el paso de inducción, suponemos que se cumple P_n para un cierto $n \in \mathbb{N}$ arbitrario. Esto es, supongamos que

$$1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n+1).$$

Como queremos concluir que P_{n+1} es cierta, añadimos $n+1$ a ambos miembros, obteniendo

$$\begin{aligned} 1 + 2 + 3 + \cdots + n + (n+1) &= \frac{1}{2}n(n+1) + (n+1) \\ &= \frac{1}{2}[n(n+1) + 2(n+1)] \\ &= \frac{1}{2}(n+1)(n+2) \\ &= \frac{1}{2}(n+1)[(n+1)+1]. \end{aligned}$$

Así que P_{n+1} es cierta siempre que P_n es cierta y, por el Principio de Inducción Matemática, concluimos que P_n es cierta para todo n. □

- Probar que $7^n - 4^n$ es múltiplo de 3, para todo $n \in \mathbb{N}$.

  Solución. Claramente, esto es cierto para $n = 1$, ya que $7^1 - 4^1 = 3$. Si suponemos que $7^n - 4^n$ es múltiplo de 3, entonces $7^n - 4^n = 3m$ para algún $m \in \mathbb{N}$. Se sigue que

$$\begin{aligned} 7^{n+1} - 4^{n+1} &= 7^{n+1} - 7 \cdot 4^n + 7 \cdot 4^n - 4 \cdot 4^n \\ &= 7(7^n - 4^n) + (7-4)4^n \\ &= 7 \cdot 3m + 3 \cdot 4^n \\ &= 3(7m + 4^n). \end{aligned}$$

  Como m y n son números naturales, también lo es $7m + 4^n$. Por tanto, $7^{n+1} - 4^{n+1}$ también es un múltiplo de 3, y por inducción concluimos que $7^n - 4^n$ es múltiplo de 3 para todo $n \in \mathbb{N}$. □

Principio de Inducción Completa

A partir del Principio de Inducción Matemática, podemos obtener la siguiente variante, que resulta de aplicación más general, como veremos en el ejemplo posterior.

Teorema 1.5 (Principio de Inducción Completa)**.** *Dada una propiedad P_n tal que*

(I) P_1 *es cierta,*

(II) P_{n+1} *es cierta, siempre que* P_1*,* P_2*,* $\ldots$*,* P_n *son ciertas,*

entonces P_n *es cierta para todo* $n \in \mathbb{N}$*.*

Demostración. Para todo $n \in \mathbb{N}$, consideremos la proposición

$$Q_n \equiv \text{“}P_1, P_2, \ldots, P_n \text{ son ciertas”},$$

y apliquemos el Principio de Inducción Matemática 1.4.

Evidentemente, Q_1 es cierta, ya que Q_1 dice lo mismo que P_1. Probemos ahora el paso de inducción. Supongamos para ello que Q_n es cierta. Entonces, P_1, P_2, $\ldots$, P_n son todas ciertas, y la segunda hipótesis del enunciado asegura entonces que P_{n+1} es cierta. Observemos ahora que, entonces, P_1, P_2, $\ldots$, P_n, P_{n+1} son todas ciertas; es decir, Q_{n+1} es cierta. El Principio de Inducción Matemática 1.4 implica ahora que Q_n es cierta para todo $n \in \mathbb{N}$. Esto claramente implica que P_n es cierta para todo $n \in \mathbb{N}$. $\square$

Para el siguiente ejemplo, recordemos cómo se define un número primo.

Definición. Un número natural se dice que es *primo* si tiene exactamente dos divisores (el 1 y él mismo).

Ejemplo (Teorema Fundamental de la Aritmética)*.* Todo número natural mayor que 1, o es primo, o se puede descomponer en producto de números primos.

Demostración. Vamos a probar la proposición equivalente: “Todo número natural, o es 1, o es primo, o se puede descomponer en producto de números primos”.

Resulta evidente que la inducción matemática habitual resulta insuficiente para probar este enunciado, ya que no hay forma de probar que, si n es primo o producto de primos, entonces $n + 1$ también lo es. Veamos que el Principio de Inducción Completa 1.5 sí nos sirve en este caso.

Es obvio que el enunciado es cierto para $n = 1$.

Para probar el paso de inducción, supongamos que $1, 2, 3, \ldots, n$ cumplen la proposición, y veamos qué ocurre con $n + 1$.

Es evidente que $n + 1 \neq 1$. Si $n + 1$ es primo, ya hemos acabado, ya que entonces se cumple la tesis de inducción. Si no lo es, existirán dos naturales p y q, ambos diferentes de 1, tales que $n + 1 = pq$. Resulta evidente que tanto p como q son menores que $n + 1$. Por la hipótesis de inducción tenemos que ambos deben ser primos o producto de primos; es decir, existen $p_1, p_2, \dots, p_k$ y $q_1, q_2, \dots, q_l$, tales que $p = p_1 p_2 \cdots p_k$ y $q = q_1 q_2 \cdots q_l$. En consecuencia,

$$n + 1 = pq = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_l$$

es producto de primos, y también en este caso se cumple la tesis de inducción.

Por el Principio de Inducción Completa 1.5, resulta entonces que el enunciado es cierto. □

Axiomas de Peano

Es un hecho notable, señalado por el matemático italiano Giuseppe Peano en su obra *Arithmetices principia nova methodo exposita* (Bocca, 1889) que todas las propiedades de los números naturales pueden deducirse de las siguientes, llamadas en su honor *Axiomas de Peano* para los números naturales.

Axiomas 1.6 (Peano)**.**

(I) *Para todo número natural n existe otro número natural n^+, que se llama siguiente o sucesor de n.*

(II) *Existe un número natural, que denotamos por 1, tal que $n^+ \neq 1$ cualquiera que sea el número natural n.*

(III) *Cualesquiera que sean los números naturales m y n, es $m^+ = n^+$ si y solo si $m = n$.*

(IV) *Si un conjunto S de números naturales contiene a 1 y siempre que $n \in S$ también es $n^+ \in S$, entonces $S = \mathbb{N}$.*

La suma y el producto, así como la relación de orden que hay en los naturales se pueden *definir* utilizando tan solo estos axiomas. Véase [6, págs. 3–9].

1.2. Números enteros

¿Qué son los números enteros?

El conjunto de los *números enteros*, $\dots, -3, -2, -1, 0, 1, 2, 3, \dots$, que amplía el de los naturales, se denota por $\mathbb{Z}$. En él hay definidas dos operaciones, suma y producto, y una relación de orden.

Propiedades algebraicas de los enteros

Las propiedades de la suma y producto de los números naturales también las cumplen los números enteros. Cumplen además algunas propiedades adicionales:

- Elemento neutro (o *nulo*) de la suma: Hay un número entero, que denotamos por 0, tal que $n + 0 = n$ para cualquier entero n.

- Elemento *opuesto* para la suma: para cada entero n hay otro entero, que denotamos por $-n$, tal que $n + (-n) = 0$.

Obsérvese que estas dos propiedades nos permiten realizar la resta de dos enteros, cosa que no era posible con los naturales.

Estas y las anteriores propiedades de la suma y el producto se resumen diciendo que $\mathbb{Z}$, con estas dos operaciones, es un *anillo conmutativo y unitario*.

Propiedades del orden de los enteros

En cuanto al orden, además de las propiedades que cumplía el orden de los naturales, podemos añadir:

- Compatibilidad del *orden* con la *suma*: Si $m \leqslant n$, entonces $m+p \leqslant n+p$.

- Compatibilidad del *orden* con el *producto*: Si $m \leqslant n$ y $p \geqslant 0$, entonces $mp \leqslant np$.

Buena ordenación (*parcial*) para los enteros

Los números enteros no están bien ordenados, pero tienen una propiedades que a efectos prácticos es casi lo mismo.

Definición 1.7. Un conjunto $S \subset \mathbb{Z}$ no vacío se dice que está *acotado inferiormente* (resp. *superiormente*), si existe un entero $k \in \mathbb{Z}$ tal que, para todo $n \in S$, es $k \leqslant n$ (resp. $k \geqslant n$).

Teorema 1.8 (Buena ordenación parcial de los enteros)**.** *Todo conjunto no vacío $S \subset \mathbb{Z}$ acotado inferiormente (resp. superiormente) tiene un elemento mínimo (resp. máximo), es decir, existe un elemento $n_0 \in S$ tal que $n_0 \leqslant n$ (resp. $n_0 \geqslant n$) para todo $n \in S$.*

Demostración. Probaremos primero lo referente a conjuntos acotados *inferiormente*.

Supongamos que $k \in \mathbb{Z}$ es tal que $k \leqslant n$ para todo $n \in S$. Si $k \geqslant 1$, el resultado es trivial, ya que entonces se tiene $S \subset \mathbb{N}$. Así que supongamos que $k \leqslant 0$, y sea

$$S^* = \{\, n - k + 1 \mid n \in S \,\}.$$

Para todo $n \in S$ se tendrá $n-k+1 \geqslant k-k+1 = 1$, por lo que $S^* \subset \mathbb{N}$. Además, es claro que $S^* \neq \varnothing$. En consecuencia, por el Principio de Buena Ordenación 1.2, S^* tiene un primer elemento m_0. Como $m_0 \in S^*$, existirá un $n_0 \in S$ tal que $m_0 = n_0 - k + 1$. Veamos que n_0 es el primer elemento de S. En efecto, si $n \in S$, entonces $n - k + 1 \in S^*$, de donde $n - k + 1 \geqslant m_0 = n_0 - k + 1$. Se obtiene así que $n \geqslant n_0$ para todo $n \in S$.

Supongamos ahora que S está acotado superiormente, es decir, existe $k \in \mathbb{Z}$ tal que $n \leqslant k$ para todo $n \in S$. Definamos

$$-S = \{ -n \mid n \in \mathbb{N} \}.$$

Entonces, para todo $n \in S$, se tiene $-k \leqslant -n$ o, lo que es lo mismo, todos los elementos de $-S$ son mayores o iguales que $-k$. Por tanto, $-S$ está acotado inferiormente y, según se ha probado en la primera parte de la demostración, esto implica que $-S$ tiene un elemento mínimo $n_0 \in -S$. Como $-n \geqslant n_0$ para todo $n \in S$, obtenemos así que $n \leqslant -n_0$ para todo $n \in S$. Es decir, $-n_0 \in S$ es un elemento máximo de S. □

Ejemplos.

- El conjunto $\{ -3, 5, 7 \}$ tiene por primer elemento el -3. También tiene por último elemento al 7.
- El conjunto $\{ n \in \mathbb{Z} \mid n \text{ es par} \}$, que es infinito, no tiene primer ni último elemento. Esto se debe a que no es acotado, ni superior ni inferiormente.
- El conjunto $\{ -4, -2, 0, 2, 4, 6, \dots \}$, en cambio, al ser acotado inferiormente, resulta que sí que tiene un primer elemento, que es el -4. No tiene último elemento, ya que no está acotado superiormente.
- Si consideramos en cambio el conjunto $\{ \dots, -6, -3, 0, 3, 6 \}$, en esta ocasión sí tenemos un máximo (el 6), pero no existe mínimo.

Un principio de inducción

En $\mathbb{Z}$ puede hablarse del siguiente a un número entero, en el sentido de que entre n y $n + 1$ no hay ningún número entero. No se cumple, sin embargo, el Principio de Inducción, sino una propiedad similar aunque en principio más débil:

Teorema 1.9. *Sea $k \in \mathbb{Z}$. Si un conjunto $S \subset \mathbb{Z}$ cumple las dos condiciones siguientes:*

(I) *$k \in S$, y*

(II) *si $n \in S$ y $n \geqslant k$, entonces $n + 1 \in S$,*

entonces S contiene a todos los enteros a partir de k, es decir,

$$S \supset \{\, n \in \mathbb{Z} \mid n \geqslant k \,\}.$$

Demostración. Supongamos que no se cumple el teorema, y sea

$$S^* = \{\, n \in \mathbb{Z} \mid n \geqslant k \quad \text{y} \quad n \notin S \,\}.$$

Nuestra suposición de que no se cumple el teorema nos dice que $S^* \neq \varnothing$ y, por otro lado, está claro que este conjunto está acotado inferiormente (por k), así que S^* tiene un mínimo, que llamaremos n_0.

