Tema 1

Axiomática de los números reales
Números complejos

1.1. La raíz cuadrada de 2 es irracional

Teorema 1.1.1 *No existe ningún número racional cuyo cuadrado sea* 2*.*

Demostraremos este resultado por reducción al absurdo (se demuestra que el teorema es cierto demostrando que no puede ser falso).

Supongamos que existen enteros p y q que satisfacen $(p/q)^2 = 2$. Podemos suponer que p y q no poseen ningún factor común. Entonces elevando al cuadrado se tendría $p^2/q^2 = 2$, es decir $p^2 = 2q^2$, luego p^2 es un número par y por tanto p es par (el cuadrado de un número impar es impar), $p = 2h$. Ahora podemos escribir $4h^2 = 2q^2$, y también $2h^2 = q^2$, lo que nos dice que también q es par. Hemos demostrado que p y q son ambos pares, cuando habíamos supuesto que no tenían ningún factor común. Esto es una contradicción.

Este descubrimiento afectó a la comprensión de los griegos de la relación existente entre **longitud** geométrica y **número** aritmético.

Antes del descubrimiento anterior se afirmaba que dados dos segmentos $\overline{AB}$ y $\overline{CD}$, la longitud de $\overline{CD}$ es un múltiplo racional de la longitud de $\overline{AB}$. Mirando a la diagonal de un cuadrado unidad (Figura 1.1) se dieron cuenta de que este no era siempre el caso (usando el teorema de Pitágoras). Como los pitagóricos interpretaban implícitamente *número* como *número racional*, se vieron obligados a aceptar que *número* era un concepto estrictamente más débil que longitud.

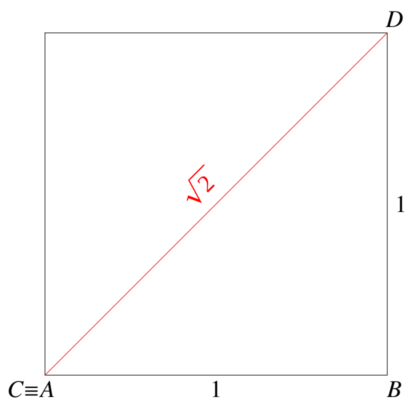

Figura 1.1: $\sqrt{2}$ existe como longitud geométrica.

En vez de abandonar la aritmética en favor de la geometría (como parece que hicieron los griegos) nuestra solución a esta limitación será reforzar el concepto de número pasando de los números racionales a un sistema numérico mayor.

Se comienza con los ***números naturales***

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

(los "números para contar"). Si nos quedamos en los números naturales podemos realizar la suma perfectamente bien, pero debemos extender el sistema a los ***enteros***

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$$

si queremos tener una identidad aditiva (cero) y los inversos aditivos necesarios para definir la resta. Lo siguiente es la multiplicación y la división. El número 1 funciona como la identidad multiplicativa pero para definir la división necesitamos tener inversos multiplicativos. Así pues extendemos de nuevo nuestro sistema a los ***números racionales***

$$\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0 \right\}.$$

Un *cuerpo conmutativo* es un conjunto en el que la suma y la multiplicación son operaciones bien definidas que son conmutativas, asociativas y cumplen la propiedad distributiva $a(b+c) = ab+ac$. Debe haber una identidad aditiva y cada elemento debe tener un inverso aditivo. Finalmente debe haber una identidad multiplicativa y cada elemento no nulo debe tener un inverso multiplicativo. Si excluimos la conmutatividad de la multiplicación tenemos simplemente un *cuerpo*. $\mathbb{Q}$ es un cuerpo conmutativo. Ni $\mathbb{N}$ ni $\mathbb{Z}$ lo son.

Se define también en $\mathbb{Q}$ un *orden* de forma natural. Dados dos números racionales r y s se verifica exactamente una de las siguientes relaciones

$$r < s, \;\; r = s \quad \text{o} \quad r > s.$$

Esta ordenación es transitiva en el sentido de que si $r < s$ y $s < t$ entonces $r < t$, lo que nos lleva a una imagen mental de los números racionales dispuestos de izquierda a derecha a lo largo de una recta numérica. A diferencia de $\mathbb{Z}$, no hay intervalos de espacio vacío. Dados dos números racionales $r < s$, el número racional $\frac{r+s}{2}$ se sitúa entre ambos a medio camino, lo que implica que los números racionales están "densamente juntos".

Recordemos ahora de lo que está desprovisto $\mathbb{Q}$. Por el teorema inicial es claro que no siempre podemos tomar raíces cuadradas. No obstante observemos que usando solamente números racionales es posible aproximar $\sqrt{2}$ bastante bien. Por ejemplo, $(1.414)^2 = 1.999396$. Añadiendo más decimales a nuestra aproximación podemos llegar aún más cerca de un valor para $\sqrt{2}$, pero aun así nos damos cuenta de que hay un "hueco"en la recta numérica racional donde debería estar $\sqrt{2}$. Desde luego hay algunos otros huecos, por ejemplo en $\sqrt{3}$ y en $\sqrt{5}$. Volviendo al dilema de los antiguos matemáticos griegos, si queremos que toda longitud a lo largo de la recta numérica corresponda a un verdadero número se necesita otra extensión de nuestro sistema numérico. Así pues, a la cadena $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$ añadimos los ***números reales*** $\mathbb{R}$.

Construir $\mathbb{R}$ a partir de $\mathbb{Q}$ es un asunto bastante complicado. No entraremos en ello. No es demasiado incorrecto decir que $\mathbb{R}$ se obtiene "rellenando los huecos que hay en $\mathbb{Q}$". Siempre que haya un hueco se define un ***número irracional*** y se coloca dentro de la ordenación que ya existe en $\mathbb{Q}$. Los números reales son entonces la unión de estos números irracionales junto con los racionales.

¿Qué propiedades tiene el conjunto de los números irracionales? ¿Cómo se unen los conjuntos de los números racionales y de los irracionales? ¿Hay algún tipo de simetría entre los racionales y los irracionales o, en algún sentido, podemos afirmar que un tipo de número real es más común que el otro? Hasta ahora el único método que hemos visto para generar ejemplos de números irracionales es el de las raíces cuadradas. Otras raíces son con mucha frecuencia irracionales: por ejemplo $\sqrt[3]{2}$ o $\sqrt[5]{3}$. ¿Pueden todos los números irracionales expresarse como combinaciones algebraicas de raíces n-ésimas y números racionales o hay aún otros números irracionales además de éstos?

¿Qué son entonces los números reales? La respuesta es: ***el sistema de los números reales es el único cuerpo conmutativo ordenado completo***.

1.2. Axiomas para los números reales

El *sistema de los números reales* consta de un conjunto $\mathbb{R}$, un subconjunto $\mathcal{P}$ de $\mathbb{R}$, y dos operaciones binarias

$$\begin{aligned} \mathbb{R}\times\mathbb{R} &\longrightarrow \mathbb{R} \\ (x,y) &\longmapsto x+y \end{aligned} \qquad\qquad \begin{aligned} \mathbb{R}\times\mathbb{R} &\longrightarrow \mathbb{R} \\ (x,y) &\longmapsto xy = x\cdot y \end{aligned}$$

tales que se satisfacen los siguientes axiomas:

Axioma I (leyes conmutativas)

$$x+y=y+x \qquad \text{y} \qquad xy=yx$$

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

Axioma II (leyes asociativas)

$$x+(y+z)=(x+y)+z \qquad \text{y} \qquad x(yz)=(xy)z$$

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

Axioma III (ley distributiva)

$$x(y+z)=xy+xz$$

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

Axioma IV (elementos identidad) Existen dos elementos distintos 0 y 1 en $\mathbb{R}$ tales que

$$0+x=x \qquad \text{y} \qquad 1x=x$$

para todo $x\in\mathbb{R}$.[1]

[1] Es fácil ver que los elementos 0 y 1 que cumplen este axioma son únicos ya que, por ejemplo, si 0 y $0'$ le cumplen, entonces $0=0'+0=0+0'=0'$.

Axioma V (elementos inversos) Si $x \in \mathbb{R}$, existe un único $-x \in \mathbb{R}$ tal que

$$x + (-x) = 0.$$

Si $x \in \mathbb{R}$ y $x \neq 0$, existe un único $x^{-1} \in \mathbb{R}$ tal que

$$xx^{-1} = 1.$$

Teorema 1.2.1 (Leyes cancelativas) *Si $x, y, z, w \in \mathbb{R}$ y $w \neq 0$, entonces*

(1) $x + z = y + z$ *implica* $x = y$,

(2) $xw = yw$ *implica* $x = y$.

