CAPÍTULO II

SISTEMAS DE NÚMEROS

Introducción.—Debemos extender suficientemente el concepto inicial de número, como número natural, hasta crear un instrumento capaz de satisfacer las necesidades de la práctica y de la teoría. En una larga y, a veces, titubeante evolución histórica fueron gradualmente aceptados el cero, los enteros negativos y las fracciones, en el mismo plano que los enteros positivos, y hoy día las reglas operativas con estos números son del dominio de todo estudiante de bachillerato. Pero para alcanzar completa libertad en las operaciones algebraicas debemos ir más allá, hasta incluir en el concepto de número las cantidades irracionales y complejas. Aunque estas extensiones del concepto de número natural han sido utilizadas en matemática durante varios siglos y, por otra parte, constituyen la base de toda la matemática moderna, hasta tiempos relativamente recientes no fueron establecidas sobre una base lógica sólida. En el presente capítulo haremos una exposición del modo como dicha base fué alcanzada.

I. LOS NÚMEROS RACIONALES

1. Los números racionales como resultado de mediciones.—Los números enteros son abstracciones del proceso de contar colecciones finitas de objetos. Pero en la vida diaria no es suficiente poder *contar objetos*' individuales, es preciso también *medir cantidades* tales como longitudes, áreas, pesos y tiempo. Si se quiere operar sin obstáculos con las medidas de estas cantidades, que son susceptibles de subdivisiones arbitrariamente pequeñas, es necesario extender el campo de la aritmética más allá de los números enteros. El primer paso será *el de reducir el problema de la medida al de contar*. Comenzaremos por elegir, de modo completamente arbitrario, una *unidad de medida* —metro, pie, gramo, libra, segundo, etc.—a la que asignaremos la medida 1. Luego, contaremos el número de esas unidades contenidas en la cantidad que deseamos medir; p. ej., una cierta masa de plomo pesa exactamente 54 Kg. Sin embargo, el proceso de contar no es suficiente en general, ya que la cantidad dada puede no ser exactamente medible mediante múltiplos enteros de la unidad elegida. Las más de las veces podremos decir únicamente que dicha cantidad está comprendida entre dos múltiplos consecutivos de la unidad; p. ej., entre 53 Kg y 54 Kg. Cuando esto ocurra, avanzaremos un paso introduciendo nuevas subunidades, obtenidas por subdivisión de la unidad inicial en un cierto número n de partes iguales. En el lenguaje ordinario, estas nuevas subunidades pueden tener nombres especiales; p. ej., el pie se divide en 12 pulgadas; el metro, en 100 centímetros; la libra, en 16 onzas; la hora, en 60 minutos; el minuto, en 60 segundos, etc. Sin embargo, en el simbolismo de las matemáticas, una subunidad obtenida dividiendo la unidad inicial en n partes iguales se designa con el símbolo $1/n$; y si una cantidad contiene exactamente m de estas subunidades, su medida se denota con el símbolo m/n. Este símbolo se llama *fracción* o *razón* (a veces se escribe $m : n$). El paso siguiente, verdaderamente decisivo, sólo se dió de modo consciente después de varios siglos de tentativas. El resultado fué que el símbolo m/n quedó desposeído de referencias concretas a procesos de medidas y a las cantidades medidas, y fué considerado simplemente como un *número*, un ente en sí mismo, en el mismo plano que los números naturales. Cuando m y n son números naturales, el símbolo m/n se llama *número racional.*