Consideremos el anterior a este número, que es $n_0 - 1$. Evidentemente, se tiene $n_0 - 1 \notin S^*$. Si fuera $n_0 - 1 < k$, se tendría $n_0 \leqslant k$, y como $n_0 \in S^*$, sería $n_0 = k$, lo cual es contradictorio, porque $k \in S$. Por tanto, debe ser $n_0 - 1 \geqslant k$. Como $n_0 - 1 \notin S^*$, esto quiere decir que $n_0 - 1 \in S$. Pero entonces, por (II), deberá ser $n_0 = (n_0 - 1) + 1 \in S$. Esto es una contradicción, ya que $n_0 \in S^*$. $\square$

Enunciado práctico

Como se puede suponer, es posible dar un enunciado del Teorema 1.9 en términos de propiedades.

Teorema 1.10. *Sea $k \in \mathbb{Z}$. Si una propiedad P_n es tal que*

(I) *P_k es cierta, y*

(II) *si P_n es cierta y $n \geqslant k$, entonces P_{n+1} es cierta,*

entonces P_n es cierta para todo entero $n \geqslant k$.

Ejemplo. Probar que $n^2 \leqslant 2^n$ para todo $n \geqslant 4$.

Solución. Vemos inmediatamente que la base de inducción (que en este caso es para $n = 4$) es cierta. En efecto, $4^2 = 16 = 2^4$.

Para dar el paso de inducción, supongamos que $n \geqslant 4$ y que $n^2 \leqslant 2^n$. Tenemos que ver que $(n+1)^2 \leqslant 2^{n+1}$. Sabemos que $(n+1)^2 = n^2 + 2n + 1$. Si conseguimos probar que

$$2n + 1 \leqslant n^2, \tag{1}$$

entonces, utilizando la hipótesis de inducción, tendremos que

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

Probemos, pues, (1). Como $n \geqslant 4$, resulta que $n^2 - 2n + 1 = (n - 1)^2 \geqslant 2$, de donde $n^2 \geqslant 2n + 1$, como queríamos probar.

El principio de inducción que acabamos de ver nos dice entonces que $n^2 \leqslant 2^n$ para todo $n \geqslant 4$.

Podríamos caer en la trampa y deducir que $n^2 \leqslant 2^n$ para todo $n \in \mathbb{N}$, ya que también se puede comprobar que para $n = 1$ se tiene $1^2 = 1 < 2 = 2^1$. Obsérvese que para verificar el paso de inducción hemos tenido que utilizar que $n \geqslant 4$ (aunque valdría también $n \geqslant 3$); sin utilizar una restricción de este tipo no se puede probar de ningún modo el paso de inducción. Es por esta razón que esta fórmula no se cumple para todo $n \in \mathbb{N}$: en efecto, para $n = 3$, se puede comprobar que $3^2 = 9 > 8 = 2^3$. $\square$

1.3. Números racionales

¿Qué son los números racionales?

En $\mathbb{Z}$ es posible la resta, pero no la división. Esta operación es posible (dividiendo por elementos distintos de 0) en el conjunto $\mathbb{Q}$ de los *números racionales*, que son cocientes de números enteros (con denominador no nulo). En este conjunto están definidas la suma y el producto, y una relación de orden.

Propiedades algebraicas de los racionales

Las propiedades de la suma, el producto y el orden de los números enteros también las cumplen los números racionales. Cumplen además una propiedad adicional:

- Elemento *inverso* para el producto: Si $a \neq 0$, hay un número racional que denotamos por a^{-1} o $\frac{1}{a}$, tal que $aa^{-1} = 1$.

Esta propiedad es la que nos permite realizar la división de un racional por otro racional no nulo. Esta operación no era posible en los enteros.

Esta y las anteriores propiedades de la suma, el producto y el orden se resumen diciendo que $\mathbb{Q}$ es un *cuerpo ordenado*.

Deficiencias de los racionales

Señalemos que en $\mathbb{Q}$ no hay ninguna propiedad similar al Principio de Inducción. Ni siquiera puede hablarse del siguiente a un número dado: concretamente, entre dos números racionales distintos siempre hay otro número racional. En efecto: si $a < b$, es fácil comprobar que $a < \frac{a+b}{2} < b$.

A pesar de que esta última ampliación resuelve bastante bien los problemas con respecto a las operaciones básicas (se puede sumar, restar, multiplicar, dividir sin apenas restricciones) es fácil descubrir *huecos* en $\mathbb{Q}$: por ejemplo, ningún número racional puede representar la diagonal de un cuadrado de lado 1. Dicho de otra forma, no existe ningún racional a tal que $a^2 = 2$.

En efecto: sea $a \in \mathbb{Q}$; podemos escribirlo como $a = \frac{m}{n}$, con m y n enteros sin factores primos comunes y $n \neq 0$. Si fuera $a^2 = 2$ se seguiría que $m^2 = 2n^2$, luego m^2 es par, y también debe serlo m; pero entonces $m = 2p$ para algún entero p, y sustituyendo en $m^2 = 2n^2$ queda $4p^2 = 2n^2$. Es decir, $2p^2 = n^2$; luego n^2 es par, y también debe serlo n. En resumen, m y n son pares; pero habíamos supuesto que m y n no tenían factores comunes. La contradicción viene de suponer que $a^2 = 2$.

Para poder hablar de números que representen cantidades tales como la que acabamos de encontrar, se necesita una nueva ampliación de los sistemas numéricos.

2. Los números reales

2.1. Operaciones algebraicas

El conjunto de los reales

Pasamos a considerar a continuación el conjunto $\mathbb{R}$ de los *números reales* o, más exactamente, las propiedades de $\mathbb{R}$ (sin entrar en su naturaleza: no decimos qué es un número real, sino cómo se manejan los números reales, fijando sus propiedades básicas como axiomas).

Propiedades algebraicas de los reales

La suma y el producto le dan a $\mathbb{R}$ una estructura de *cuerpo conmutativo*. Esto quiere decir que se verifican las siguientes propiedades:

Axiomas 1.11 (de la suma)**.**

(I) *Propiedad asociativa de la suma:* $(a + b) + c = a + (b + c)$.

(II) *Propiedad conmutativa de la suma:* $a + b = b + a$.

(III) *Elemento neutro (o nulo) de la suma: hay un número real, denotado por* 0, *tal que* $a + 0 = a$, *cualquiera que sea* a.

(IV) *Elemento opuesto para la suma: para cada real* a, *hay un número real, que denotamos por* $-a$, *tal que* $a + (-a) = 0$.

Axiomas 1.12 (del producto)**.**

(V) *Propiedad asociativa del producto:* $(ab)c = a(bc)$.

(VI) *Propiedad conmutativa del producto:* $ab = ba$.

(VII) *Elemento neutro (o identidad) para el producto: hay un número real distinto de* 0*, que denotamos por* 1*, tal que* $a \cdot 1 = a$*, cualquiera que sea* a*.*

(VIII) *Elemento inverso para el producto: si* $a \neq 0$*, hay un número real, que denotamos por* a^{-1} *o* $\frac{1}{a}$*, tal que* $aa^{-1} = 1$*.*

Axioma 1.13 (Relación de suma y producto)**.**

(IX) *Propiedad distributiva del producto con respecto a la suma:* $a(b+c) = ab + ac$*.*

Consecuencias de las propiedades básicas

De estas propiedades pueden deducirse sucesivamente muchas más, como vemos a continuación. Estas consecuencias las utilizaremos de aquí en adelante sin más comentario según las necesitemos. En lo que sigue, a, b, c, d representan números reales cualesquiera.

Proposición 1.14.

(I) *Si* $a + c = b + c$*, entonces* $a = b$*. (Ley de Cancelación).*

(II) *Si* $a + b = a$*, entonces* $b = 0$*. En consecuencia, en el conjunto de los reales hay un único elemento nulo.*

(III) *Si* $a + b = 0$*, entonces* $b = -a$*. En consecuencia, cada número real tiene un único opuesto.*

Demostración.

(I) Como $a + c = b + c$, sumando $-c$ a ambos miembros y aplicando la propiedad asociativa, obtenemos

$$\begin{aligned} a &= a + 0 = a + [c + (-c)] = (a + c) + (-c) \\ &= (b + c) + (-c) = b + [c + (-c)] = b + 0 = b. \end{aligned}$$

(II) Como $a + b = a + 0$, la Ley de Cancelación (I) nos dice que $b = 0$. En consecuencia, si $0'$ es un elemento nulo, se tendrá $a + 0' = a$, y según acabamos de ver solo puede ser $0' = 0$.

(III) Supongamos que $a + b = 0$. Entonces,

$$b + a = a + b = 0 = a + (-a) = (-a) + a,$$

así que, por la Ley de Cancelación (I), tiene que ser $b = -a$. □

Proposición 1.15.

(I) *Si* $ac = bc$, *y* $c \neq 0$, *entonces* $a = b$. *(Ley de Cancelación)*

(II) *Si* $ab = a$ *y* $a \neq 0$, *entonces* $b = 1$. *Por tanto, en el conjunto de los reales hay un único elemento identidad.*

(III) *Si* $a \neq 0$ *y* $ab = 1$, *entonces* $b = \frac{1}{a}$. *En consecuencia, cada número real no nulo tiene un único inverso.*

Demostración. Se demuestra de forma análoga a 1.14. □

Obsérvese que la exigencia en (III) de que $a \neq 0$ no es en realidad necesaria, ya que, según veremos en la proposición siguiente, esto se da automáticamente si $ab = 1$.

La Propiedad Distributiva 1.13 (IX) tiene las siguientes consecuencias:

Proposición 1.16.

(I) $a \cdot 0 = 0$. *(Se dice que* 0 *es un elemento absorbente).*

(II) *Si* $ab = 0$ *entonces* $a = 0$ *o* $b = 0$.

(III) $-a = (-1)a$.

(IV) $(-1)(-a) = a$. *Por tanto,* $-(-a) = a$. *(Ley de Idempotencia).*

(V) $(-a)(-b) = ab$.

(VI) *Si* $a \neq 0$, *entonces* $1/a \neq 0$ *y* $1/(1/a) = a$. *(Ley de Idempotencia)*

Demostración.

(I) Tenemos

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0,$$

así que, por 1.14 (II), debe ser $a \cdot 0 = 0$.

(II) Si fuera $b \neq 0$, tendríamos, por el apartado anterior, $ab = 0 = 0 \cdot b$. Por la Ley de Cancelación del producto (1.15 (I)), tiene que ser $a = 0$.

(III) Tenemos que

$$a + (-1)a = 1 \cdot a + (-1)a = [1 + (-1)]a = 0 \cdot a = 0.$$

Aplicando 1.14 (III), vemos que $(-1)a = -a$.

(IV) Tenemos que

$$\begin{aligned}(-1)(-a) + (-a) &= (-1)(-a) + 1(-a)\\ &= [(-1) + 1](-a) = 0(-a) = 0 = a + (-a).\end{aligned}$$

Utilizando la Propiedad de Cancelación, resulta que $(-1)(-a) = a$. Por tanto, por (III), será $-(-a) = (-1)(-a) = a$.

(V) Claramente,

$$(-a)(-b) = [(-1)a](-b) = [a(-1)](-b) = a[(-1)(-b)] = ab.$$

(VI) Si fuera $1/a = 0$, entonces sería $1 = a(1/a) = a \cdot 0 = 0 \neq 1$, lo que es una contradicción. Por tanto, $1/a \neq 0$, y cabe hablar de $1/(1/a)$. Además, como $(1/a)a = 1$, se tiene por 1.15 (III) que $a = 1/(1/a)$. □

Abreviaturas

Es habitual utilizar las siguientes abreviaturas, que nosotros usaremos a partir de ahora:

- $a - b \coloneqq a + (-b), \qquad \frac{a}{b} \coloneqq a \cdot \frac{1}{b},$
- $a + b + c \coloneqq (a + b) + c = a + (b + c), \qquad abc \coloneqq (ab)c = a(bc),$
- $a^2 \coloneqq aa, \qquad a^3 \coloneqq aaa, \qquad \dots$
- $2a \coloneqq a + a, \qquad 3a \coloneqq a + a + a, \qquad \dots$

2.2. Desigualdades fundamentales en $\mathbb{R}$

Propiedades básicas del orden

En $\mathbb{R}$ hay una relación de orden que extiende la de los números racionales. Las propiedades básicas son las siguientes (a, b, c representan números reales cualesquiera):

Axiomas 1.17.