Teorema 1.2.2 *Si $x, y, z, w \in \mathbb{R}, z \neq 0, w \neq 0$, entonces*

(1) $x0 = 0$,

(2) $-(-x) = x$,

(3) $(w^{-1})^{-1} = w$,

(4) $(-1)x = -x$,

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

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

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

(8) $(x/z)(y/w) = (xy)/(zw)$,[2]

(9) $(x/z) + (y/w) = (wx + zy)/(zw)$.

Los axiomas I-V expresan que $\mathbb{R}$ es un *cuerpo conmutativo*.

Los tres axiomas restantes se refieren al subconjunto $\mathcal{P}$ de $\mathbb{R}$ que induce un orden en $\mathbb{R}$.

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

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

[2] Usualmente escribimos a/b o $\frac{a}{b}$ para denotar ab^{-1}.

Definición 1.2.1 *Los elementos de $\mathcal{P}$ se llaman **números positivos** y los elementos de $-\mathcal{P}$ se llaman **números negativos**. Si $x, y \in \mathbb{R}$, $x < y$ e $y > x$ significan que $y - x \in \mathcal{P}$.*[3] *Se escribe $x \leq y$ e $y \geq x$ para expresar que o bien $y - x \in \mathcal{P}$ o bien $y = x$.*

Teorema 1.2.3 *Para todos $x, y, z \in \mathbb{R}$ se tiene*

(1) (transitividad) $x < y$ e $y < z$ implican $x < z$,

(2) (tricotomía) se verifica exactamente una de las relaciones $x < y, x = y, x > y$,

(3) $x < y$ implica $x + z < y + z$,

(4) $x < y, z > 0$ implican $xz < yz$,

(5) $x < y, z < 0$ implican $xz > yz$,

(6) $1 > 0$ y $-1 < 0$,

(7) $z > 0$ implica $1/z > 0$,

(8) $0 < x < y$ implica $0 < 1/y < 1/x$.

Es fácil establecer teoremas similares al anterior en los que algunos casos de $<$ se reemplazan por $\leq$. En particular, se tiene

Teorema 1.2.4 *Si $a, b, c, d \in \mathbb{R}$ y $a \leq b$ y $c \leq d$, entonces $a + c \leq b + d$.*

Con frecuencia, los números reales se representan geométricamente como puntos de una recta, denominada *recta real*. Se elige un punto para que represente el 0 y otro a la derecha de él para que represente el 1. Esta elección determina la escala. A cada punto de la recta real corresponde un número real y uno sólo, y recíprocamente, cada número real está representado por un punto de la recta real y uno sólo. Es usual referirse al punto x en vez de referirse al punto correspondiente al número real x.

La ordenación admite una interpretación geométrica simple. Si $x < y$, el punto x está a la izquierda del punto y. Los números positivos están a la derecha del 0 y los números negativos están a la izquierda del 0. Si $a < b$, un punto x satisface $a < x < b$ si, y sólo si, x está entre a y b.

Definición 1.2.2 *Dados dos números reales a y b tales que $a < b$, se definen cuatro intervalos de extremos a y b de la forma siguiente*

$$\begin{aligned}
(a, b) &= \{x \in \mathbb{R} : a < x < b\} \\
[a, b] &= \{x \in \mathbb{R} : a \leq x \leq b\} \\
(a, b] &= \{x \in \mathbb{R} : a < x \leq b\} \\
[a, b) &= \{x \in \mathbb{R} : a \leq x < b\}.
\end{aligned}$$

El primero se denomina intervalo abierto y el segundo intervalo cerrado. Los otros dos se llaman semiabiertos.

[3] Escribimos $y - x$ para denotar $y + (-x)$.

Se definen también los intervalos "infinitos"

$$\begin{aligned}
(a,+\infty) &= \{x \in \mathbb{R} : a < x\} \text{ (abierto)}\\
[a,+\infty) &= \{x \in \mathbb{R} : a \leq x\} \text{ (cerrado)}\\
(-\infty,b) &= \{x \in \mathbb{R} : x < b\} \text{ (abierto)}\\
(-\infty,b] &= \{x \in \mathbb{R} : x \leq b\} \text{ (cerrado)}\\
(-\infty,+\infty) &= \mathbb{R}.
\end{aligned}$$

(Los símbolos $+\infty$ y $-\infty$ se utilizan aquí tan sólo por conveniencia de notación y no deben ser considerados como números reales. Más adelante extenderemos el sistema de los números reales incluyendo estos dos símbolos).

Una propiedad obvia de los intervalos es que si dos puntos x, y con $x < y$ pertenecen a un intervalo I, entonces cualquier punto situado entre ellos también pertenece a I. Es decir, si se tiene $x < t < y$, entonces el punto t pertenece al mismo intervalo que x e y. En otras palabras, si x e y pertenecen a un intervalo I, entonces el intervalo $[x, y]$ está contenido en I. El teorema siguiente nos dice que un subconjunto de $\mathbb{R}$ que posea esta propiedad debe ser un intervalo.

Teorema 1.2.5 *Si S es un subconjunto de $\mathbb{R}$ que contiene al menos dos puntos y tiene la propiedad*

$$(x, y \in S, x < y) \Longrightarrow [x, y] \subset S,$$

entonces S es un intervalo.

Definición 1.2.3 *Para cada $x \in \mathbb{R}$ se define el* ***valor absoluto*** *de x como el número $|x|$ dado por*

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

Lema 1.2.1 *Si $a, b \in \mathbb{R}$ y $b \geq 0$, entonces $|a| \leq b$ si, y sólo si, $-b \leq a \leq b$.*

Teorema 1.2.6 *Para números reales cualesquiera x e y se tiene*

(1) $|xy| = |x||y|$,

(2) $|x + y| \leq |x| + |y|$,

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

Nota

La importante desigualdad $|x + y| \leq |x| + |y|$ se emplea con frecuencia de la manera siguiente. Dados tres números reales a, b y c, se tiene

$$|a - b| = |(a - c) + (c - b)|.$$

Entonces

$$|(a - c) + (c - b)| \leq |a - c| + |c - b|$$

de modo que

$$|a-b| \leq |a-c| + |c-b|.$$

Es claro que $|x-y|$ es la distancia entre los puntos x e y de la recta real.

Los siete axiomas que hemos presentado expresan que $\mathbb{R}$ es un *cuerpo conmutativo ordenado*. Ahora bien, $\mathbb{Q}$ también lo es. Lo que distingue a los números reales de los racionales es el siguiente axioma:

Axioma VIII (axioma de completitud) Todo conjunto no vacío de números reales acotado superiormente tiene un supremo.

¿Qué significa esto exactamente?

Definición 1.2.4 *Sea A un conjunto no vacío de números reales. Un número $b \in \mathbb{R}$ se llama* ***cota superior*** *(resp.* ***inferior****) de A si $x \leq b$ (resp. $b \leq x$) para todo $x \in A$. En el caso de que exista un tal b se dice que A está* ***acotado superiormente*** *(resp.* ***inferiormente****). Si A tiene tanto una cota superior como una cota inferior, entonces se dice que A es* ***acotado****.*

Si una cota superior (resp. inferior) b pertenece también a A entonces recibe el nombre de ***elemento máximo*** *(resp.* ***mínimo****) de A. Es claro que a lo sumo puede existir un b que sea elemento máximo (resp. mínimo) de A. Si existe, se escribe*

$$b = \text{máx}\, A \quad (\textit{resp. } b = \text{mín}\, A)$$

Un número $s \in \mathbb{R}$ se llama ***supremo*** *(o* ***extremo superior*** *o* ***mínima cota superior****) de A si s tiene las dos propiedades siguientes:*

(1) s es cota superior de A,

(2) si b es cota superior de A, entonces $s \leq b$.

Es claro que A puede tener a lo sumo un supremo. Si A tiene un supremo s se escribe

$$s = \sup A.$$

De forma análoga, un número $i \in \mathbb{R}$ se llama ***ínfimo*** *(o* ***extremo inferior*** *o* ***máxima cota inferior****) de A si i tiene las dos propiedades siguientes:*

(1) i es cota inferior de A,

(2) si b es cota inferior de A, entonces $b \leq i$.

Es claro que A puede tener a lo sumo un ínfimo. Si A tiene un ínfimo i se escribe

$$i = \text{ínf}\, A.$$

Ejemplos

(1) Sea $A = [1, +\infty) = \{x \in \mathbb{R} : x \geq 1\}$. Cualquier número menor o igual que 1 es una cota inferior de A y $1 = \text{ínf}\, A$, pero A no tiene cotas superiores.