El uso de la palabra número (inicialmente reservada para los números naturales) para estos nuevos símbolos está justificado por el hecho de que la adición y la multiplicación de estos entes obedecen a las mismas leyes que rigen dichas operaciones con los números naturales. Para probar esto, debemos definir previamente la adición, la multiplicación y la igualdad de números racionales. Como es bien sabido, estas definiciones son:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},\qquad \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd} \tag{1}$$

$$\frac{a}{a}=1,\qquad \frac{a}{b}=\frac{c}{d}\ \text{si}\ ad=bc,$$

para enteros cualesquiera a, b, c, d; p. ej.:

$$\frac{2}{3}+\frac{4}{5}=\frac{2\cdot 5+3\cdot 4}{3\cdot 5}=\frac{10+12}{15}=\frac{22}{15},\qquad \frac{2}{3}\cdot\frac{4}{5}=\frac{2\cdot 4}{3\cdot 5}=\frac{8}{15}.$$

$$\frac{3}{3}=1,\qquad \frac{8}{12}=\frac{6}{9}=\frac{2}{3}$$

Estas definiciones se nos presentan forzosamente si deseamos que los números racionales sean apropiados para medir longitudes, áreas, etc. Pero hablando en sentido estricto, estas reglas de adición, multiplicación e igualdad de nuestros símbolos quedan establecidas por su propia definición y no aparecen impuestas por otras necesidades que las de ser no contradictorias y resultar útiles para las aplicaciones. A partir de las definiciones [1] se puede probar que *las leyes fundamentales de la aritmética de los números naturales continúan siendo válidas en el dominio de los números racionales*:

$$\begin{array}{rll} p + q &= q + p & \text{(ley conmutativa de la adición),} \\ p + (q + r) &= (p + q) + r & \text{(ley asociativa de la adición),} \\ pq &= qp & \text{(ley conmutativa de la multiplicación),} \\ p(qr) &= (pq)r & \text{(ley asociativa de la multiplicación),} \\ p(q + r) &= pq + pr & \text{(ley distributiva).} \end{array} \qquad [2]$$

P. ej., la prueba de la ley conmutativa de la adición de fracciones resulta de las ecuaciones

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{cb + da}{db} = \frac{c}{d} + \frac{a}{b},$$

en las cuales el primero y el último signo de igualdad corresponden a la definición [1] de la adición, mientras que el del centro es una consecuencia de las leyes conmutativas de la adición y de la multiplicación de números naturales. El lector puede comprobar las otras cuatro leyes de manera análoga.

Para la efectiva comprensión de estos hechos se debe insistir una vez más en que los números racionales son creación nuestra, y que las reglas [1] dependen de nuestra voluntad. Podríamos haber definido caprichosamente la adición por la fórmula $\frac{a}{b} + \frac{c}{d} = \frac{a + c}{b + d}$, la cual habría dado en particular $1/2 + 1/2 = 2/4$, lo que sería absurdo aplicado a la medición de cantidades. Reglas de tal tipo, aunque permisibles lógicamente, harían de la aritmética de nuestros nuevos símbolos un juego carente de sentido. El juego libre del intelecto debe estar guiado aquí por la necesidad de crear un instrumento capaz de ser utilizado para la medida.

2. Necesidad intrínseca de la introducción de los números racionales. Principio de generalización.—Junto a las razones *prácticas* que indujeron a la introducción de los números racionales, existen otras de carácter intrínseco y en cierto modo más apremiantes, que vamos a discutir independientemente de los argumentos anteriores. Estas razones son de carácter aritmético y típicas de una tendencia dominante en el proceso matemático.

En la aritmética ordinaria de los números naturales se pueden efectuar siempre las dos operaciones fundamentales: adición y multiplicación. En cambio, las *operaciones inversas* no son siempre posibles. La diferencia $b - a$ de dos enteros a, b es el entero c tal que $a + c = b$; es decir, es la solución de la ecuación $a + x = b$. Pero en el dominio de los números naturales el símbolo $b - a$ posee significación únicamente cuando es $b > a$, ya que únicamente entonces tiene la ecuación $a + x = b$ una solución que sea un número natural. Un gran paso para suprimir esta restricción se dió cuando se introdujo el símbolo 0 mediante la relación $a - a = 0$. De mayor importancia aún fué la introducción de los símbolos -1, -2, -3, ..., junto con la definición