(X) *Propiedad reflexiva: $a \leqslant a$.*

(XI) *Propiedad antisimétrica: Si $a \leqslant b$ y $b \leqslant a$ entonces $a = b$.*

(XII) *Propiedad transitiva: Si $a \leqslant b$ y $b \leqslant c$ entonces $a \leqslant c$.*

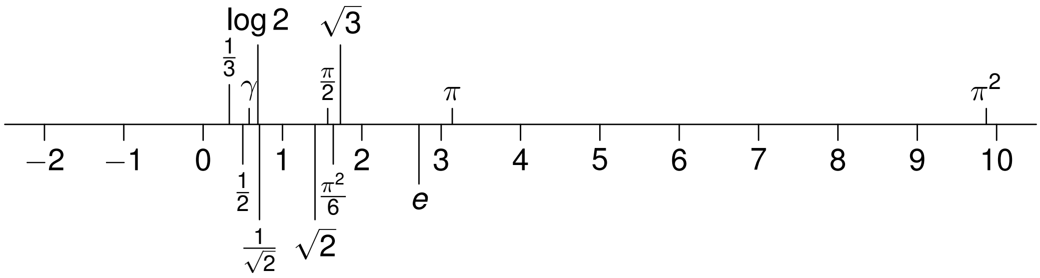
(XIII) *Propiedad de orden total: Siempre es $a \leqslant b$ o $b \leqslant a$.*

(XIV) *Compatibilidad con la suma: Si $a \leqslant b$ entonces $a + c \leqslant b + c$.*

(XV) *Compatibilidad con el producto: Si $c \geqslant 0$ y $a \leqslant b$ entonces $ac \leqslant bc$. (En particular, si $c \geqslant 0$, $b \geqslant 0$ entonces $bc \geqslant 0$.)*

La recta real

Debido a estas propiedades, los números reales se pueden representar gráficamente como puntos de una recta. Esto permite, sobre todo, visualizar la ordenación de estos números.



Desigualdad estricta

Introducimos la siguiente notación:

Definición 1.18. Sean $a, b \in \mathbb{R}$. Decimos que $a < b$ (o que $b > a$) si $a \leqslant b$ y $a \neq b$.

Se prueba fácilmente la siguiente propiedad:

Teorema 1.19 (Ley de Tricotomía)**.** *Sean $a, b \in \mathbb{R}$. Se da uno y solo uno de los siguientes casos:*

(I) $a < b$,

(II) $a = b$,

(III) $a > b$.

Demostración. Veamos en primer lugar que siempre se cumple al menos una de estas tres propiedades. Por la Propiedad de Orden Total 1.17 (XIII), debe ser $a \leqslant b$ o $a \geqslant b$. Supongamos, por ejemplo, que $a \leqslant b$. Si no es $a = b$, entonces, por definición del orden estricto, se tiene $a < b$. Si $a \geqslant b$ se razona de manera análoga.

Veamos ahora que solo se puede cumplir una de las tres. En efecto, por la definición de orden estricto 1.18, si $a = b$ es evidente que no puede ser $a < b$ ni $a > b$. Por otro lado, si se cumpliera $a < b$ y $a > b$, entonces sería $a \leqslant b$ y $b \leqslant a$, de donde $a = b$. Esto es claramente una contradicción. $\square$

Consecuencias de las desigualdades básicas

De estas desigualdades pueden deducirse las siguientes, que también utilizaremos en lo sucesivo sin más comentario según las necesitemos. En lo que sigue, a, b, c, d representan números reales cualesquiera.

Proposición 1.20.

(I) *Si* $a \leqslant b$, $b < c$ *entonces* $a < c$.

(II) *Si* $a < b$, $b \leqslant c$ *entonces* $a < c$.

(III) *Si* $a < b$ *entonces* $a + c < b + c$.

(IV) *Si* $a \leqslant b$, $c \leqslant d$, *entonces* $a + c \leqslant b + d$, *siendo entonces* $a + c = b + d$ *si y solo si* $a = b$ *y* $c = d$.

(V) $a > 0$ *si y solo si* $-a < 0$.

Demostración.

(I) Por la Propiedad Transitiva 1.17 (XII), sabemos que $a \leqslant c$. Si fuera $a = c$, entonces se tendría $a \leqslant b$ y $b < a$, lo que es una contradicción. Por tanto, ha de ser $a < c$.

(II) Análogo.

(III) Por la compatibilidad del orden con la suma 1.17 (XIV), sabemos que $a + c \leqslant b + c$. Si fuera $a + c = b + c$, por la Ley de Cancelación 1.14 (I) sería $a = b$, lo cual es absurdo. Así, ha de ser $a + c < b + c$.

(IV) Utilizando de nuevo la compatibilidad del orden con la suma 1.17 (XIV), será

$$a + c \leqslant a + d \leqslant b + d.$$

En el caso en que $a + c = b + d$, la cadena de desigualdades anterior debe ser una cadena de igualdades:

$$a + c = a + d = b + d.$$

Aplicando dos veces la Propiedad de Cancelación 1.14 (I), obtenemos que $c = d$ y $a = b$.

(V) Como $a > 0$, sumando $-a$ a ambos miembros obtenemos

$$0 = a - a > 0 - a = -a.$$

El recíproco es similar. □

Proposición 1.21.

(I) *Si* $a > 0$, $b > 0$, *entonces* $ab > 0$.

(II) *Si* $a > 0$*,* $b < 0$*, entonces* $ab < 0$*.*

(III) *Si* $a < 0$*,* $b < 0$*, entonces* $ab > 0$*.*

(IV) *Cualquiera que sea* a*, es* $a^2 \geqslant 0$*. Se tiene* $a^2 = 0$ *si y solo si* $a = 0$*.*

(V) $1 > 0$ *y* $-1 < 0$*.*

Demostración.
(I) Por la compatibilidad del orden con el producto 1.17 (XV), sabemos que $ab \geqslant 0$. Si fuera $ab = 0$, entonces debe ser $a = 0$ o $b = 0$. Cualquiera de ambas posibilidades constituyen una contradicción.
(II) Como $b < 0$, es $-b > 0$, así que, por (I), será $-(ab) = a(-b) > 0$. Por tanto, $ab < 0$.
(III) Tenemos que $-a > 0$ y $-b > 0$, de forma que $ab = (-a)(-b) > 0$.
(IV) Si $a > 0$, (I) nos dice que $a^2 = a \cdot a > 0$. Si $a < 0$, es (III) quien nos hace llegar a la misma conclusión. Si $a = 0$, es evidente que $a^2 = 0$.
(V) Por (IV), tenemos $1 = 1^2 > 0$. En consecuencia, $-1 < 0$. □

Proposición 1.22.

(I) *Si* $a < b$*,* $c > 0$*, entonces* $ac < bc$*.*

(II) *Si* $a < b$*,* $c < 0$*, entonces* $ac > bc$*.*

(III) *Si* $a \leqslant b$*,* $c \leqslant 0$*, entonces* $ac \geqslant bc$*.*

Demostración.
(I) Como $a < b$, restando a a ambos miembros, se obtiene

$$0 = a - a < b - a.$$

Multiplicando ahora por $c > 0$ obtenemos

$$bc - ac = (b - a)c > 0.$$

Si ahora sumamos ac, obtenemos finalmente

$$bc = (bc - ac) + ac > 0 + ac = ac.$$

(II) Como $-c > 0$, de (I) obtenemos que $-ac < -bc$. Sumando $ac + bc$ a ambos miembros, obtenemos

$$bc = (ac + bc) - ac < (ac + bc) - bc = ac.$$

(III) Análogo. □

Proposición 1.23.

(I) *Si* $0 \leqslant a \leqslant b$, *entonces* $a^2 \leqslant b^2$.

(II) *Si* $0 \leqslant a < b$, *entonces* $a^2 < b^2$.

Demostración.

(I) Como a y b son no negativos, utilizando la compatibilidad del orden con el producto 1.17 (XV) dos veces, obtenemos

$$a^2 \leqslant ab \leqslant b^2.$$

(II) Análogo. □

Proposición 1.24.

(I) *Si* $a > 0$ *entonces* $\frac{1}{a} > 0$. *Si* $a < 0$ *entonces* $\frac{1}{a} < 0$.

(II) *Si* $0 < a < b$ *entonces* $\frac{1}{b} < \frac{1}{a}$.

(III) *Si* $a < b < 0$ *entonces* $\frac{1}{b} < \frac{1}{a}$.

Demostración.

(I) Supongamos que $a > 0$. Si fuera $\frac{1}{a} < 0$, tendríamos $1 = a \cdot \frac{1}{a} < 0$. Contradicción. Ha de ser, por tanto, $\frac{1}{a} > 0$. (Ya sabemos que $\frac{1}{a} \neq 0$.) El otro caso es análogo.

(II) Como $a, b > 0$, será también $ab > 0$. Si dividimos por ab, obtenemos

$$\frac{1}{b} = \frac{a}{ab} < \frac{b}{ab} = \frac{1}{a}.$$

(III) Similar. □

Si a y b tienen el mismo signo, los apartados (II) y (III) de 1.24 nos dicen que la operación de inversión cambia el orden en que estos se encuentran; es decir, si $a < b$ entonces $1/b < 1/a$. Esto, no obstante, no es cierto (y se trata de un error frecuente) si a y b tienen distinto signo. En efecto, por el apartado (I) se deduce que si $a < 0 < b$ entonces $1/a < 0 < 1/b$.

2.3. Valor absoluto de un número real. Desigualdades básicas

Valor absoluto y distancia

Definición 1.25. El *valor absoluto* de un número real a es el número real no negativo

$$|a| = \begin{cases} a, & \text{si } a \geqslant 0, \\ -a, & \text{si } a \leqslant 0. \end{cases}$$

Gráficamente corresponde a la distancia de a al origen.

Definición 1.26. Dados $a, b \in \mathbb{R}$, se llama *distancia* entre a y b al número real no negativo $|a - b|$.

Gráficamente, $|a - b|$ mide la distancia geométrica entre los puntos a y b.

Propiedades del valor absoluto

Recogemos a continuación las propiedades del valor absoluto que son de mayor interés para el resto del curso. En lo sucesivo, a, b, c y d denotan números reales cualesquiera.

Proposición 1.27.

(I) $|a| \geqslant 0$.

(II) $|a| = 0$ *si, y solo si,* $a = 0$.

(III) $|-a| = |a|$.

(IV) $|a| \leqslant b$ *si, y solo si,* $-b \leqslant a \leqslant b$.

(V) $|a| > b$ *si, y solo si,* $a > b$ *o* $a < -b$.

(VI) $-|a| \leqslant a \leqslant |a|$.

Demostración.

(I) Si $a \geqslant 0$, se tiene $|a| = a \geqslant 0$. Si $a < 0$, es $|a| = -a > 0$.

(II) Es obvio que si $a = 0$ entonces $|a| = 0$.

Supongamos ahora que $|a| = 0$. Como el valor absoluto de a solo puede ser a o $-a$, en cualquiera de los dos casos obtenemos que $a = 0$.

(III) Si $a \geqslant 0$, entonces $-a \leqslant 0$, de donde $|-a| = -(-a) = a = |a|$.

Si $a \leqslant 0$, teniendo en cuenta que $-a \geqslant 0$, será $|-a| = -a = |a|$.

(IV) Supongamos primero que $|a| \leqslant b$. Es obvio que debe ser $b \geqslant 0$. Si $a \geqslant 0$, entonces $-b \leqslant 0 \leqslant a = |a| \leqslant b$. Si $a \leqslant 0$, tenemos análogamente que $-b \leqslant 0 \leqslant -a = |a| \leqslant b$, de donde también en este caso es $-b \leqslant a \leqslant b$.

Recíprocamente, supongamos que $-b \leqslant a \leqslant b$. Como $-b \leqslant a$, se tendrá $-a \leqslant b$. Sabemos además que $a \leqslant b$. Como $|a|$ solo puede tomar los valores a y $-a$, resulta que en cualquier caso debe ser $|a| \leqslant b$.

(V) Consecuencia inmediata de (IV).

(VI) Basta tomar $b = |a|$ en (IV). □

Proposición 1.28.

(I) $|ab| = |a||b|$.

(II) $\left|\frac{1}{a}\right| = \frac{1}{|a|}$.

(III) $a^2 \leqslant b^2$ *si, y solo si,* $|a| \leqslant |b|$.

(IV) $a^2 = b^2$ *si, y solo si,* $|a| = |b|$.