(2) Consideremos el intervalo abierto

$$A = (0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$$

y el intervalo cerrado

$$B = [0, 1] = \{x \in \mathbb{R} : 0 \leq x \leq 1\}.$$

Ambos conjuntos están acotados superiormente (e inferiormente) y ambos tienen el mismo supremo, a saber, 1. Ahora bien, A no tiene máximo y B sí lo tiene: $\max B = 1$. Así pues, el supremo puede existir y no ser un máximo, pero cuando existe el máximo entonces es también el supremo. De forma análoga $\inf A = 0 \notin A$, $\inf B = \min B = 0$.

Como consecuencia del axioma VIII se tiene el siguiente

Teorema 1.2.7 *Todo conjunto no vacío de números reales acotado inferiormente tiene un ínfimo.*

El siguiente teorema proporciona una caracterización útil del supremo.

Teorema 1.2.8 *Sea A un conjunto no vacío de números reales y supongamos que $s \in \mathbb{R}$ es una cota superior de A. Entonces $s = \sup A$ si, y sólo si, para cada $\varepsilon > 0$ existe $x \in A$ tal que $x > s - \varepsilon$.*

Así pues, $\mathbb{R}$ es un *cuerpo conmutativo ordenado que verifica el axioma VIII (axioma de completitud o principio del supremo).*

Suponemos la existencia de un objeto $\mathbb{R}$ que satisface los ocho axiomas anteriores. Cualquier construcción con números reales y cualquier otra propiedad se puede obtener a partir de ellos. Además, si construimos un conjunto $\mathbb{R}'$ que verifique esos ocho axiomas, se puede comprobar que esencialmente $\mathbb{R}$ y $\mathbb{R}'$ son iguales (isomorfos). Por estas dos razones se dice que los axiomas I-VIII *caracterizan* a los números reales.

1.3. Los números naturales

Hablando sin mucho rigor, un número natural es un número real que puede expresarse como la suma de un montón de 1's. Pero seamos más precisos.

Definición 1.3.1 *Un conjunto $I \subset \mathbb{R}$ se llama* ***conjunto inductivo*** *si*

(1) $1 \in I$ *y*

(2) $x \in I$ *implica* $x + 1 \in I$.

Observemos que $\mathbb{R}$ es un conjunto inductivo y también lo es $\{t \in \mathbb{R} : t \geq 1\}$. Denotemos por $\mathcal{I}$ la familia de todos los subconjuntos inductivos de $\mathbb{R}$ y pongamos $\mathbb{N} = \cap \mathcal{I}$, es decir

$$\mathbb{N} = \{x \in \mathbb{R} : x \in I \text{ para todo conjunto inductivo } I \subset \mathbb{R}\}.$$

Los elementos de $\mathbb{N}$ se llaman ***números naturales*** (o ***enteros positivos***).

Es claro que si I es un conjunto inductivo contenido en $\mathbb{R}$, entonces $\mathbb{N} \subset I$. Observemos también que $1 \in \mathbb{N}$ y si $x \in \mathbb{N}$ entonces $x \in I$ para todo $I \in \mathcal{I}$, de modo que $x + 1 \in I$ para todo $I \in \mathcal{I}$ y por consiguiente $x + 1 \in \mathbb{N}$. Por tanto $\mathbb{N}$ es un conjunto inductivo.

Se definen

$$2 = 1 + 1,\ 3 = 2 + 1,\ 4 = 3 + 1, \ldots$$

Teorema 1.3.1 (Principio de inducción matemática) *Sea $S \subset \mathbb{N}$ tal que*

(1) $1 \in S$ *y*

(2) $x \in S$ *implica* $x + 1 \in S$.

Entonces $S = \mathbb{N}$.

Este principio permite establecer propiedades importantes de $\mathbb{N}$.

Teorema 1.3.2 *Para cada* $n \in \mathbb{N}$ *tenemos*

(1) $1 \leq n$,

(2) $n > 1$ *implica* $n - 1 \in \mathbb{N}$,

(3) $x \in \mathbb{R}, x > 0, x + n \in \mathbb{N}$ *implican* $x \in \mathbb{N}$,

(4) $m \in \mathbb{N}, m > n$ *implican* $m - n \in \mathbb{N}$,

(5) $a \in \mathbb{R}, n - 1 < a < n$ *implican* $a \notin \mathbb{N}$.

Teorema 1.3.3 *Si* $m, n \in \mathbb{N}$, *entonces* $m + n \in \mathbb{N}$ *y* $mn \in \mathbb{N}$.

Una afirmación lógicamente equivalente al principio de inducción matemática es el

Teorema 1.3.4 (Principio de buena-ordenación) *Si A es un subconjunto no vacío de $\mathbb{N}$, entonces A tiene un elemento mínimo.*

El manejo y la idea misma del principio de inducción queda claro con el siguiente experimento. Colocamos sobre una mesa las fichas de dominó de pie y en fila, un poco separadas pero de tal modo que, si cae una de ellas, ésta empuja y hace caer a la siguiente. Si efectivamente podemos estar seguros de que

(1) cae la primera, y

(2) están colocadas de modo que la caída de una ficha provoca la caída de la siguiente,

entonces está claro que podemos estar seguros de que caen todas las fichas.

Los números naturales se pueden concebir como fichas de dominó. El principio de inducción sirve para asegurarnos que una determinada propiedad $P(n)$ es verdadera para todos ellos, aplicándolo al conjunto

$$S = \{n \in \mathbb{N} : P(n) \text{ es verdadera}\}.$$

Así pues, para demostrar que $P(n)$ es verdadera para todo $n \in \mathbb{N}$ tenemos que demostrar

(1) $P(1)$ es cierta (1 satisface la propiedad), y

(2) $P(k)$ cierta, implica $P(k + 1)$ cierta (si la propiedad se satisface para un número k, entonces también se satisface para $k + 1$).

Hay una forma alternativa, lógicamente equivalente, que es:

(1) $P(1)$ es verdadera, y

(2′) si $P(1), P(2), \ldots, P(k)$ son verdaderas, entonces $P(k+1)$ es verdadera,

entonces $P(n)$ es verdadera para todo $n \in \mathbb{N}$.

En general, fijado un número natural n_0, podemos establecer que una propiedad $P(n)$ es verdadera para cada natural $n \geq n_0$ cuando se cumple

(1) $P(n_0)$ es verdadera, y

(2) si $P(k)$ es verdadera ($k \geq n_0$), entonces $P(k+1)$ es verdadera,

o bien

(1) $P(n_0)$ es verdadera, y

(2′) si $P(n_0), P(n_0+1), \ldots, P(k)$ son verdaderas ($k \geq n_0$), entonces $P(k+1)$ es verdadera.

Ejemplos

(a) Al observar las siguientes relaciones

$$\begin{aligned} 1 = {} & 1 && = \frac{1 \cdot 2}{2} \\ 1+2 = {} & 3 && = \frac{2 \cdot 3}{2} \\ 1+2+3 = {} & 6 && = \frac{3 \cdot 4}{2} \\ 1+2+3+4 = {} & 10 && = \frac{4 \cdot 5}{2} \\ 1+2+3+4+5 = {} & 15 && = \frac{5 \cdot 6}{2} \end{aligned}$$

podemos sospechar que se verifique en general

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

¿Cómo podemos confirmar esta conjetura con certeza? Se trata de una propiedad que parece cumplir cada número natural n: *si sumamos los n primeros números naturales el resultado es* $\frac{n(n+1)}{2}$. Podemos proceder a demostrar por inducción esta afirmación. La propiedad $P(n)$ es la frase en cursiva.

(1) Nos aseguramos de que $P(1)$ es cierta, es decir

$$1 = \frac{1 \cdot 2}{2},$$

lo cual es evidente.

(2) Trataremos de asegurarnos de que, si $P(k)$ es cierta, es decir, si

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

entonces $P(k+1)$ también lo es. Decir que $P(k+1)$ es cierta es decir que

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

¿Es esto verdadero? Observamos que, si $P(k)$ es verdadera

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

Y esto es precisamente $P(k+1)$.

Concluimos de (1) y (2) que $P(n)$ es cierta para cada n.

(b) Deseamos saber cuánto vale la suma de los n primeros números impares. Experimentamos un poco y observamos que

$$\begin{aligned} 1 &= 1 &= 1^2\\ 1+3 &= 4 &= 2^2\\ 1+3+5 &= 9 &= 3^2\\ 1+3+5+7 &= 16 &= 4^2\\ 1+3+5+7+9 &= 25 &= 5^2 \end{aligned}$$

Resulta el cuadrado de 1 cuando hay un número, el cuadrado de 2 cuando sumamos los dos primeros impares... Surge la conjetura de que la suma de los n primeros impares será n^2.

El impar n-ésimo es el anterior a $2n$, es decir, $2n-1$. Llegamos pues a nuestra proposición $P(n)$:

$$1+3+5+\cdots+(2n-1)=n^2.$$

¿Será verdadera para cada n? Procederemos por inducción.