$$b - a = -(a - b)$$

para el caso $b < a$, que permitió la sustracción, sin restricciones, *en el dominio de los enteros positivos y negativos*. Para incluir los nuevos símbolos -1, -2, -3, ..., en una aritmética más amplia, que comprenda tanto los enteros positivos como los negativos, debemos, naturalmente, *definir las operaciones* con ellos de tal manera que *las reglas de las operaciones aritméticas con los números naturales se conserven para el nuevo dominio*; p. ej., la regla

$$(-1)(-1) = 1, \tag{3}$$

que servirá para regir la multiplicación de los enteros negativos, es una consecuencia del deseo de conservar la ley distributiva $a(b + c) = ab + ac$. Puesto que si hubiéramos convenido, p. ej., en que fuera $(-1)\ (-1) = -1$, poniendo $a = -1$, $b = 1$, $c = -1$ resultaría $-1\ (1 - 1) = -1 - 1 = -2$, mientras que por otro lado se tendría $-1(1 - 1) = -1 \cdot 0 = 0$. Fué necesario mucho tiempo para que los matemáticos comprendieran que la «regla de los signos» [3], junto con todas las demás definiciones que se refieren a los enteros negativos y a las fracciones, no podían ser «demostradas». Todas eran *creaciones* hechas con objeto de alcanzar libertad en las operaciones, conservando siempre las leyes fundamentales de la aritmética. Lo que *puede*—y debe—probarse es únicamente el hecho de que con tales definiciones las leyes conmutativa, asociativa y distributiva de la aritmética se conservan. Aun el gran matemático Euler dió un argumento poco convincente para mostrar que $(-1)\ (-1)$ «debe» ser igual a $+1$. Decía: dicho producto debe ser $+1$ ó -1, pero no puede ser -1, puesto que $-1 = (+1)\ (-1)$.

Del mismo modo que la introducción de los enteros negativos y del cero despejó el camino para la sustracción sin restricciones, la introducción de los números fraccionarios suprime análogos obstáculos para la división. El cociente $x = b/a$ de dos enteros a y b, definido por la ecuación

$$ax = b, \tag{4}$$

existe, *como entero,* únicamente cuando a es un divisor de b. Si no es ése el caso, como, p. ej., si es $a = 2$, $b = 3$, introducimos simplemente el símbolo b/a, al que llamamos fracción, para el que establecemos la regla $a(b/a), = a$, de modo que b/a es, «por definición», una solución de [4]. La introducción de las fracciones como nuevos números hace posible la división sin restricciones, *excepto la división por cero,* la cual será *excluída en todos los casos.*

Expresiones del tipo $1/0$, $3/0$, $0/0$, etc., serán siempre símbolos sin significado para nosotros, puesto que si se admitiera la división por cero, podríamos deducir de ecuaciones correctas, como $0 \cdot 1 = 0 \cdot 2$, la consecuencia absurda $1 = 2$. Sin embargo, a veces puede ser útil designar expresiones del tipo $3/0$ por el símbolo ∞ (léase «infinito»), *siempre que no se pretenda operar con el símbolo ∞ como si estuviera sujeto a las leyes ordinarias del cálculo numérico.*

La significación aritmética propia del sistema de *todos los números racionales*—enteros y fraccionarios, negativos y positivos—resulta ahora clara. Para el dominio de los números así extendido no sólo valen las leyes formales asociativa, conmutativa y distributiva, sino que ahora también las ecuaciones $a + x = b$ y $ax = b$ tienen las soluciones $x = b - a$ y $x = b/a$, sin restricción alguna, con tal que para la última se tenga $a \neq 0$. En otros términos, en el dominio de los números racionales las llamadas *operaciones racionales*—adición, sustracción, multiplicación y división—son posibles sin restricción y los resultados pertenecen siempre a aquel dominio de números. Un dominio de números *cerrado* respecto de dichas operaciones se llama un *cuerpo.* Daremos otros ejemplos de cuerpos más adelante, en este capítulo y en el siguiente.