Demostración.
(I) Si a o b son nulos, entonces

$$|ab| = 0 = |a||b|.$$

Si $a, b > 0$, se tiene $ab > 0$, de donde

$$|ab| = ab = |a||b|.$$

Si a y b tienen distinto signo (por ejemplo $a > 0$ y $b < 0$) entonces $ab < 0$, de donde

$$|ab| = -ab = a(-b) = |a||b|.$$

Si ambos son negativos, entonces $ab > 0$ y

$$|ab| = ab = (-a)(-b) = |a||b|.$$

(II) Multiplicando, y teniendo en cuenta (I), obtenemos

$$|a|\left|\frac{1}{a}\right| = \left|a \cdot \frac{1}{a}\right| = 1.$$

Esto nos indica que $\left|\frac{1}{a}\right|$ es el inverso de $|a|$. Es decir, $\left|\frac{1}{a}\right| = \frac{1}{|a|}$.
(III) Teniendo en cuenta que $a^2 \geqslant 0$ y (I), se tiene

$$a^2 = |a^2| = |a|^2.$$

Como $0 \leqslant |a| \leqslant |b|$, podemos utilizar 1.23 (I), de donde

$$a^2 = |a|^2 \leqslant |b|^2 = b^2.$$

Para la implicación directa, si suponemos $|b| < |a|$, podemos utilizar 1.23 (II), y entonces será

$$b^2 = |b|^2 < |a|^2 = a^2.$$

(IV) Consecuencia inmediata de (III). $\square$

Desigualdad triangular

Las siguientes propiedades son especialmente útiles y se usarán con mucha frecuencia en lo sucesivo.

Teorema 1.29 (Desigualdad Triangular)**.** *Si a y b son números reales cualesquiera,*

$$|a+b| \leqslant |a| + |b|.$$

Demostración. La demostración es sencilla: según las propiedades anteriores,

$$-|a| \leqslant a \leqslant |a|, \qquad -|b| \leqslant b \leqslant |b|.$$

Sumamos las dos desigualdades y resulta $-|a| - |b| \leqslant a + b \leqslant |a| + |b|$, es decir,

$$-(|a| + |b|) \leqslant a + b \leqslant |a| + |b|.$$

Usamos ahora 1.27 (IV) y deducimos que $|a+b| \leqslant |a| + |b|$. □

Ejemplos. A veces la desigualdad anterior es una igualdad, y otras veces es una desigualdad estricta.

- Si los dos números tienen el mismo signo, la Desigualdad Triangular es en realidad una igualdad. Por ejemplo, $|3+5| = 8 = |3| + |5|$.
- Si, por el contrario los dos números son de signo opuesto, la Desigualdad Triangular es una desigualdad estricta. Por ejemplo, $|-3+5| = 2 < 8 = |-3| + |5|$.

Teorema 1.30 (Desigualdad Triangular Inversa)**.** *Si a y b son números reales cualesquiera,*

$$\big||a| - |b|\big| \leqslant |a-b|.$$

Demostración. Esta desigualdad es consecuencia de la Desigualdad Triangular. En efecto: aplicando esta a los números b y $a-b$, resulta

$$|a| = |(a-b) + b| \leqslant |a-b| + |b|,$$

es decir,

$$|a| - |b| \leqslant |a-b|.$$

Cambiando los papeles de a y b, tenemos $|b| - |a| \leqslant |b-a| = |a-b|$, es decir

$$-|a-b| \leqslant |a| - |b|.$$

De aquí se deduce que $\big||a| - |b|\big| \leqslant |a-b|$. □

Ejemplos. Como ocurría con la Desigualdad Triangular, también aquí se trata de una desigualdad estricta o una igualdad, dependiendo de los signos de los números implicados.

- $||3| - |4|| = 1 = |3-4|$.
- $||-3| - |4|| = 1 < 8 = |-3-4|$.

2.4. Conjuntos acotados en $\mathbb{R}$. El Axioma del Supremo

Cotas superiores e inferiores. Conjuntos acotados

Definición 1.31. Sea S un subconjunto no vacío de $\mathbb{R}$.

(I) Si a es un número real y $a \leqslant s$ para todo $s \in S$, decimos que a es una *cota inferior* de S y que S está *acotado inferiormente* (por a).

(II) Si b es otro número real y $b \geqslant s$ para todo $s \in S$, decimos que b es una *cota superior* de S y que S está *acotado superiormente* (por b).

(III) Si un conjunto está acotado superiormente e inferiormente, decimos que está *acotado*.

Ejemplos.

- El conjunto $S = \{ s \in \mathbb{R} \mid s \geqslant -3 \}$ tiene por cota inferior al -3, ya que para todo $s \in S$ es $-3 \leqslant s$. No es la única. También el -4, el -5, el $-\frac{13}{2}$, ..., son todos cotas inferiores de S. Por otro lado, S no tiene cotas superiores. Para cualquier número $a \in \mathbb{R}$, siempre podemos encontrar un $s \in S$ tal que $s > a$. Así, podemos concluir que S es acotado inferiormente, pero no superiormente.

- El conjunto $T = \{ s \in \mathbb{R} \mid s < 3 \}$ tiene al 3 por cota superior (y al 4, y muchos otros). Pero no tiene cotas inferiores. Por tanto, es acotado superiormente, pero no inferiormente.

- El conjunto $U = \{ s \in \mathbb{R} \mid -3 < s \leqslant 3 \}$ tiene al 3 por cota superior y al -3 por cota inferior. Así, S es acotado superior e inferiormente, y, en consecuencia, es acotado.

Máximo y mínimo

Definición 1.32. Sea S un subconjunto de $\mathbb{R}$.

(I) Un número real m se dice que es un *mínimo* de S si pertenece a él y es una cota inferior de este, es decir, si $m \in S$ y $m \leqslant s$ para todo $s \in S$. Se escribe entonces $m = \min S$.

(II) Un número real M se dice que es un *máximo* de S si pertenece a él y es una cota superior de este, es decir, si $M \in S$ y $M \geqslant s$ para todo $s \in S$. Se escribe entonces $M = \max S$.

Ejemplos.

- El conjunto $S = \{ s \in \mathbb{R} \mid s \geqslant -3 \}$ tiene por mínimo al -3. En efecto, según vimos antes, -3 es una de sus cotas inferiores. Además, $-3 \in S$. Por otro lado, al no estar acotado superiormente, no tiene máximo.

- El conjunto $T = \{ s \in \mathbb{R} \mid s < 3 \}$ no tiene máximo ni mínimo. (Puede parecer a primera vista que $3 = \max T$, pero esto no es así).

- Especial atención se debe prestar al conjunto $U = \{ s \in \mathbb{R} \mid -3 < s \leqslant 3 \}$. Obsérvese que 3 es el máximo de T. Pero, aunque a primera vista pueda parecer que -3 es su mínimo, esto no es verdad, ya que $-3 \notin U$. Es obvio que -3 cumple un papel especial con respecto a este conjunto, que vamos a ver un poco más adelante.

Los máximos y mínimos son únicos

Ya hemos visto en los ejemplos que cuando un conjunto tiene una cota, en realidad tiene muchas, es decir, las cotas de conjuntos, de existir, no son únicas. Algo bastante diferente ocurre con los máximos y mínimos.

Proposición 1.33. *Si un conjunto de números reales tiene máximo, este es único.*

Demostración. Supongamos que el conjunto S tiene dos máximos, que denotamos por M y M'. Entonces, ambos son cotas superiores de S, y ambos son elementos de S. Como $M \in S$ y M' es cota superior de S, se tiene necesariamente que $M \leqslant M'$. De forma análoga, también se prueba que $M' \leqslant M$. En consecuencia, debe ser $M = M'$. $\square$

Proposición 1.34. *Si un conjunto de números reales tiene mínimo, este es único.*

Demostración. Análogo al teorema anterior. $\square$

Ínfimo y supremo

En los ejemplos vistos anteriormente, nos aparecían algunos puntos especiales, parecidos a máximos y mínimos, pero que sin embargo no se ajustaban a la definición de estos. Introducimos ahora un concepto que sí sirve para ellos.

Definición 1.35. Sea S un subconjunto de $\mathbb{R}$.

(I) Un número real a se dice que es el *ínfimo* de S si es la mayor cota inferior de S. En este caso se escribe $a = \text{ínf}\, S$.

(II) Un número real b se dice que es el *supremo* de S si es la menor cota superior de S. En este caso se escribe $a = \sup S$.

Los ínfimos y supremos son únicos

Claramente, b es el supremo de S si es el mínimo del conjunto de sus cotas superiores y a el ínfimo de S si es el máximo del conjunto de sus cotas inferiores. Considerando que los máximos y mínimos son únicos, lo mismo tiene que ocurrir con los ínfimos y supremos.

Proposición 1.36. *Si un conjunto de números reales tiene supremo, este es único.*

Proposición 1.37. *Si un conjunto de números reales tiene ínfimo, este es único.*

Máximo y supremo

Los conceptos de ínfimo y supremo son generalizaciones de los de mínimo y máximo.

Proposición 1.38. *Sea S un conjunto de números reales. Entonces, $b \in \mathbb{R}$ es el máximo de S si, y solo si, es su supremo y además $b \in S$.*

Demostración. Si $b = \text{máx}\, S$, entonces, por definición, b es una cota superior de S. Sea c otra de sus cotas superiores. Como $b \in S$, debe ser $b \leqslant c$. Así pues, b es la mínima cota superior de S. Es decir, $b = \sup S$.

Recíprocamente, supongamos que $b \in S$ y $b = \sup S$. Entonces, b es una cota superior de S y, así, verifica las condiciones de la definición de máximo. $\square$

Algo similar se tiene para mínimo e ínfimo.

Proposición 1.39. *Sea S un conjunto de números reales. Entonces, $a \in \mathbb{R}$ es el mínimo de S si y solo si es su ínfimo y además $a \in S$.*

Demostración. Análogo a la proposición anterior. $\square$

Ejemplo. Consideremos el conjunto $U = \{ s \in \mathbb{R} \mid -3 < s \leqslant 3 \}$. Ya hemos visto que 3 es el máximo de U, así que, sin dar ningún argumento más, podemos decir que 3 es el supremo de U.

En cuanto al ínfimo, probaremos a continuación que es -3. En efecto, ya vimos que -3 es una cota inferior de U. Por otro lado, si consideramos un elemento $a > -3$, y llamamos b al mínimo de 3 y a, siempre podemos encontrar un elemento c tal que $-3 < c < b$ (por ejemplo, $\frac{b-3}{2}$). Es fácil ver que $c \in U$, y además $c < a$, de donde a no es cota inferior de U. Es decir, -3 es la mínima cota inferior de U.

Caracterización "ε" de supremos e ínfimos

Ya hemos dicho que b es el supremo de S si es el mínimo del conjunto de sus cotas superiores, esto es, si b es cota superior de S, y ningún $b' < b$ es cota superior de S; o dicho de otra forma, si b es cota superior de S y para todo $b' < b$ existe un $s \in S$ tal que $s > b'$. Teniendo en cuenta que todo $b' < b$ se puede escribir en la forma $b' = b - \varepsilon$ con $\varepsilon > 0$ (concretamente, con $\varepsilon = b - b'$), obtenemos lo siguiente:

Proposición 1.40 (Caracterización "ε" del supremo)**.** *Sea S un conjunto de números reales. Entonces $b \in \mathbb{R}$ es el supremo de S si, y solo si, verifica las dos siguientes condiciones:*

(I) *b es cota superior de S.*

(II) *Para todo $\varepsilon > 0$, existe un $s \in S$ tal que $s > b - \varepsilon$.*

Es decir, el supremo de S es una cota superior que tiene elementos de S tan cerca como queramos. Algo parecido se puede decir acerca del ínfimo.

Proposición 1.41 (Caracterización "ε" del ínfimo)**.** *Sea S un conjunto de números reales. Entonces $a \in \mathbb{R}$ es el ínfimo de S si, y solo si, verifica las dos siguientes condiciones:*

(I) *a es cota inferior de S.*

(II) *Para todo $\varepsilon > 0$, existe un $s \in S$ tal que $s < a + \varepsilon$.*

El supremo no funciona bien en los racionales

Ya vimos que los números naturales están bien ordenados, es decir, todos sus subconjuntos no vacíos tienen mínimo. Los números enteros no cumplen esto, pero sí verifican que un conjunto no vacío acotado inferiormente tiene mínimo y un conjunto no vacío acotado superiormente tiene máximo. También vimos que, al pasar a los números racionales, esta propiedad se pierde. Lo mismo le ocurre a los reales.