(1) $P(1)$ es cierta: $1=1^2$.

(2) Trataremos de asegurarnos de que, si

$$1+3+5+\cdots+(2k-1)=k^2$$

entonces

$$1+3+5+\cdots+(2k-1)+(2k+1)=(k+1)^2.$$

Pero esto es fácil, pues

$$1+3+5+\cdots+(2k-1)+(2k+1)=k^2+(2k+1)=(k+1)^2.$$

(c) La proposición $2n<2^n-1$ no es verdadera cuando n es 1 o 2, y sí lo es cuando n es 3,4 o 5, y parece serlo también para cualquier $n\geq 3$. Esto se puede probar haciendo uso del principio de inducción.

(1) Comprobamos que $P(3)$ es verdadera. Efectivamente, se verifica que $2\cdot 3<2^3-1$.

(2) Tratamos de ver que si $P(k)$ es verdadera ($k \geq 3$), entonces $P(k+1)$ también lo es. En efecto, si suponemos $2k < 2^k - 1$, resulta

$$2(k+1) = 2k + 2 < 2^k - 1 + 2 < 2^k - 1 + 2^k = 2^{k+1} - 1.$$

El principio de inducción establece entonces que $P(n)$ es verdadera para cada $n \geq 3$.

Concluimos esta sección con dos propiedades importantes, consecuencias del axioma de completitud.

Teorema 1.3.5 (Propiedad arquimediana) *Si $a, b \in \mathbb{R}$ y $a > 0$, entonces existe $n \in \mathbb{N}$ tal que $na > b$. En particular, $\mathbb{N}$ no está acotado superiormente.*

Geométricamente, esta propiedad significa que cada segmento, tan largo como se quiera, puede ser recubierto por un número finito de segmentos de longitud positiva dada, tan pequeña como se quiera (una regla corta puede medir distancias tan largas como se quiera colocándola consecutivamente).

Teorema 1.3.6 (Principio de los intervalos encajados) *Sea $\{I_n : n \in \mathbb{N}\}$ una familia de intervalos de $\mathbb{R}$ cerrados tales que $I_{n+1} \subset I_n$ para cada $n \in \mathbb{N}$. Entonces $\bigcap_{n=1}^{\infty} I_n \neq \emptyset$.*

Si además se verifica que dado cualquier número real $\varepsilon > 0$ la longitud de I_n es menor que ε para algún n, entonces $\bigcap_{n=1}^{\infty} I_n = \{z\}$ para algún $z \in \mathbb{R}$.

1.4. Los enteros

Definición 1.4.1 *Un número real x se llama **entero** si $x = 0$ o $x \in \mathbb{N}$ o $-x \in \mathbb{N}$. El conjunto de todos los enteros se designa por $\mathbb{Z}$.*

Teorema 1.4.1 *Si $m, n \in \mathbb{Z}$, entonces $-n \in \mathbb{Z}$,$m + n \in \mathbb{Z}$ y $mn \in \mathbb{Z}$.*

La propiedad arquimediana y el principio de buena ordenación permiten demostrar la existencia de la *función parte entera.*

Teorema 1.4.2 *Sea $x \in \mathbb{R}$. Entonces existe un único entero n tal que*

$$n \leq x < n + 1, \quad x - 1 < n \leq x.$$

*Este entero n se denota por $[x]$ y se llama la **parte entera de x**.*[4]

Definimos ahora las potencias enteras de números reales. La definición y las propiedades siguientes son válidas en cualquier cuerpo conmutativo, en particular para los números complejos, que veremos más adelante.

Definición 1.4.2 *Sea $x \in \mathbb{R}$. Se define $x^0 = 1$ (si $x \neq 0$), $x^1 = x$ y $x^{n+1} = x^n x$ para $n \in \mathbb{N}$. Si $x \neq 0$ y $n \in \mathbb{N}$, se define $x^{-n} = 1/x^n$.*

[4] Así, $[x]$ es el mayor entero que es menor o igual que x.

Teorema 1.4.3 (Leyes de los exponentes) *Sean* $x, y \in \mathbb{R} \setminus \{0\}$ *y* $m, n \in \mathbb{Z}$. *Entonces*

(1) $x^m x^n = x^{m+n}$,

(2) $x^n y^n = (xy)^n$,

(3) $(x^m)^n = x^{mn}$.

Si $n > 0, x > 0, y > 0$, *entonces*

(4) $x < y$ *si, y sólo si,* $x^n < y^n$.[5]

Y concluimos esta sección con un resultado importante:

Teorema 1.4.4 (Algoritmo de la división) *Si* $n, b \in \mathbb{Z}$ *con* $b > 0$, *entonces existen enteros únicos* q *y* r *tales que*

(1) $n = bq + r$,

(2) $0 \leq r < b$.

1.5. Raíces

El axioma de completitud permite demostrar la existencia de raíces n-ésimas de números reales no negativos.

Teorema 1.5.1 *Sea* $a \geq 0$ *un número real y sea* $n \in \mathbb{N}$. *Entonces existe un único número real* x *tal que* $x \geq 0$ *y* $x^n = a$.

Este número x se llama la *raíz n-ésima* (no negativa) de a y se designa por $\sqrt[n]{a}$ o por $a^{1/n}$. En el caso $n = 2$ escribimos $\sqrt{a}$ en lugar de $\sqrt[2]{a}$.

Corolario 1.5.1 *Si* $a \geq 0$ *y* $b \geq 0$, *entonces* $\sqrt[n]{ab} = \sqrt[n]{a}\,\sqrt[n]{b}$.

Nota

Sea $n \in \mathbb{N}$.

(1) Supongamos que n es impar. Si $a < 0$ entonces $-a > 0$ y por tanto existe un único $y \in \mathbb{R}$ tal que $y > 0$ e $y^n = -a$. Ahora bien

$$y^n = -a \Leftrightarrow -y^n = a \Leftrightarrow (-y)^n = a.$$

Así pues, si $a < 0$ existe un único $x \in \mathbb{R}$ tal que $x < 0$ y $x^n = a$. Este x recibe el nombre de raíz n-ésima de a.

(2) Si n es par se tiene que $x^n \geq 0$ para todo $x \in \mathbb{R}$, luego los números reales negativos no tienen raíz n-ésima real.

[5] Consecuencia inmediata de esta propiedad es que si $n > 0, x > 0, y > 0$ entonces $x < y$ si, y sólo si, $y^{-n} < x^{-n}$.

1.6. Números racionales e irracionales

Definición 1.6.1 *Un **número racional** es un número real x que puede expresarse en la forma $x = a/b$, donde a y b son enteros y $b \neq 0$. El conjunto de todos los números racionales se designa por $\mathbb{Q}$. Los números de $\mathbb{R} \setminus \mathbb{Q}$ se llaman **números irracionales**.*[6]

Teorema 1.6.1 *Si x e y son números racionales, entonces también lo son $-x, x+y, xy$, y (para $x \neq 0$) x^{-1}. Así, $\mathbb{Q}$ es un subcuerpo de $\mathbb{R}$: satisface los axiomas I-V.*

A diferencia de los enteros, ningún número racional tiene un vecino racional que sea el más próximo:

Teorema 1.6.2 ($\mathbb{Q}$ es denso en $\mathbb{R}$) *Si $x, y \in \mathbb{R}$ con $x < y$, entonces existe un número racional z tal que $x < z < y$.*

Y también

Teorema 1.6.3 ($\mathbb{R} \setminus \mathbb{Q}$ es denso en $\mathbb{R}$) *Si $x, y \in \mathbb{R}$ con $x < y$, entonces existe un número irracional z tal que $x < z < y$.*

Sea a un número real positivo. Es fácil ver que si m, n, p, q son números enteros, $n > 0, q > 0$, y $r = m/n = p/q$, entonces

$$(a^m)^{1/n} = (a^p)^{1/q}.$$

Por tanto tiene sentido la siguiente definición:

Definición 1.6.2 *Sea $a > 0$ y $r = m/n \in \mathbb{Q}$. Se define*

$$a^r = (a^m)^{1/n}.$$

Teorema 1.6.4 (Leyes de los exponentes) *Sean x e y números reales positivos y $r, s \in \mathbb{Q}$. Entonces*

(1) $x^r x^s = x^{r+s}$,

(2) $x^r y^r = (xy)^r$,

(3) $(x^r)^s = x^{rs}$,

(4) *si $r > 0$ entonces $x < y$ si, y sólo si, $x^r < y^r$, y*
si $r < 0$ entonces $x < y$ si, y sólo si, $y^r < x^r$.