Ahora bien, ¿qué ocurrirá si sustituimos en esta propiedad “máximo” por “supremo” y “mínimo” por “ínfimo”? ¿Será verdad, al menos, que todo conjunto no vacío acotado superiormente tiene supremo? ¿Y la propiedad simétrica para ínfimos? Comprobaremos en el siguiente ejemplo que los racionales *no verifican* esta propiedad.

Ejemplo. El conjunto

$$S = \{\, x \in \mathbb{Q} \mid x > 0,\ x^2 \leqslant 2 \,\}$$

no es vacío y está acotado superiormente, pero no tiene supremo en $\mathbb{Q}$.

Está claro que S no es vacío, ya que $1 \in S$, y está acotado superiormente, ya que, si $x \in S$, entonces $x^2 \leqslant 2 < 2^2$, de donde $x < 2$.

Para ver que S no tiene supremo en $\mathbb{Q}$, procederemos por reducción al absurdo. Supongamos que S tiene un supremo $s \in \mathbb{Q}$. Está claro que $s > 0$, ya que $s \geqslant 1$. Además, es también obvio que no puede ser $s^2 = 2$ (porque ya hemos visto que esta condición no la verifica ningún número racional), así que deberá cumplirse que $s^2 > 2$ o $s^2 < 2$. Vamos a ver que ambos casos conducen a una contradicción.

Supongamos primero que $s^2 > 2$. Sea

$$r = \frac{s^2 - 2}{2s^2}$$

y definamos $p = s(1-r)$. Claramente, $p \in \mathbb{Q}$ y $0 < r < 1/2$, de donde $0 < p < s$. Además, tenemos que

$$p^2 = s^2(1-r)^2 = s^2(1-2r+r^2) > s^2(1-2r) = s^2 \cdot \frac{2}{s^2} = 2.$$

En consecuencia, si $x \in S$, se cumplirá $x^2 < 2 < p^2$, de donde $x < p$, y así p es una cota superior de S. Esto es imposible, ya que entonces s no sería la *mínima* cota superior de S.

Veamos ahora qué ocurre si suponemos que $s^2 < 2$. Sea

$$r = \frac{2 - s^2}{4}$$

y definamos $p = s/(1-r)$. También en este caso $p \in \mathbb{Q}$ y $0 < r < 1/2$. Por otra parte, a diferencia de lo que ocurría en el caso anterior, ahora se cumple que $p > s$. Además

$$p^2 = \frac{s^2}{(1-r)^2} = \frac{s^2}{1-2r+r^2} < \frac{s^2}{1-2r} = \frac{s^2}{s^2/2} = 2.$$

Se concluye de esta manera que $p \in S$. Pero esto también es contradictorio, ya que entonces s no es cota superior de S.

La Propiedad del Supremo de los reales

Esta es de hecho la propiedad clave que diferencia a los reales de los racionales. Se cumple en el primero de estos conjuntos, y no se cumple en el otro, como acabamos de ver. De momento, fijaremos esta propiedad como el último de nuestros axiomas para los reales.

Axioma 1.42 (Propiedad del Supremo, o de Completitud)**.**

(XVI) *Todo subconjunto no vacío de* $\mathbb{R}$ *acotado superiormente tiene supremo.*

Es inmediato que, exigiendo este axioma, la propiedad simétrica a ella también se cumple.

Proposición 1.43. *Todo subconjunto no vacío de* $\mathbb{R}$ *acotado inferiormente tiene ínfimo.*

Demostración. Sea $S \subset \mathbb{R}$ no vacío y acotado inferiormente, y sea

$$-S = \{\, x \in \mathbb{R} \mid -x \in S \,\}.$$

Si c es una cota inferior de S, es fácil ver que $-c$ es una cota superior de $-S$ (*¿por qué?*), así que $-S$ es acotado superiormente, y, por tanto, existe $b = \sup(-S)$. Veremos que $-b = \operatorname{ínf} S$. En efecto, como b es una cota superior de $-S$, resulta que $-b$ es cota inferior de S (*¿por qué?*). Sea $x > -b$, entonces $-x < b$, de donde $-x$ no es cota superior de $-S$ (*¿por qué?*). En consecuencia, $-b$ es la *máxima* cota inferior de S. Es decir, $-b = \operatorname{ínf} S$. □

2.5. Propiedad Arquimediana de $\mathbb{R}$. Consecuencias

La Propiedad Arquimediana

Una consecuencia fundamental de la Propiedad del Supremo es la Propiedad Arquimediana, que nos habla del papel que juegan los naturales dentro de $\mathbb{R}$.

Teorema 1.44 (Propiedad Arquimediana)**.** *Dados dos números reales* a *y* b *con* $a > 0$*, existe algún número natural* n *tal que* $na > b$*.*

Demostración. Sean $a, b \in \mathbb{R}$, con $a > 0$. Razonemos por reducción al absurdo: supongamos que la tesis no es cierta, es decir, $na \leqslant b$ para todo número natural n, y veamos que se llega a una contradicción. En tal caso, el conjunto

$$S = \{\, na \mid n \in \mathbb{N} \,\},$$

que no es vacío, estaría acotado superiormente (por b), luego por el Axioma del Supremo tendría supremo. Sea s este supremo, es decir,

$$s = \sup S = \sup\{\, na \mid n \in \mathbb{N} \,\}.$$

Puesto que $a > 0$, es $s - a < s$; según la definición de supremo, $s - a$ ya no puede ser cota superior del conjunto S, de modo que existirá algún elemento en S estrictamente mayor que $s - a$. Dicho elemento será de la forma ma con $m \in \mathbb{N}$, y así $s - a < ma$. Pero esto implica que $s < ma + a = (m+1)a$ y obviamente $(m+1)a \in S$, con lo cual s no es una cota superior de S. Hemos llegado a una contradicción. □

Otros enunciados de la Propiedad Arquimediana

La Propiedad Arquimediana aparece frecuentemente enunciada en las siguientes formulaciones alternativas. (Es fácil ver que todas ellas son equivalentes a nuestro enunciado.)

Teorema 1.45. *Dados un número real b, existe algún número natural n tal que $n > b$.*

Teorema 1.46. *Los números naturales no constituyen un conjunto acotado (en $\mathbb{R}$).*

Teorema 1.47. *Dado $\varepsilon > 0$, existe un número natural n tal que $1/n < \varepsilon$.*

En lo que sigue, siempre que nombremos la Propiedad Arquimediana, haremos referencia a alguno de estos cuatro enunciados indistintamente.

Parte entera de un número real

Como consecuencia de la Propiedad Arquimediana se puede probar que todo número real está comprendido entre dos enteros consecutivos.

Teorema 1.48. *Dado $x \in \mathbb{R}$, existe un número entero m (y uno solo), tal que*

$$m \leqslant x < m + 1.$$

Para demostrar este teorema, podemos utilizar cualquiera de los siguientes caminos:

Demostración 1. Si consideramos el conjunto $S = \{\, n \in \mathbb{Z} \mid n \leqslant x \,\}$, resulta que este conjunto es no vacío, pues por la Propiedad Arquimediana existe $n \in \mathbb{Z}$ tal que $n > -x$ y así $-n < x$, luego $-n \in S$; además, S está acotado superiormente (por x o por cualquier número natural superior a x, si no queremos salirnos de $\mathbb{Z}$). Por lo tanto, S tiene un elemento máximo, llamémosle m. Como $m \in S$, se tendrá $m \leqslant x$. Y como m es el máximo de S y $m < m + 1$, se deduce que $m + 1 \notin S$, es decir, $x < m + 1$.

Para la unicidad, obsérvese que, si existieran dos enteros m_1 y m_2, tales que

$$m_1 \leqslant x < m_1 + 1 \qquad \text{y} \qquad m_2 \leqslant x < m_2 + 1,$$

sería entonces $m_1 \leqslant x < m_2 + 1$, de donde $m_1 \leqslant m_2$. De forma análoga, se tendría $m_2 \leqslant m_1$. En conclusión, $m_1 = m_2$. □

Demostración 2. Utilizamos que todos los números naturales son mayores o iguales que 1 (se puede demostrar por inducción) y que los números naturales son justamente los enteros positivos. Llamando nuevamente S al conjunto de enteros menores o iguales que x, S es no vacío por el argumento anterior y está acotado superiormente por x; aplicando el Axioma del Supremo, S tiene un supremo, al que vamos a llamar s. Como $s-1$ ya no es cota superior de S, por ser estrictamente menor que s, existirá $m \in S$ tal que $s - 1 < m \leqslant s$. Pero m también es cota superior de S, dado que si algún $n \in S$ verificase $n > m$ obtendríamos $m < n \leqslant s < m + 1$, de donde $0 < n - m < 1$, y $n - m$ sería un entero positivo menor que 1, lo que es imposible. Por tanto, vemos que hay un elemento de S que es cota superior de S, es decir, que es el máximo de S, y como antes deberá cumplir $m \leqslant x < m + 1$.

La unicidad se obtiene de la misma forma que en la *demostración 1*. □

Definición 1.49. Al número m del teorema anterior se le llama *parte entera* de x, y se denota con $[x]$.

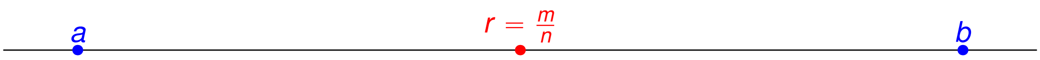
Ejemplos.

$$[3{,}5] = 3, \qquad [1{,}2] = 1, \qquad [-7{,}3] = -8.$$

Los racionales son densos

La Propiedad Arquimediana permite también deducir cómo están distribuidos en $\mathbb{R}$ los números racionales.

Teorema 1.50 (Densidad de los Racionales)**.** *Dados dos números reales a y b, con $a < b$, existe algún número racional r tal que $a < r < b$.*



Si existe tal r, podrá escribirse en la forma $r = m/n$ con $m \in \mathbb{Z}$ y $n \in \mathbb{N}$, de modo que tenemos que encontrar $m \in \mathbb{Z}$ y $n \in \mathbb{N}$ tales que $a < m/n < b$ o, lo que es lo mismo, $na < m < nb$. Es intuitivamente claro, pensando en la representación gráfica de $\mathbb{R}$, que entre dos números a distancia mayor que 1 siempre se puede incluir un número entero (suponiendo los dos números positivos, por ejemplo, superponiendo el segmento unidad consigo mismo hacia la derecha, la primera vez que sobrepasemos el número más al origen, no habremos sobrepasado el otro número). Esta es la idea que vamos a tratar de utilizar.

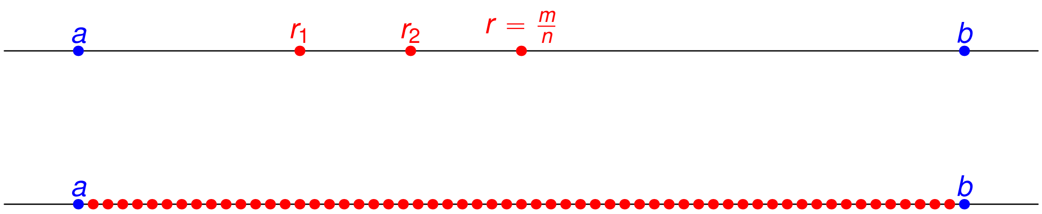
Demostración. La Propiedad Arquimediana aplicada a $b-a > 0$ y a 1 nos asegura la existencia de un $n \in \mathbb{N}$ tal que $n(b-a) > 1$, con lo cual $nb > na + 1$.

Sea ahora $p \in \mathbb{Z}$ tal que $p \leqslant na < p+1$, y definamos $m = p+1$. Entonces,

$$na < m = p + 1 \leqslant na + 1 < nb.$$

En consecuencia, $a < m/n < b$. Basta ahora tomar $r = m/n$. □

Obsérvese que el teorema que acabamos de ver no asegura tan solo que podemos "colocar" un número racional entre a y b, sino toda una infinidad de ellos. En efecto, una vez que hemos colocado un número racional r, podríamos colocar otro más entre a y r, que llamaríamos r_1, y entre r_1 y r podríamos colocar otro, llamémosle r_2, a así sucesivamente. La Densidad de los Racionales nos indica por tanto que los racionales están distribuidos en la recta real de forma muy uniforme y también muy *densa*: allá donde miremos, siempre vamos a encontrar infinitos racionales.



2.6. Números irracionales

Los números irracionales

Definición 1.51. Los números reales que no son racionales se llaman *números irracionales*.

Nos proponemos ahora probar que existen números irracionales. Ya vimos que no existe ningún número racional cuyo cuadrado sea 2. Veremos a continuación que sí que existe un número *real* con esta propiedad, así que este deberá ser irracional. En realidad, probaremos algo más general.

Teorema 1.52. *Sea p un número real no negativo y $n \in \mathbb{N}$. Existe un único numero real v tal que $v^n = p$.*

Demostración. Si $n = 1$ el resultado es obvio, así que supondremos en lo sucesivo que $n \geqslant 2$. Si $p = 0$, basta escoger $v = 0$. Supongamos pues también que $p > 0$.

Consideremos el conjunto

$$S = \{ x > 0 \mid x^n \leqslant p \}.$$

Este conjunto es no vacío, ya que $x_0 = \text{mín}\{p, 1\} \in S$. En efecto, si $p \geqslant 1$ podemos ver que $x_0 = 1 \in S$. Si, por el contrario, $p < 1$, entonces $p^n \leqslant p$, así que $x_0 = p \in S$.

Por otra parte, S está acotado superiormente por $c = \text{máx}\{p, 1\}$. Si $p \geqslant 1$, entonces para todo $x \in S$ se tiene $x^n \leqslant p \leqslant p^n = c^n$. Por la Identidad Ciclotómica (que probaremos en un ejercicio), se tiene

$$0 \leqslant c^n - x^n = (c - x)(c^{n-1} + c^{n-2}x + \cdots + cx^{n-2} + x^{n-1}),$$

de donde $x \leqslant c$. En el caso en que $p < 1$, para todo $x \in S$ obtenemos de la misma manera que $x^n \leqslant p < 1 = c^n$, así que $x < c$.

En consecuencia, S tiene un supremo. Sea $v = \sup S$. Como $x_0 = \text{mín}\{p, 1\} \in S$ y $x_0 > 0$, deberá ser $v > 0$. Vamos a probar que no puede ser $v^n > p$ ni $v^n < p$, con lo que solo restará la posibilidad $v^n = p$.

Supongamos primero que $v^n > p$. Si $0 < \varepsilon < 1$, definamos $u = v(1 - \varepsilon)$. Observemos que $0 < u < v$. Utilizando la Desigualdad de Bernouilli (que se probará en un ejercicio), obtenemos que

$$u^n = v^n(1 - \varepsilon)^n > v^n(1 - n\varepsilon).$$

Así pues, si escogemos

$$\varepsilon = \frac{v^n - p}{nv^n}$$

(obsérvese que en este caso se tendrá $0 < \varepsilon < 1/n$), obtendremos que

$$u^n > v^n(1 - n\varepsilon) = v^n\Big(1 - n \cdot \frac{v^n - p}{nv^n}\Big) = p \geqslant x^n$$

cualquiera que sea $x \in S$, de donde se deduce que $u > x$ para todo $x \in S$. O, lo que es lo mismo, u es una cota superior de S. Esto es absurdo ya que $u < v$ y v es la mínima cota superior de S.

Supongamos ahora que $v^n < p$. Si $0 < \varepsilon < 1$ definamos en este caso $u = v/(1 - \varepsilon)$. En esta ocasión resulta que $u > v$. Utilizando de nuevo la Desigualdad de Bernouilli, se obtiene que

$$u^n = \frac{v^n}{(1 - \varepsilon)^n} < \frac{v^n}{1 - n\varepsilon}$$

siempre que $0 < \varepsilon < 1/n$. Esta última condición se verifica si escogemos

$$\varepsilon = \frac{p - v^n}{np}.$$

Con esta elección se tiene además

$$u^n < \frac{v^n}{1 - n\varepsilon} = \frac{v^n}{1 - n\frac{p-v^n}{np}} = p.$$

Hemos demostrado que $u \in S$. Pero esto no puede ser, ya que $u > v$ y además $v = \sup S$.

Para probar la unicidad, supongamos que existen $v, w > 0$ tales que $v^n = w^n = p$. Entonces, utilizando la Identidad Ciclotómica,

$$0 = p - p = v^n - w^n = (v - w)(v^{n-1} + v^{n-2}w + \cdots + vw^{n-2} + w^{n-1}).$$

Como $v, w > 0$, se deduce que

$$v^{n-1} + v^{n-2}w + \cdots + vw^{n-2} + w^{n-1} > 0$$

y, como consecuencia, tendrá que ser $v - w = 0$, es decir, $v = w$. $\square$

El número v que aparece en el enunciado del Teorema 1.52 se denomina *raíz n-ésima* de p y se denota $v = \sqrt[n]{p}$.

Como ya avanzamos antes, este teorema nos proporciona, en particular, un número real v tal que $v^2 = 2$. Este número claramente no puede ser racional, así que obtenemos lo siguiente:

Corolario 1.53. *Existen números irracionales.*

Los irracionales son densos

Acabamos de probar que existe al menos un número irracional. Pero lo cierto es que existen muchos. Vamos a ver a continuación que los irracionales se distribuyen por la recta real de forma bastante similar a como lo hacen los racionales.

Teorema 1.54 (Densidad de los Irracionales)**.** *Dados dos números reales a y b, con $a < b$, existe algún número irracional x tal que $a < x < b$.*

Demostración. Sea $y \in \mathbb{R}\backslash\mathbb{Q}$ cualquiera. (Ya hemos visto que existe alguno). Puesto que $a - y < b - y$, según el teorema anterior existe algún $r \in \mathbb{Q}$ tal que $a - y < r < b - y$, de donde $a < r + y < b$. Por último, $x = r + y$ es un número irracional, ya que si fuera racional se tendría $y = (r + y) + (-r) \in \mathbb{Q}$. $\square$

2.7. Números algebraicos y trascendentes

Concepto de número algebraico

Definición 1.55. Se dice que un número real es *algebraico* si es un cero de un polinomio con coeficientes enteros. El conjunto de los números algebraicos se denota por $\mathbb{A}$.

Observación. En la definición anterior, se puede cambiar "coeficientes enteros" por "coeficientes racionales". En efecto, supongamos que el número α es un cero del polinomio con coeficientes racionales

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Definir d como el máximo común divisor de los denominadores de $a_0, a_1, \ldots, a_n$. Entonces el polinomio

$$p^*(x) = da_n x^n + da_{n-1}x^{n-1} + \cdots + da_1 x + da_0$$

tiene coeficientes enteros y los mismos ceros que $p(x)$. En particular, α es un cero de $p^*(x)$ y por tanto es algebraico.

Además, si utilizamos coeficientes racionales en lugar de enteros, se puede suponer siempre que el coeficiente principal a_n es igual a 1.

Proposición 1.56. *Todo número racional es algebraico.*

Demostración. Basta observar que si $r \in \mathbb{Q}$, entonces r es un cero del polinomio $p(x) = x - r$. □

Los racionales no son los únicos números algebraicos, como se verá en los siguientes ejemplos. También veremos más adelante que existen números que no disfrutan de esta propiedad. Esto, combinado con la proposición 1.56, hace que el concepto de número algebraico sea interesante hablando de números irracionales, y solo de números irracionales.

Ejemplos.

- $\sqrt{2}$.

  En efecto, este número es un cero del polinomio $x^2 - 2$.

- $\sqrt[3]{3}$.

  Es cero del polinomio $x^3 - 3$.

- La *razón áurea* $\frac{1+\sqrt{5}}{2}$.

  Es un cero del polinomio $x^2 - x - 1$.

- $\sqrt{2} + \sqrt{3}$.

  Es un cero del polinomio $x^4 - 10x^2 + 1$.

Operaciones con números algebraicos

Los números algebraicos son estables para las operaciones usuales, como se ve en el siguiente resultado. Las propiedades (I) a (IV) del siguiente teorema nos dicen que $\mathbb{A}$ tiene estructura de cuerpo conmutativo.

Teorema 1.57. *Sean α y β dos números algebraicos. Entonces*

(I) $\alpha + \beta$ *es algebraico.*

(II) $\alpha\beta$ *es algebraico.*

(III) $-\alpha$ *es algebraico.*

(IV) *Si $\alpha \neq 0$ entonces $1/\alpha$ es algebraico. En consecuencia, β/α es algebraico.*

(V) *Si $\alpha > 0$ y $p \in \mathbb{N}$, entonces $\sqrt[p]{\alpha}$ es algebraico.*

Demostración. Si α o β son iguales a 0, todos los apartados son triviales, así que supondremos que ninguno de los dos es nulo.

Supongamos que

$$\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = 0$$

y

$$\beta^n + b_{n-1}\beta^{n-1} + \cdots + b_1\beta + b_0 = 0.$$

donde los a_j y b_k son racionales. Sea $w \in \mathbb{R}^{mn}$ el vector

$$(1, \alpha, \alpha^2, \ldots, \alpha^{m-1}, \beta, \alpha\beta, \alpha^2\beta, \ldots, \alpha^{m-1}\beta, \beta^2, \alpha\beta^2, \ldots, \alpha^{m-1}\beta^{n-1}).$$

Consideremos ahora el vector αw. Las coordenadas de este vector tienen todas la forma $\alpha^{j+1}\beta^k$ donde $0 \leqslant j < m$ y $0 \leqslant k < n$. Si $j + 1 < m$ esto es también una de las coordenadas de w; si $j + 1 = m$ se tiene

$$\alpha^m\beta^k = -a_{m-1}\alpha^{m-1}\beta^k - \cdots - a_1\alpha\beta^k - a_0\beta^k.$$

En cualquier caso $\alpha^{j+1}\beta^k$ es una combinación lineal, con coeficientes racionales, de coordenadas de w. Por tanto, existe una matriz A ($mn \times mn$ con componentes racionales) tal que $\alpha w = wA$. De forma similar, existe una matriz B ($mn \times mn$ con componentes racionales) tal que $\beta w = wB$.

En lo que sigue, denotemos por I la matriz identidad $mn \times mn$.

(I) Se tendrá

$$w(A + B) = wA + wB = \alpha w + \beta w = (\alpha + \beta)w = (\alpha + \beta)wI.$$

Por tanto,

$$w(A + B - (\alpha + \beta)I) = 0.$$

Esto indica que el vector w representa una solución no trivial del sistema de ecuaciones homogéneo asociado a la matriz $A + B - (\alpha + \beta)I$. Por el Teorema de Rouché-Frobenius, obtenemos que $\det(A + B - (\alpha + \beta)I) = 0$. Es decir, si consideramos el polinomio $P(x)$ de grado mn con coeficientes racionales definido por $P(x) = \det(A + B - xI)$, resulta que $P(\alpha + \beta) = 0$, con lo que $\alpha + \beta$ es algebraico.

(II) Tendremos ahora que

$$wAB = \alpha wB = \alpha\beta w = \alpha\beta wI.$$

En consecuencia,

$$w(AB - \alpha\beta I) = 0.$$

Como en el apartado (I), esto implica que $\det(AB - \alpha\beta I) = 0$. Sea $Q(x)$ el polinomio definido por $Q(x) = \det(AB - xI)$. Según hemos visto, $Q(\alpha\beta) = 0$ así que $\alpha\beta$ es algebraico.

(III) Basta aplicar el apartado (II) con $\beta = -1$.

(IV) Es suficiente observar que

$$\begin{aligned} 0 &= \frac{1}{\alpha^m} \cdot (\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0) \\ &= 1 + a_{m-1} \cdot \frac{1}{\alpha} + \cdots + a_1 \cdot \frac{1}{\alpha^{m-1}} + a_0 \cdot \frac{1}{\alpha^m}, \end{aligned}$$

así que si definimos el polinomio

$$R(x) = a_0x^m + a_1x^{m-1} + \cdots + a_{m-1}x + 1$$

tendremos que $R(1/\alpha) = 0$ y por tanto $1/\alpha$ es algebraico.

(V) Es evidente que $\sqrt[p]{\alpha}$ es un cero del polinomio

$$T(x) = x^{pm} + a_{m-1}x^{p(m-1)} + \cdots + a_1x^p + a_0. \qquad \square$$

Una consecuencia del resultado anterior es que cualquier número que se pueda construir a partir de números racionales (o enteros) utilizando solamente una cantidad finita de sumas, restas, productos, divisiones y raices ha de ser un número algebraico.

Ejemplo. El número

$$\sqrt[3]{\frac{1 + \sqrt{5} + \sqrt[7]{2}}{\sqrt[4]{3} + \sqrt{5}}}$$

es algebraico.