Si $r < s$, se tiene

(5) *si $x > 1$ entonces $x^r < x^s$, y*
si $0 < x < 1$ entonces $x^s < x^r$.

[6]El conjunto de los números irracionales se designa también por $\mathbb{I}$.

1.7. Representaciones decimales de los números reales

Un número real de la forma

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

donde a_0 es un entero no negativo y $a_1, \ldots, a_n$ son enteros que satisfacen $0 \leq a_i \leq 9$, se expresa usualmente de la siguiente forma:

$$r = a_0.a_1 a_2 \ldots a_n \,.$$

Dicha expresión recibe el nombre de *representación decimal finita de* r. Por ejemplo:

$$\frac{1}{2} = \frac{5}{10} = 0.5, \qquad \frac{1}{50} = \frac{2}{10^2} = 0.02, \qquad \frac{29}{4} = 7 + \frac{2}{10} + \frac{5}{10^2} = 7.25\,.$$

Los números reales de este tipo son necesariamente racionales y, de hecho, todos ellos son de la forma $r = a/10^n$, donde a es un entero. Sin embargo no todos los números racionales pueden expresarse mediante representaciones decimales finitas. Por ejemplo, si $1/3$ pudiese expresarse así, tendríamos que $1/3 = a/10^n$, es decir, $3a = 10^n$ para un cierto entero a. Pero esto es imposible, ya que 3 no divide a ninguna potencia de 10.

Hacemos uso ahora del axioma de completitud para demostrar que los números reales pueden aproximarse, con la exactitud que se desee, por medio de números racionales que admitan representación decimal finita.

Teorema 1.7.1 *Supongamos que $x \geq 0$. Entonces, para todo entero $n \geq 1$, existe un decimal finito $r_n = a_0.a_1 a_2 \ldots a_n$ tal que*

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

Demostración. Sea S el conjunto de todos los enteros no negativos menores o iguales que x. S es no vacío pues $0 \in S$, y está acotado superiormente por x. Por lo tanto, S admite un supremo: $a_0 = \sup S = [x]$. Se tiene

$$a_0 \leq x < a_0 + 1.$$

Sea ahora $a_1 = [10x - 10a_0]$. Como es $0 \leq 10x - 10a_0 = 10(x - a_0) < 10$, tenemos que $0 \leq a_1 \leq 9$ y $a_1 \leq 10x - 10a_0 < a_1 + 1$. En otras palabras, a_1 es el mayor entero que satisface

$$a_0 + \frac{a_1}{10} \leq x < a_0 + \frac{a_1 + 1}{10}\,.$$

En general, habiendo elegido $a_1, \ldots, a_{n-1}$ con $0 \leq a_i \leq 9$, sea a_n el mayor entero que satisfaga las desigualdades

$$a_0 + \frac{a_1}{10} + \cdots + \frac{a_n}{10^n} \leq x < a_0 + \frac{a_1}{10} + \cdots + \frac{a_n + 1}{10^n}\,. \tag{1}$$

Entonces $0 \leq a_n \leq 9$ y tendremos

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

donde $r_n = a_0.a_1 a_2 \ldots a_n$. Esto completa la demostración. Es fácil verificar que x es, de hecho, el supremo del conjunto $\{r_n : n \in \mathbb{N}\}$.

Los enteros $a_0, a_1, a_2, \ldots$ obtenidos en la demostración del teorema anterior pueden utilizarse para definir una representación decimal infinita de x. Escribiremos

$$x = a_0.a_1 a_2 \ldots$$

para indicar que a_n es el mayor entero que satisface (1). Por ejemplo, si $x = 1/8$, obtendremos $a_0 = 0, a_1 = 1, a_2 = 2, a_3 = 5$ y $a_n = 0$ para todo $n \geq 4$. Por lo tanto, podemos escribir

$$\frac{1}{8} = 0.125000\ldots$$

Si intercambiamos los signos de desigualdad $\leq$ y $<$ en (1) obtenemos una definición ligeramente diferente de representación decimal. Los decimales finitos r_n satisfacen $r_n < x \leq r_n + \frac{1}{10^n}$, sin embargo los dígitos $a_0, a_1, a_2, \ldots$ necesarios no son los mismos que en (1). Por ejemplo, si aplicamos esta segunda definición a $x = 1/8$, obtenemos la representación decimal infinita

$$\frac{1}{8} = 0.124999\ldots$$

El que un número real admita dos representaciones decimales distintas es un simple ejemplo del hecho de que dos conjuntos diferentes de números reales pueden tener el mismo supremo.

1.8. Extensión del sistema de los números reales

Definición 1.8.1 *Sean $+\infty$ (más infinito) y $-\infty$ (menos infinito) dos objetos fijos distintos ninguno de los cuales es un elemento de $\mathbb{R}$. Se llama recta real ampliada o extensión del sistema de los números reales al conjunto*

$$\mathbb{R}^\sharp = \mathbb{R} \cup \{+\infty, -\infty\}.$$

Introducimos una ordenación en $\mathbb{R}^\sharp$ como sigue. Para $x, y \in \mathbb{R}$, $x < y$ tiene su significado usual y escribimos $x < +\infty, x > -\infty, -\infty < +\infty$. Los símbolos $\leq, >, \geq$ tienen significados obvios.

Introducimos también en $\mathbb{R}^\sharp$ algunas operaciones aritméticas. Para $x, y \in \mathbb{R}$,$x + y, x - y$ y xy tienen sus significados usuales. Si $x \in \mathbb{R}$ definimos

$$x + (+\infty) = (+\infty) + x = x - (-\infty) = +\infty,$$

$$x + (-\infty) = (-\infty) + x = x - (+\infty) = -\infty,$$

$$\frac{x}{+\infty} = \frac{x}{-\infty} = 0.$$

Si $x > 0$,

$$(+\infty) \cdot x = x \cdot (+\infty) = +\infty,$$

$$x \cdot (-\infty) = (-\infty) \cdot x = -\infty.$$

Si $x < 0$,

$$(+\infty) \cdot x = x \cdot (+\infty) = -\infty,$$

$$x \cdot (-\infty) = (-\infty) \cdot x = +\infty.$$

Definimos también

$$(+\infty) + (+\infty) = (+\infty) \cdot (+\infty) = (-\infty) \cdot (-\infty) = +\infty,$$

$$(-\infty) + (-\infty) = (+\infty) \cdot (-\infty) = (-\infty) \cdot (+\infty) = -\infty.$$

Definición 1.8.2 *Sea $A \subset \mathbb{R}^\sharp$. Si A no está acotado superiormente por un número real, entonces decimos que $+\infty$ es el supremo de A y escribimos* $\sup A = +\infty$. *Si A no está acotado inferiormente por un número real decimos que $-\infty$ es el ínfimo de A y escribimos* $\inf A = -\infty$. *Así pues todo subconjunto no vacío de $\mathbb{R}^\sharp$ tiene un supremo y un ínfimo en $\mathbb{R}^\sharp$.*

Definición 1.8.3 *Para $a \leq b$ en $\mathbb{R}^\sharp$, definimos los cuatro intervalos que tienen por extremo izquierdo a y por extremo derecho b:*

$$\begin{aligned}(a,b) &= \{x \in \mathbb{R}^\sharp : a < x < b\}\\ [a,b) &= \{x \in \mathbb{R}^\sharp : a \leq x < b\}\\ (a,b] &= \{x \in \mathbb{R}^\sharp : a < x \leq b\}\\ [a,b] &= \{x \in \mathbb{R}^\sharp : a \leq x \leq b\}.\end{aligned}$$

(a,b) se llama intervalo abierto *y $[a,b]$* intervalo cerrado. *Observemos que si $a = b$ entonces $[a,b] = \{a\}$ mientras que los otros tres son vacíos. La* longitud *de cada uno de estos intervalos es $b - a$.*

1.9. Los números complejos

Definición 1.9.1 *Un* ***número complejo*** *es un par ordenado (a,b), donde a y b son números reales. El conjunto de todos los números complejos se designa por $\mathbb{C}$. Para $z = (a,b)$ y $w = (c,d)$ en $\mathbb{C}$, escribimos $z = w$ si, y sólo si, $a = c$ y $b = d$. Se definen*

$$\begin{aligned}z + w &= (a + c, b + d),\\ zw &= (ac - bd, ad + bc).\end{aligned}$$

Teorema 1.9.1 *Se verifican los axiomas I-V con $\mathbb{R}$ reemplazado por $\mathbb{C}$, 0 reemplazado por $(0,0)$, y 1 reemplazado por $(1,0)$. Es decir, $\mathbb{C}$ es un cuerpo conmutativo.*

Teorema 1.9.2 *Con los reemplazamientos señalados en el teorema 1.9.1, los teoremas 1.2.1 y 1.2.2 siguen siendo válidos.*

El inverso aditivo $-z$ de z es $-z = (-a, -b)$ y, si $z \neq (0,0)$, el inverso multiplicativo z^{-1} (o $1/z$) de z viene dado por

$$z^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right).$$

Observemos que si $a, b \in \mathbb{R}$, entonces

$$\begin{aligned}(a,0) + (b,0) &= (a + b, 0),\\ (a,0)(b,0) &= (ab, 0),\\ -(a,0) &= (-a, 0),\end{aligned}$$

y si $a \neq 0$,

$$(a,0)^{-1} = (a^{-1}, 0).$$

Así pues los números complejos de la forma $(a,0)$ tienen las mismas propiedades aritméticas que los números reales a. El conjunto de los números complejos de la forma $(a,0)$ constituye un subcuerpo de $\mathbb{C}$ estructuralmente indistinguible del cuerpo de los números reales (isomorfo a $\mathbb{R}$, según se expresa en el lenguaje del Álgebra). Por esta razón identificaremos $(a,0)$ con a. Con este convenio, $\mathbb{R}$ se considera como un subcuerpo de $\mathbb{C}$ y en este sentido puede decirse que $\mathbb{C}$ es una ampliación de $\mathbb{R}$.