El recíproco no es cierto. El Teorema de Abel-Ruffini establece que existen polinomios con coeficientes racionales (de grado mayor que 4), cuyos ceros no se pueden expresar de esta manera. Obsérvese que dichos ceros son siempre números algebraicos.

Los números algebraicos son numerables

Otra propiedad interesante de los números algebraicos es que constituyen un conjunto numerable.

Teorema 1.58 (de Cantor)**.** *El conjunto $\mathbb{A}$ de los números algebraicos es numerable.*

Demostración. Para cada $n \in \mathbb{N} \cup \{0\}$, sea

$$\begin{aligned}\mathbb{Q}_n[x] = \{\, P(x) \mid P(x) &\text{ es un polinomio en } x \\ &\text{de grado menor o igual que } n \text{ con coeficientes racionales} \,\}.\end{aligned}$$

Evidentemente, la aplicación $f\colon \mathbb{Q}^{n+1} \to \mathbb{Q}_n[x]$ dada por

$$f(a_0, a_1, \ldots, a_{n-1}, a_n) = a_n x^n + a_{n-1} x^n + \cdots + a_1 x + a_0$$

es una biyección. Esto implica que $\mathbb{Q}_n[x]$ tiene el mismo cardinal que $\mathbb{Q}^{n+1}$, y por tanto es numerable.

Definamos ahora el conjunto

$$\mathbb{Q}[x] = \{\, P(x) \mid P(x) \text{ es un polinomio en } x \text{ con coeficientes racionales} \,\}.$$

Está claro que se puede escribir

$$\mathbb{Q}[x] = \bigcup_{n=0}^{\infty} \mathbb{Q}_n[x].$$

Como es una unión numerable de conjuntos numerables, resulta que $\mathbb{Q}[x]$ es numerable.

Finalmente, para cada $P(x) \in \mathbb{Q}[x]$, consideremos el conjunto de sus ceros

$$\mathcal{Z}(P(x)) = \{\, \alpha \in \mathbb{R} \mid P(\alpha) = 0 \,\}.$$

Observemos que $\mathcal{Z}(P(x))$ es siempre un conjunto finito. Basta ahora observar que

$$\mathbb{A} = \bigcup_{P(x) \in \mathbb{Q}[x]} \mathcal{Z}(P(x)).$$

Por tanto, $\mathbb{A}$ es una unión numerable de conjuntos finitos, y por tanto es numerable. $\square$

Números trascendentes

Teniendo en cuenta que el conjunto de los números reales no es numerable, el resultado anterior pone de manifiesto que existen números reales que no son algebraicos. Y no solo eso, sino que los números algebraicos constituyen una minoría dentro de los números reales. Daremos un nombre a este tipo de números.

Definición 1.59. Se dice que un número real es *trascendente* si no es algebraico.

Paradójicamente, aunque los números trascendentes son los más abundantes, resultan siempre muy escurridizos: probar que un número concreto es trascendente es a menudo una tarea tremendamente difícil. Daremos a continuación unos cuantos ejemplos sin demostración.

Ejemplos.

- La *constante de Liouville* $L = \sum_{k=1}^{\infty} 10^{-k!} = 0{,}110001000\ldots$ fue el primer ejemplo de número trascendente que se encontró (Liouville, 1844).
- El *número* e es trascendente (Hermite, 1873).
- El *número* π es trascendente (Lindemann, 1882).
- e^{α}, $\cos\alpha$, $\operatorname{sen}\alpha$, $\tan\alpha$, $\cosh\alpha$, $\operatorname{senh}\alpha$, $\tanh\alpha$, $\arccos\alpha$, … son todos ellos trascendentes si α es un número algebraico no nulo (Lindemann, 1882).
- $\log\alpha$ es trascendente si α es un algebraico positivo diferente de 1 (Lindemann, 1882).
- α^{β} es trascendente si α es un número algebraico positivo distinto de 1 y β es un número algebraico irracional (Gelfond, 1934; Schneider, 1935).
- $\log_{\alpha}\beta$ es trascendente si α es un número algebraico positivo distinto de 1 y β es un número algebraico positivo que no es una potencia racional de α (Gelfond, 1934; Schneider, 1935).
- e^{π} es trascendente (Gelfond, 1934; Schneider, 1935).
- La *constante de Copeland-Erdős* $E = 0{,}235711131719\ldots$ es trascendente (Copeland-Erdős, 1945).
- La *constante de Chapernowne* $C = 0{,}12345678910111213\ldots$ es trascendente (Mahler, 1961).

- Los valores pares de la *función Zeta de Riemann*

$$\zeta(2n) = \sum_{k=1}^{\infty} \frac{1}{k^{2n}} = 1 + \frac{1}{2^{2n}} + \frac{1}{3^{2n}} + \frac{1}{4^{2n}} + \cdots$$

  son trascendentes.

Relacionadas con la trascendencia de números, hay numerosas preguntas abiertas.

Ejemplos. No se sabe si son trascendentes los siguientes números:

- e^e, π^π, π^e.
- $\pi + e$, πe (aunque se sabe que al menos uno de los dos es trascendente).
- La *constante de Catalan*

$$K = \sum_{k=1}^{\infty} \frac{1}{(2k-1)^2} = 1 + \frac{1}{3^2} + \frac{1}{5^2} + \cdots$$

- La *constante de Euler-Mascheroni*

$$\gamma = \lim_n \Big(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n\Big).$$

  (En este caso, ni siquiera se sabe si es irracional.)

- Los valores impares de la *función Zeta de Riemann*

$$\zeta(2n+1) = \sum_{k=1}^{\infty} \frac{1}{k^{2n+1}} = 1 + \frac{1}{2^{2n+1}} + \frac{1}{3^{2n+1}} + \frac{1}{4^{2n+1}} + \cdots$$

  Solo muy recientemente se ha probado que $\zeta(3)$ es irracional (Apéry, 1979). Hasta hoy no se sabe tan siquiera si lo es $\zeta(5)$.

2.8. Intervalos en $\mathbb{R}$

Intervalos

Definición 1.60. Reciben el nombre de *intervalos* los subconjuntos de $\mathbb{R}$ definidos del siguiente modo (a y b son número reales cualesquiera):

(I) intervalo *acotado* y *abierto*: $(a, b) = \{\, x \in \mathbb{R} \mid a < x < b \,\}$;

(II) intervalo *acotado*, *cerrado* por la izquierda y *abierto* por la derecha: $[a, b) = \{ x \in \mathbb{R} \mid a \leqslant x < b \}$;

(III) intervalo *acotado*, *abierto* por la izquierda y *cerrado* por la derecha: $(a, b] = \{ x \in \mathbb{R} \mid a < x \leqslant b \}$;

(IV) intervalo *acotado* y *cerrado*: $[a, b] = \{ x \in \mathbb{R} \mid a \leqslant x \leqslant b \}$;

(V) intervalo *abierto*, *acotado inferiormente* pero *no superiormente*: $(a, \infty) = \{ x \in \mathbb{R} \mid x > a \}$;

(VI) intervalo *cerrado*, *acotado inferiormente* pero *no superiormente*: $[a, \infty) = \{ x \in \mathbb{R} \mid x \geqslant a \}$;

(VII) intervalo *abierto*, *acotado superiormente* pero *no inferiormente*: $(-\infty, b) = \{ x \in \mathbb{R} \mid x < b \}$;

(VIII) intervalo *cerrado*, *acotado superiormente* pero *no inferiormente*: $(-\infty, b] = \{ x \in \mathbb{R} \mid x \leqslant b \}$;

(IX) intervalo *no acotado* ni inferior ni superiormente: $(-\infty, \infty) = \mathbb{R}$.

Nótese que si $a \geqslant b$ entonces $(a, b) = \varnothing$, de modo que el conjunto vacío es un intervalo. También lo son los conjuntos con un solo número real, ya que $\{a\} = [a, a]$.

Caracterización de los intervalos

Los intervalos de $\mathbb{R}$ se caracterizan por la siguiente propiedad.

Proposición 1.61 (Propiedad de los Valores Intermedios)**.** *Un subconjunto I de $\mathbb{R}$ es un intervalo si, y solo si, dados $x, y \in I$, cada $z \in \mathbb{R}$ tal que $x \leqslant z \leqslant y$ también pertenece a I.*

Demostración. Para probar la implicación directa basta un examen de todos los casos. Por ejemplo, si $I = (a, b)$, $x, y \in I$, y $z \in \mathbb{R}$ es tal que $x \leqslant z \leqslant y$, se tiene $a < x \leqslant z \leqslant y < b$, luego $a < z < b$ y por definición $z \in I$.

La implicación recíproca es trivial en caso de que $I = \varnothing$. Suponemos, pues, $I \neq \varnothing$. Pueden presentarse la siguientes situaciones:

(I) I es acotado,

(II) I es acotado superiormente pero no inferiormente,

(III) I es acotado inferiormente pero no superiormente,

(IV) I no es acotado ni inferior ni superiormente.

Veamos cada una de ellas.

(I) *I es acotado.* Sea $a = \inf I$, $b = \sup I$. Se tendrá $(a, b) \subset I \subset [a, b]$, pues $c \in (a, b)$ si, y solo si, $a < c < b$, y por definición de supremo e ínfimo existirán un $x \in I$ con $x < c$ y un $y \in I$ con $c < y$, luego $c \in I$; por otra parte, también por definición de supremo e ínfimo, de $x \in I$ se sigue $a \leqslant x \leqslant b$, o sea, $x \in [a, b]$. Ahora,

- si $a, b \in I$, entonces
$$[a, b] = (a, b) \cup \{a, b\} \subset I \subset [a, b],$$
luego $I = [a, b]$;
- si $a \in I$, $b \notin I$, entonces
$$[a, b) = (a, b) \cup \{a\} \subset I \subset [a, b] \backslash \{b\} = [a, b),$$
luego $I = [a, b)$;
- si $a \notin I$, $b \in I$, entonces
$$(a, b] = (a, b) \cup \{b\} \subset I \subset [a, b] \backslash \{a\} = (a, b],$$
luego $I = (a, b]$;
- si $a \notin I$, $b \notin I$, entonces
$$(a, b) \subset I \subset [a, b] \backslash \{a, b\} = (a, b),$$
luego $I = (a, b)$.

(II) *I es acotado superiormente pero no inferiormente.* Sea $a = \sup I$, con lo que $(-\infty, a) \subset I \subset (-\infty, a]$, pues para cada $z \in I$ es $z \leqslant a$ y, dado $z < a$, existe $y \in I$ con $z < y$ (por definición de supremo) y existe $x \in I$ con $x < z$ (I no está acotado inferiormente), que con la hipótesis del enunciado da $z \in I$. En consecuencia,

- si $a \in I$, se tiene
$$(-\infty, a] = (-\infty, a) \cup \{a\} \subset I \subset (-\infty, a],$$
luego $I = (-\infty, a]$;
- si $a \notin I$, se tiene
$$(-\infty, a) \subset I \subset (-\infty, a] \backslash \{a\} = (-\infty, a),$$
luego $I = (-\infty, a)$.

Los restantes casos se analizan de forma análoga: en (III) se obtiene $I = (a, \infty)$ o $I = [a, \infty)$, donde $a = \inf I$, y en (IV) queda $I = \mathbb{R}$. $\square$

El Teorema de los Intervalos Encajados

El siguiente teorema tiene una enorme cantidad de aplicaciones.

Teorema 1.62 (de los Intervalos Encajados, de Cantor)**.** *Para cada* $n \in \mathbb{N}$*, sea* $I_n = [a_n, b_n]$ *un intervalo cerrado y acotado (no vacío). Supongamos que para todo* $n \in \mathbb{N}$ *se cumple* $I_{n+1} \subset I_n$*. Entonces,* $\bigcap_{n\in\mathbb{N}} I_n$ *es no vacío. Si, además, el tamaño de los intervalos se puede hacer tan pequeño como se quiera, es decir,* $\operatorname{ínf}\{\, (b_n - a_n) \mid n \in \mathbb{N} \,\} = 0$*, entonces* $\bigcap_{n\in\mathbb{N}} I_n$ *consta exactamente de un punto.*

Demostración. Evidentemente, para todo $n \in \mathbb{N}$ se tiene $a_n \leqslant b_n$. Obsérvese además que, como $I_{n+1} \subset I_n$, para todo $n \in \mathbb{N}$ se tiene que

$$a_n \leqslant a_{n+1} \leqslant b_{n+1} \leqslant b_n.$$

Esto tiene como consecuencia que, si $m \geqslant n$, entonces

$$a_n \leqslant a_m \leqslant b_m \leqslant b_n \tag{2}$$

Sean ahora los dos conjuntos

$$A = \{\, a_n \mid n \in \mathbb{N} \,\}, \qquad B = \{\, b_n \mid n \in \mathbb{N} \,\}.$$

Vamos a ver a continuación que *cualquier* elemento de A es menor o igual que *cualquier* elemento de B, es decir, $a_n \leqslant b_m$ si $m, n \in \mathbb{N}$. En efecto, si $n \leqslant m$ obtenemos por (2) que $a_n \leqslant b_m$. Si, por el contrario, tenemos $n > m$, intercambiando los papeles de m y n en (2) volvemos a obtener que $a_n \leqslant b_m$.