Definición 1.9.2 *El número complejo* $(0,1)$ *se designa por* i *y se llama* ***unidad imaginaria****.*

Observemos que
$$i^2 = (0,1)(0,1) = (-1,0) = -1$$
(en $\mathbb{C}$, la ecuación $x^2 = -1$ tiene solución; i es una solución).

Si $a, b \in \mathbb{R}$ se tiene
$$(a,b) = (a,0) + (0,b) = (a,0) + (b,0)(0,1) = a + bi.$$
Los números complejos de la forma $(0,b) = bi$ se llaman *imaginarios puros*.

Si $z = a + bi$ es un número complejo, a se llama la *parte real* de z y b la *parte imaginaria* de z y se escribe
$$a = \mathrm{Re}\,(z), \qquad b = \mathrm{Im}\,(z).$$

Existe una gran diferencia entre $\mathbb{R}$ y $\mathbb{C}$. El cuerpo de los números complejos es "no ordenable"en el sentido de que no existe un subconjunto $\mathcal{P}$ de $\mathbb{C}$ que satisfaga los axiomas VI y VII. En efecto, supongamos que existiera un tal subconjunto $\mathcal{P}$. Como $i \neq 0$, se tendría o bien $i \in \mathcal{P}$ o bien $-i \in \mathcal{P}$. En ambos casos
$$i^2 = (-i)^2 = -1 \in \mathcal{P}$$
y entonces
$$1 = (-1)^2 \in \mathcal{P}$$
lo que contradice el axioma VI.

La forma usual de representar gráficamente los números complejos es representar $z = x + yi$, dependiendo del contexto, como el punto de coordenadas (x,y) en el plano cartesiano o como el vector que va desde el origen hasta ese punto. En este marco, se llama al plano cartesiano el *plano complejo*, al eje x el *eje real* y al eje y el *eje imaginario*.

Definición 1.9.3 *El* ***conjugado*** *del número complejo* $z = a + bi$ *es el número complejo*
$$\overline{z} = a - bi.$$

Teorema 1.9.3 *Si* $z, w \in \mathbb{C}$, *se tiene*

(1) $\overline{z+w} = \overline{z} + \overline{w}$,

(2) $\overline{zw} = \overline{z}\,\overline{w}$,

(3) $\overline{\overline{z}} = z$,

(4) $\overline{-z} = -\overline{z}$,

(5) $\overline{z^{-1}} = (\overline{z})^{-1}$ *si* $z \neq 0$,

(6) $\mathrm{Re}\,(z) = (z + \overline{z})/2$,

(7) $\mathrm{Im}\,(z) = (z - \overline{z})/(2i)$,

(8) $z = \overline{z}$ *si, y sólo si,* $z \in \mathbb{R}$.

Definición 1.9.4 *El* ***valor absoluto*** *o* ***módulo*** *del número complejo $z = a+bi$ es el número real*

$$|z| = \sqrt{a^2 + b^2}.$$

Claramente $|z|$ es la longitud del vector que corresponde a z en el plano complejo. En general $|z-w|$ es la distancia ordinaria entre los puntos del plano que representan z y w.

Teorema 1.9.4 *Si $z, w \in \mathbb{C}$, se tiene*

(1) $|0| = 0$, $|z| > 0$ *si* $z \neq 0$,

(2) $|\overline{z}| = |-z| = |z|$,

(3) $z\overline{z} = |z|^2$,

(4) $|zw| = |z||w|$,

(5) $z^{-1} = \overline{z}/|z|^2$ *y* $|z^{-1}| = |z|^{-1}$ *si* $z \neq 0$,

(6) $|\operatorname{Re}(z)| \leq |z|$, $|\operatorname{Im}(z)| \leq |z|$.

Teorema 1.9.5 *Si $z, w \in \mathbb{C}$, entonces*

(1) $|z+w| \leq |z| + |w|$ *(desigualdad triangular),*

(2) $||z| - |w|| \leq |z-w|$.

El nombre de "desigualdad triangular" para el teorema 1.9.5(1) proviene del hecho de que establece que la longitud de un lado de un triángulo no excede la suma de las longitudes de los otros dos lados.

Teorema 1.9.6 (Desigualdad de Cauchy) *Si $a_1, \ldots, a_n$ y $b_1, \ldots, b_n$ son números complejos, entonces*

$$\left|\sum_{j=1}^{n} a_j b_j\right|^2 \leq \left(\sum_{j=1}^{n} |a_j|^2\right)\left(\sum_{j=1}^{n} |b_j|^2\right).$$

Si no todos los b_j son cero, se verifica la igualdad si, y sólo si, existe $z \in \mathbb{C}$ tal que $a_j = z\overline{b}_j$ para cada j.[7]

[7] En general, si en un conjunto X se ha definido una suma "+" asociativa y conmutativa, se define $x_1 + x_2 + \cdots + x_n$ de forma recursiva, poniendo $x_1 + x_2 + \cdots + x_n = (x_1 + x_2 + \cdots + x_{n-1}) + x_n$. Esta suma se expresa con frecuencia por $\sum_{j=1}^{n} x_j$, es decir

$$x_1 + x_2 + \cdots + x_n = \sum_{j=1}^{n} x_j.$$

El matemático francés Augustin-Louis Cauchy (1789-1857) publicó su famosa desigualdad, para el caso de números reales, en 1821, en la segunda de las nueve notas con las que concluye su libro *Cours d'Analyse de l'École Royale Polytechnique, Première Partie, Analyse Algébrique*. Posteriormente, el ruso V. Y. Bunyakovskii (1804-1889) y el alemán H. A. Schwarz (1843-1921) obtuvieron versiones para integrales (cf. tema 4, ejercicio 13).

Teorema 1.9.7 *(a) Dado $w \in \mathbb{C}$, existe $z \in \mathbb{C}$ de manera que $z^2 = (-z)^2 = w$.*

(b) Si a, b y c son números complejos con $a \neq 0$, la ecuación $az^2 + bz + c = 0$ tiene solución en $\mathbb{C}$.

Demostración. (a) Sea $w = a + bi$. Supongamos primeramente que $b > 0$. Buscamos un $z = x + yi$ que verifique $(x + yi)^2 = a + bi$, es decir

$$\begin{aligned} x^2 - y^2 &= a \\ 2xy &= b. \end{aligned}$$

Elevando estas dos expresiones al cuadrado y sumando, obtenemos

$$x^4 + y^4 - 2x^2y^2 + 4x^2y^2 = (x^2 + y^2)^2 = a^2 + b^2$$

luego

$$x^2 + y^2 = \sqrt{a^2 + b^2}$$

y puesto que $x^2 - y^2 = a$,

$$\begin{aligned} 2x^2 &= a + \sqrt{a^2 + b^2} \\ 2y^2 &= -a + \sqrt{a^2 + b^2}, \end{aligned}$$

es decir

$$z = \pm \left(\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} + \sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}\, i \right).$$

Si $b < 0$, entonces

$$z = \pm \left(\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} - \sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}\, i \right).$$

Si $b = 0$, es $w = a \in \mathbb{R}$

(1) si $w \geq 0$, entonces

$$z = \pm\sqrt{a},$$

(2) si $w < 0$, entonces, como $\sqrt{a^2} = |a| = -a$, es $x = 0$ e $y^2 = -a$, luego

$$z = \pm\sqrt{-a}\, i.$$

Los valores obtenidos para z se designan por $\pm\sqrt{w}$.