Teniendo en cuenta lo que acabamos de probar, cualquier elemento $b_m \in B$ es una cota superior de A. Por tanto, A tiene un supremo $a = \sup A$ y, además, $a \leqslant b_m$ para todo $m \in \mathbb{N}$. Esto tiene como consecuencia que a es una cota inferior de B, de donde B tiene un ínfimo $b = \operatorname{ínf} B$ y, además, se tiene que $a \leqslant b$.

Escojamos ahora un elemento x tal que $a \leqslant x \leqslant b$. Entonces, dado un $n \in \mathbb{N}$, se obtiene que $a_n \leqslant a \leqslant x \leqslant b \leqslant b_n$. O sea, $x \in I_n$ para todo $n \in \mathbb{N}$, con lo que hemos probado que $\bigcap_{n\in\mathbb{N}} I_n \neq \varnothing$.

Para ver la unicidad, supongamos que

$$\operatorname{ínf}\{\, (b_n - a_n) \mid n \in \mathbb{N} \,\} = 0 \tag{3}$$

y que existen $x, y \in \bigcap_{n\in\mathbb{N}} I_n$ tales que $x \neq y$. Será $|x - y| > 0$ y, por (3), existirá al menos un $n_0 \in \mathbb{N}$ tal que $b_{n_0} - a_{n_0} < |x - y|$. Como $x, y \in I_{n_0} = [a_{n_0}, b_{n_0}]$, tendrá que ser $|x - y| \leqslant b_{n_0} - a_{n_0} < |x - y|$, que es una contradicción. □

Ejemplos.

- $\displaystyle\bigcap_{n\in\mathbb{N}}[0,1/n]=\{0\}$.

  Para ver esto, observemos en primer lugar que $0\in[0,1/n]$ para todo $n\in\mathbb{N}$, así que $0\in\bigcap_{n\in\mathbb{N}}[0,1/n]$. Queda por ver que ningún otro número real pertenece a esta intersección. En efecto, si $x<0$ es evidente que x no pertenece a $[0,1/n]$, cualquiera que sea $n\in\mathbb{N}$, de modo que $x\notin\bigcap_{n\in\mathbb{N}}[0,1/n]$. Por otro lado, si $x>0$, la Propiedad Arquimediana nos asegura la existencia de un $n_0\in\mathbb{N}$ tal que $1/n_0<x$, y para este será $x\notin[0,1/n_0]$. Se sigue de aquí, de nuevo en este caso, que $x\notin\bigcap_{n\in\mathbb{N}}[0,1/n]$.

- $\displaystyle\bigcap_{n\in\mathbb{N}}(0,1/n]=\varnothing$.

  En efecto, es evidente que, si $x\leqslant 0$ entonces $x\notin\bigcap_{n\in\mathbb{N}}(0,1/n]$; por otra parte, si $x>0$, por la Propiedad Arquimediana, podemos encontrar un número natural n tal que $1/n<x$, y para tal n será $x\notin(0,1/n]$, de donde $x\notin\bigcap_{n\in\mathbb{N}}(0,1/n]$. En consecuencia la intersección buscada es vacía. Comprobamos de esta manera que, en el teorema anterior, es imprescindible que los intervalos sean cerrados.

- $\displaystyle\bigcap_{n\in\mathbb{N}}[n,\infty)=\varnothing$.

  En efecto, dado $x\in\mathbb{R}$ la Propiedad Arquimediana nos proporciona un número natural n tal que $n>x$. Por tanto, $x\notin[n,\infty)$ y, así, $x\notin\bigcap_{n\in\mathbb{N}}[n,\infty)$. Se deduce que esta intersección de nuevo es vacía, con lo que se pone de manifiesto que también es necesario que los intervalos sean acotados.

Apéndice

A. Expresión decimal de un número real

Representación decimal finita

En esta exposición seguimos esencialmente la que puede verse en [2, págs. 13–15].

Definición 1.63. Los números reales de la forma

$$a_0+\frac{a_1}{10}+\frac{a_2}{10^2}+\cdots+\frac{a_n}{10^n},$$

donde a_0 es un número entero no negativo y $a_1, \ldots, a_n$ son enteros que satisfacen $0 \leqslant a_j \leqslant 9$, se expresan normalmente de la forma $a_0, a_1 a_2 \ldots a_n$. Esta expresión se llama *representación decimal finita*.

Estos números son racionales, pero no todo número racional tiene una representación decimal finita (véase [2, págs. 13, 14]).

Aproximaciones decimales

Sin embargo, todo número racional positivo, o incluso todo número real positivo, admite una aproximación tan precisa como se desee a través de estos números.

Proposición 1.64 (Aproximaciones decimales finitas de los números reales)**.** *Dado un número real $x \geqslant 0$. para todo $n \in \mathbb{N}$ existe un decimal finito*

$$r_n = a_0, a_1 a_2 \ldots a_n,$$

tal que

$$r_n \leqslant x < r_n + \frac{1}{10^n}.$$

En consecuencia,

$$x = \sup\{ r_n \mid n \in \mathbb{N} \}.$$

Demostración. Para construir los r_n basta tomar

$$a_0 = [x], \qquad a_k = [10^k x] - 10[10^{k-1}x], \quad 1 \leqslant k \leqslant n.$$

Observemos en primer lugar que se verifica

$$r_{n+1} = r_n + \frac{a_{n+1}}{10^n}.$$

Probaremos por inducción que $[10^n x] = 10^n r_n$ para todo $n \in \mathbb{N} \cup \{0\}$. Si conseguimos esto, se tendrá

$$10^n r_n \leqslant 10^n x < 10^n r_n + 1,$$

de donde

$$r_n \leqslant x < r_n + \frac{1}{10^n}.$$

Procedamos a la demostración por inducción anunciada antes. Para $n = 0$, está claro que

$$[10^0 x] = [x] = a_0 = 10^0 r_0.$$

Supongamos que $[10^n x] = 10^n r_n$ para cierto $n \in \mathbb{N} \cup \{0\}$. Entonces, utilizando la definición de a_{n+1}, obtenemos que

$$[10^{n+1}x] = a_{n+1} + 10[10^n x] = a_{n+1} + 10^n r_n = 10^n \Big(r_n + \frac{a_{n+1}}{10^n} \Big) = 10^n r_n,$$

con lo cual concluimos la demostración por inducción.

Por otra parte, x es cota superior de $\{ r_n \mid n \in \mathbb{N} \}$ por construcción, y es la menor de las cotas superiores porque si $y < x$ es posible encontrar un $n \in \mathbb{N}$ de manera que $n > \frac{1}{x-y}$ y tendremos entonces que $10^n > n > \frac{1}{x-y}$. Para este n es $y < x - \frac{1}{10^n} < (r_n + \frac{1}{10^n}) - \frac{1}{10^n} = r_n$. □

Representación decimal infinita

Definición 1.65. Que x es el supremo del conjunto $\{ r_n \mid n \in \mathbb{N} \}$ (donde r_n, $n \in \mathbb{N}$, es como en el teorema anterior) suele expresarse poniendo

$$x = a_0, a_1 a_2 \ldots a_n \ldots$$

y se dice entonces que $a_0, a_1 a_2 \ldots a_n \ldots$ es una *representación decimal infinita* de x.

En ciertos casos, es posible obtener el mismo supremo para dos representaciones decimales infinitas. (Ver [2, pág. 15]).

Definición 1.66. Para $x = 0$, suele tomarse como representación decimal

$$0 = 0, 00 \ldots 0 \ldots$$

Para $x < 0$, se parte de una representación decimal de $-x$ y se coloca un signo $-$ delante.

Hay una presentación más geométrica y computacional en [5].

Si en lugar de potencias de 10 se utilizan potencias de 2, se obtiene la *representación binaria* de los números reales; la *representación hexadecimal* resulta al tomar potencias de 16. Ambas son muy importantes (especialmente la primera) en relación con los ordenadores. Puede verse detalles en [1, cap. 3] y [3, pág. 73 y sigs.]

Referencias

[1] L. Abellanas, A. Galindo, *Métodos de cálculo*, Serie Schaum, McGraw-Hill/Interamericana de España, Madrid, 1989.

En el capítulo 3 se trata el tema de cálculo de las aproximaciones decimales, y se relaciona un poco con la teoría de errores.

[2] T. M. Apostol, *Análisis Matemático* (2a. ed.), Reverté, Barcelona, 1991.

En el capítulo 1 se presentan los axiomas de los reales y de los números complejos (que veremos más adelante). En lugar de partir de los naturales para llegar tras pasos sucesivos a los reales, se procede en el sentido contrario: se parte de los reales, y luego se definen naturales, enteros (y posteriormente racionales) a través del concepto de *conjunto inductivo*.

[3] R. G. Bartle y D. R. Sherbert, *Introducción al Análisis Matemático de una variable*, Limusa, México, 1990.

En el capítulo 2 (apartados 1 y 2) se estudian los números reales de forma axiomática, de manera bastante similar a como lo hacemos nosotros.

[4] M. de Guzmán y B. Rubio, *Problemas, conceptos y métodos del Análisis Matemático I*, Pirámide, 1993.

En el capítulo 1 de este libro se presentan los números reales, aunque desde un punto de vista totalmente diferente. En lugar de presentar los números de forma axiomática, se emplea el método constructivo: después de estudiar los racionales y su expresión decimal periódica, se definen los números reales como números con infinitos decimales, para posteriormente obtener como teoremas todos los axiomas que nosotros hemos utilizado. Este método es muy atractivo (y está contado desde un punto de vista muy didáctico) pero, lamentablemente, exige estudiar antes algunos rudimentos de series. No obstante, es una lectura muy interesante.

[5] P. Lax, S. Burstein y A. Lax, *Calculus with applications and computing*, Springer-Verlag, Berlín, 1976.

Aunque en este libro no se presente el tema con excesivo rigor, sí que resulta interesante su presentación desde un punto de vista geométrico de la representación decimal.

[6] B. Rubio, *Números y convergencia*, B. Rubio, 2006.

Los mismos comentarios que hemos hecho para el libro de Guzmán y Rubio resultan pertinentes aquí. Al ser un libro más moderno, se han pulido algunos detalles.

[7] W. Rudin, *Principios de Análisis Matemático* (3a. ed.), McGraw-Hill, 1976.

En el capítulo 1 se estudian los números reales (y los complejos) de forma axiomática. Los axiomas de orden que utiliza no son exactamente los que nosotros hemos utilizado. Merece la pena comparar. En un apéndice realiza una construcción del conjunto de los números reales (definiendo un número real a través de algo llamado *cortadura de Dedekind*), y obtiene los axiomas como teoremas. Hay que tener un poco de cuidado con la traducción, pues al estar publicado en México, algunos de los términos no coinciden con los que se utilizan aquí. Otra pega de este libro de Rudin es que a veces resulta un poco sucinto en sus demostraciones, dejando para el lector los detalles. No obstante, su rigor hace aconsejable su lectura.

[8] M. Spivak, *Cálculo infinitesimal* (2a. ed.), Reverté, 1994.

Este libro ha sido desde su publicación un auténtico clásico. Su exposición didáctica y amena hace especialmente accesibles todos los conceptos del Análisis. En lo que respecta a los números reales, Spivak los estudia de forma axiomática en el prólogo del libro, y en el epílogo realiza una construcción similar a la del libro de Rudin.

[9] V. A. Zorich, *Mathematical Analysis I*, Springer-Verlag, Berlín, 2003.

Aquí se estudian los números reales en los dos primeros apartados del capítulo 2. Se hace de forma axiomática, y posiblemente sea en este libro en el que el proceso se realiza de forma más rigurosa. Es de destacar su presentación un poco diferente del Axioma de Completitud, en el que no se utiliza el concepto de supremo.