(b) Multiplicando por $4a$ y sumando y restando b^2 podemos escribir la ecuación así

$$\begin{aligned} &(2az + b)^2 + 4ac - b^2 = 0 \\ \iff &(2az + b)^2 = b^2 - 4ac \\ \iff &2az + b = \pm\sqrt{b^2 - 4ac} \\ \iff &z = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \end{aligned}$$

Ejemplos

(1) Resolución de la ecuación

$$z^2 + z + 1 = 0.$$

Aquí $w = b^2 - 4ac = -3$, con lo que

$$z = \frac{-1 \pm \sqrt{3}\, i}{2} = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}\, i.$$

(2) Resolución de la ecuación

$$z^2 - 1 + i = 0.$$

Aquí $w = b^2 - 4ac = 4(1 - i)$, con lo que

$$z = \pm \left(\sqrt{\frac{1+\sqrt{2}}{2}} - \sqrt{\frac{-1+\sqrt{2}}{2}}\, i \right).$$

El apartado (b) del teorema anterior es un caso particular de un resultado muy importante:

Teorema 1.9.8 (Teorema Fundamental del Álgebra) *Si $n \in \mathbb{N}$ y $a_0, a_1, \ldots, a_n \in \mathbb{C}, a_n \neq 0$, la ecuación*

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = 0$$

tiene una solución compleja.

1.10. Ejercicios

Los ejercicios señalados en rojo proporcionan resultados importantes que complementan la teoría.

1. Demuestra por inducción las siguientes fórmulas:

(a) $1^2 + 2^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$,

(b) $1^3 + 2^3 + \cdots + n^3 = \left[\dfrac{n(n+1)}{2}\right]^2$,

(c) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \dfrac{n(n+1)(n+2)}{3}$,

(d) $\dfrac{1}{1 \cdot 3} + \dfrac{1}{3 \cdot 5} + \dfrac{1}{5 \cdot 7} + \cdots + \dfrac{1}{(2n-1)(2n+1)} = \dfrac{n}{2n+1}$.

2. Se define recursivamente el número *factorial de n*, denotado por $n!$, para enteros $n \geq 0$ como sigue:

$$0! = 1, \qquad (n+1)! = n!(n+1).$$

Si $n \geq 1$ se tiene $n! = 1 \cdot 2 \cdot 3 \cdots n$.

Para n y k enteros con $0 \leq k \leq n$ se define el *coeficiente binomial* $\binom{n}{k}$ por

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

(a) Si n y k son enteros con $1 \leq k \leq n$ entonces

(a.1) $\displaystyle \binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$,

(a.2) $\displaystyle \binom{n}{k}$ es un entero positivo.

(b) Demuestra el **teorema binomial:** *Si a y b son números complejos y n es un entero no negativo, entonces*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

(c) Demuestra que

(c.1) $\displaystyle \sum_{k=0}^{n} \binom{n}{k} = 2^n$,

(c.2) $\displaystyle \sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$

(d) Demuestra que si a y b son números complejos y n es un entero positivo, entonces

$$a^n - b^n = (a-b) \sum_{k=1}^{n} a^{n-k} b^{k-1}.$$

3. Demuestra que si $z \in \mathbb{C}, z \neq 1$ y $n \in \mathbb{N}$ entonces

$$\sum_{j=0}^{n} z^j = \frac{z^{n+1}-1}{z-1}.$$

4. Demuestra que si n es un número natural, entonces $6^n - 5n + 4$ es divisible por 5.

5. Demuestra las siguientes afirmaciones:

(a) Si $x^n = y^n$ y n es impar, entonces $x = y$.

(b) Si $x^n = y^n$ y n es par, entonces $x = y$ o $x = -y$.

6. Razona tus respuestas:

(a) Si a es racional y b es irracional, ¿es $a+b$ necesariamente irracional? ¿Y si a y b son ambos irracionales?

(b) Si a es racional y b es irracional, ¿es ab necesariamente irracional?

(c) ¿Existe algún número a tal que a^2 es irracional, pero a^4 es racional?

(d) ¿Existen dos números irracionales tales que sean racionales tanto su suma como su producto?

7. Demuestra que si $k \geq 2$ y n son números naturales y n no es una potencia k-ésima perfecta, entonces $\sqrt[k]{n}$ es irracional.

8. El número $\sqrt{2}+\sqrt{3}+\sqrt{5}$ ¿es racional o irracional?

9. Los números reales no nulos a, b satisfacen la ecuación

$$a^2b^2(a^2b^2+4) = 2(a^6+b^6).$$

Demuestra que a y b no pueden ser ambos racionales.

10. Sean a, b, c, d números racionales y x un número irracional tal que $cx+d \neq 0$. Demuestra que $\frac{ax+b}{cx+d}$ es irracional si, y sólo si, $ad \neq bc$.

11. Sea A un conjunto no vacío de números reales. Se define $-A = \{x : -x \in A\}$. Demuestra que

$$\sup(-A) = -\operatorname{ínf} A, \qquad \operatorname{ínf}(-A) = -\sup A.$$

12. Determina el supremo y el ínfimo del siguiente conjunto:

$$A = \left\{ (-1)^{n+1} + \frac{1}{n} : n \in \mathbb{N} \right\}.$$

13. Determina el supremo y el ínfimo del siguiente conjunto:

$$A = \left\{ \frac{m}{n} : m, n \in \mathbb{N},\ m < 2n \right\}.$$

14. Encuentra el supremo y el ínfimo del conjunto

$$A = \{2^{-p} + 3^{-q} + 5^{-r} : p, q, r \in \mathbb{N}\}.$$

15. ¿Qué número es mayor $\sqrt[n]{n!}$ o $\sqrt[n+1]{(n+1)!}$, para todo $n \in \mathbb{N}$?

16. Demuestra las siguientes desigualdades:

(a) Para todo $n \in \mathbb{N}$, se tiene

$$\sqrt{n+1} - \sqrt{n} < \frac{1}{2\sqrt{n}} < \sqrt{n} - \sqrt{n-1}\,.$$

(b) Si $k \in \mathbb{N}$ y $k > 1$, entonces

$$2\sqrt{k+1} - 2 < \sum_{n=1}^{k} \frac{1}{\sqrt{n}} < 2\sqrt{k} - 1.$$

17. Sean $a_1, a_2, \ldots, a_n$ números reales que satisfacen las desigualdades $a_k \geq 0$ $(k = 1, 2, \ldots, n)$, o bien $-1 < a_k < 0$ $(k = 1, 2, \ldots, n)$. Demuestra que

$$(1 + a_1)(1 + a_2) \cdots (1 + a_n) \geq 1 + a_1 + a_2 + \cdots + a_n.$$

En el caso $a_1 = a_2 = \cdots = a_n = a$ se obtiene la *desigualdad de Bernoulli*

$$(1 + a)^n \geq 1 + na, \qquad a > -1.$$

Para los enteros $n > 1$ se tiene la igualdad si, y sólo si, $a = 0$.

18.1. Se definen la *media aritmética* y la *media geométrica* de los números reales no negativos $a_1, a_2, \ldots, a_n$ respectivamente por

$$\mathcal{A}_n(a_1, a_2, \ldots, a_n) = \frac{a_1 + a_2 + \cdots + a_n}{n}, \qquad \mathcal{G}_n(a_1, a_2, \ldots, a_n) = \sqrt[n]{a_1 a_2 \cdots a_n}\,.$$

Demuestra que $\mathcal{G}_n(a_1, a_2, \ldots, a_n) \leq \mathcal{A}_n(a_1, a_2, \ldots, a_n)$, y que se obtiene la igualdad si, y sólo si, $a_1 = a_2 = \cdots = a_n$.

18.2. Se define la *media armónica* de los números reales positivos $a_1, a_2, \ldots, a_n$ por

$$\mathcal{H}_n(a_1, a_2, \ldots, a_n) = \frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}}\,.$$

Demuestra que $\mathcal{H}_n(a_1, a_2, \ldots, a_n) \leq \mathcal{G}_n(a_1, a_2, \ldots, a_n)$, y que se obtiene la igualdad si, y sólo si, $a_1 = a_2 = \cdots = a_n$.

19. Sean $x_0 > x_1 > \cdots > x_n$ números reales. Demuestra que

$$x_0 + \frac{1}{x_0 - x_1} + \frac{1}{x_1 - x_2} + \cdots + \frac{1}{x_{n-1} - x_n} \geq x_n + 2n.$$

20. Demuestra que si $a_1, a_2, \ldots, a_n$ y $w_1, w_2, \ldots, w_n$ son números reales positivos con $\sum\limits_{j=1}^{n} w_j = 1$, entonces

$$\left(\sum_{j=1}^{n} a_j w_j \right)^2 \leq \sum_{j=1}^{n} a_j^2 w_j,$$

verificándose la igualdad si, y sólo si, $a_1 = a_2 = \cdots = a_n$.

21. Demuestra que si $a_1, a_2, \ldots, a_n$ son números reales positivos, entonces

$$\left(\sum_{j=1}^{n} a_j \right) \left(\sum_{j=1}^{n} \frac{1}{a_j} \right) \geq n^2,$$

verificándose la igualdad si, y sólo si, $a_1 = a_2 = \cdots = a_n$.

22. Demuestra que si $a_1, a_2, \ldots, a_n$ son números reales positivos tales que $a_1 + a_2 + \cdots + a_n = 1$, entonces

$$\sum_{j=1}^{n} \left(a_j + \frac{1}{a_j} \right)^2 \geq \frac{(n^2+1)^2}{n},$$

verificándose la igualdad si, y sólo si, $a_1 = a_2 = \cdots = a_n$.

23. *Lema de Schur*. Demuestra que para cada colección rectangular $\{c_{jk} : 1 \leq j \leq m, 1 \leq k \leq n\}$, y cada par de sucesiones $\{x_j : 1 \leq j \leq m\}$ y $\{y_k : 1 \leq k \leq n\}$ de números reales, se tiene

$$\left| \sum_{j=1}^{m} \sum_{k=1}^{n} c_{jk} x_j y_k \right| \leq \sqrt{RC} \left(\sum_{j=1}^{m} |x_j|^2 \right)^{\frac{1}{2}} \left(\sum_{k=1}^{n} |y_k|^2 \right)^{\frac{1}{2}},$$

donde R y C se definen por

$$R = \max_j \sum_{k=1}^{n} |c_{jk}| \quad \text{y} \quad C = \max_k \sum_{j=1}^{m} |c_{jk}|.$$

24. Sean a, b, c, d números reales positivos cuya suma es 1. Demuestra que

$$\frac{a^2}{a+b} + \frac{b^2}{b+c} + \frac{c^2}{c+d} + \frac{d^2}{d+a} \geq \frac{1}{2}$$

con igualdad si, y sólo si, $a = b = c = d = 1/4$.

25. Sean $x, y, z > 1$ y tales que $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 2$. Demuestra que

$$\sqrt{x+y+z} \geq \sqrt{x-1} + \sqrt{y-1} + \sqrt{z-1}.$$

26. Sea P un polinomio con coeficientes positivos. Demuestra que si

$$P\left(\frac{1}{x}\right) \geq \frac{1}{P(x)}$$

se verifica para $x = 1$, entonces se verifica para todo $x > 0$.

27. Sean $x, y, z \geq 0$. Demuestra que para todo $\alpha > 0$ se verifica la *desigualdad de Schur*

$$x^\alpha (x-y)(x-z) + y^\alpha (y-x)(y-z) + z^\alpha (z-x)(z-y) \geq 0.$$

La igualdad se verifica si, y sólo si, $x = y = z$ o dos de los números reales x, y, z son iguales y el tercero es cero.

28. Demuestra que si a y b son números reales no nulos tales que $a + b > 0$, entonces

$$\frac{a}{b^2} + \frac{b}{a^2} \geq \frac{1}{a} + \frac{1}{b}.$$

29. Demuestra la siguiente desigualdad:

$$X^2 + Y^2 + Z^2 \geq XY + YZ + ZX \qquad (X, Y, Z \in \mathbb{R}).$$

Demuestra que:

(a) Si $x, y, z \in \mathbb{R}$, entonces

$$x^4 + y^4 + z^4 \geq xyz(x + y + z).$$

(b) Si a, b y c son números reales positivos, entonces

$$a + b + c \leq \frac{bc}{a} + \frac{ca}{b} + \frac{ab}{c}\,.$$

30. Sean a, b y c números reales positivos. Demuestra la *desigualdad de Nesbitt*

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geq \frac{3}{2}\,.$$

31. Sean a y b números reales positivos. Demuestra que:

(a) Si $ab \leq 1$, entonces

$$\left(1 + \frac{1}{a}\right)\left(1 + \frac{1}{b}\right) \geq 4.$$

(b) Si $a + b = 1$, entonces

$$\left(1 + \frac{1}{a}\right)\left(1 + \frac{1}{b}\right) \geq 9.$$

32. Sean α y β números reales positivos y m un número entero no negativo. Demuestra que

$$\left(1 + \frac{\alpha}{\beta}\right)^m + \left(1 + \frac{\beta}{\alpha}\right)^m \geq 2^{m+1}.$$

33. Sean a, b, c y d números reales. Demuestra que los números $a - b^2, b - c^2, c - d^2$ y $d - a^2$ no pueden ser todos mayores que $\frac{1}{4}$.

34. Sea α un número real tal que $\alpha + 1/\alpha \in \mathbb{Z}$. Demuestra que

$$\alpha^n + \frac{1}{\alpha^n} \in \mathbb{Z}$$

para todo $n \in \mathbb{N}$.

35. Sean $a, b \geq 0$. Entonces

$$(n-1)a^n + b^n \geq na^{n-1}b, \;\; n \in \mathbb{N}.$$

Para los enteros $n > 1$ se verifica la igualdad si, y sólo si, $a = b$.

36. Demuestra que entre todas las cajas con un área dada, el cubo tiene el mayor volumen.

37. Demuestra que para cualquier triángulo con lados a, b, c y área A, se verifica la *desigualdad de Weitzenböck*

$$a^2 + b^2 + c^2 \geq 4\sqrt{3}A.$$

La igualdad se verifica si, y sólo si, el triángulo es equilátero.

38. Demuestra que, para $n = 1, 2, 3, \ldots,$

(a) $(n+1)^n \geq 2^n n!,$

(b) $(n+1)^n (2n+1)^n \geq 6^n (n!)^2.$

39. Para $a_k \in \mathbb{R}$, $b_k > 0$, $k = 1, 2, \ldots, n$, sean

$$m = \min\left\{\frac{a_k}{b_k} : k = 1, 2, \ldots, n\right\} \quad \text{y} \quad M = \max\left\{\frac{a_k}{b_k} : k = 1, 2, \ldots, n\right\}.$$

Demuestra que

$$m \leq \frac{a_1 + a_2 + \cdots + a_n}{b_1 + b_2 + \cdots + b_n} \leq M.$$

Como aplicación, demuestra que para cualquier polinomio $P(\xi) = c_0 + c_1\xi + c_2\xi^2 + \cdots + c_n\xi^n$ con coeficientes positivos, se tiene

$$0 < x \leq y \implies \left(\frac{x}{y}\right)^n \leq \frac{P(x)}{P(y)} \leq 1.$$

40. Describe geométricamente los siguientes subconjuntos de $\mathbb{C}$:

(a) $A = \left\{z \in \mathbb{C} : \operatorname{Re} \frac{1}{z} < \frac{1}{2}\right\},$

(b) $B = \{z \in \mathbb{C} : \operatorname{Im} z^2 > 0\},$

(c) $C = \{z \in \mathbb{C} : |z-1| = 2|z+1|\},$

(d) $D = \{z \in \mathbb{C} : |z+1| < |z-1|\},$

(e) $E = \{z \in \mathbb{C} : |1-z|^2 \leq 1 - |z|^2\}.$

41. Demuestra que si $a, b \in \mathbb{C}$, entonces

$$|a+b|^2 + |a-b|^2 = 2\big(|a|^2 + |b|^2\big).$$

Interpreta geométricamente.

42. Demuestra que si los números complejos $a_1, a_2, \ldots, a_n$ y $b_1, b_2, \ldots, b_n$ satisfacen $|a_j| \leq 1$ y $|b_j| \leq 1$ para todo $1 \leq j \leq n$ entonces

$$|a_1 a_2 \cdots a_n - b_1 b_2 \cdots b_n| \leq \sum_{j=1}^{n} |a_j - b_j|.$$

43. *Desigualdades de Abel.* Sea $z_1, z_2, \ldots, z_n$ una sucesión de números complejos con sumas parciales $S_k = z_1 + z_2 + \ldots + z_k, 1 \leq k \leq n$. Demuestra que para cada sucesión de números reales tal que $a_1 \geq a_2 \geq \cdots \geq a_n \geq 0$, se tiene

$$|a_1 z_1 + a_2 z_2 + \cdots + a_n z_n| \leq a_1 \max_{1 \leq k \leq n} |S_k|,$$

y que para cada sucesión de números reales tal que $0 \leq b_1 \leq b_2 \leq \cdots \leq b_n$, se tiene

$$|b_1 z_1 + b_2 z_2 + \cdots + b_n z_n| \leq 2b_n \max_{1 \leq k \leq n} |S_k|.$$