Extender un dominio por la introducción de nuevos símbolos, de tal modo que las leyes que valen en el primero continúen rigiendo en el segundo, es uno de los aspectos del proceso de *generalización* característico de la matemática. La generalización del concepto de número natural al de número racional satisface, por una parte, la necesidad teórica de suprimir las restricciones a la sustracción y a la división, y cumple, por otra, la necesidad práctica de tener números para representar los resultados de mediciones. Del hecho de que los números racionales satisfagan esa doble necesidad resulta verdaderamente su gran importancia. Como hemos visto, esta extensión del concepto de número ha sido posible por la creación de nuevos números en la forma de símbolos abstractos tales como 0, -2, y $^3/_4$. Hoy, acostumbrados como estamos a tratarlos como cosa corriente, resulta difícil creer que hasta el siglo XVII no fueron admitidos con los mismos derechos que los enteros positivos y que, aunque usados cuando se hacían necesarios, no era sin ciertas dudas y prevenciones. A la natural tendencia humana a apoyarse en lo *concreto*, y como tales aparecían los números naturales, se debe la lentitud con que se dió este paso inevitable. Únicamente en el dominio de lo abstracto puede ser creado un sistema satisfactorio de aritmética.

3. Interpretación geométrica de los números racionales.—La construcción que sigue dará una interpretación geométrica intuitiva del sistema de los números racionales.

Tomemos sobre una recta, «recta numérica», un segmento de 0 a 1 (Fig. 8). Elijamos dicho segmento como unidad de longitudes, unidad que puede ser tomada arbitrariamente. Los enteros positivos y negativos serán representados por puntos equidistantes sobre la recta numérica, los positivos a la derecha del 0 y los negativos a la izquierda.

FIG. 8.—La recta numérica.

Para representar las fracciones de denominador n, dividimos cada uno de los segmentos de longitud unidad en n partes iguales; los puntos de subdivisión representan las fracciones con denominador n. Si efectuamos esa construcción para todo entero n, todos los números racionales vendrán representados por puntos de la recta numérica. Llamaremos a los puntos así obtenidos *puntos racionales*, y usaremos las expresiones «número racional» y «punto racional» como equivalentes.

En el capítulo primero, I, se definió la relación $A < B$ para números naturales. Esta relación tiene una interpretación en la recta numérica, que resulta del hecho de que si un número natural A es menor que otro B, el punto A está a la izquierda del punto B. Esta relación geométrica tiene significado para *todos* los puntos racionales, por lo que parece natural intentar extender la relación aritmética a los números racionales, de modo que corresponda al orden geométrico de los puntos racionales. Se llega a ese resultado con la definición siguiente: Diremos que el número racional A es *menor que* el número racional B ($A < B$), y B se dice *mayor que* A ($B > A$) cuando $B - A$ es positivo. De la definición se sigue que, si es $A < B$, los puntos (números) *entre* A y B son aquellos que satisfacen simultáneamente las condiciones de ser $> A$ y $< B$. Todo par de puntos distintos, junto con los puntos comprendidos entre ellos, forman el *segmento* o *intervalo* $[A, B]$.

La distancia de un punto A al origen, considerada como positiva, se llama *valor absoluto* de A y se indica con el símbolo

$$|A|$$

Es decir; si es $A \geqslant 0$, se tiene $|A| = A$; y si es $A \leqslant 0$, se tiene $|A| = -A$. Es fácil ver que si A y B tienen el mismo signo, vale la igualdad $|A + B| = |A| + |B|$; mientras que si A y B tienen signos distintos, es $|A + B| < |A| + |B|$. Por tanto, combinando estos dos resultados, se tendrá en todo caso

$$|A + B| \leqslant |A| + |B|,$$

cualesquiera que sean los signos de A y B.

Para la representación que consideramos se tiene la siguiente proposición de fundamental importancia: *Los puntos racionales forman un conjunto denso en la recta.* Con esto se quiere decir que interiores a todo intervalo, por pequeño que sea, hay siempre puntos racionales. Basta tomar el denominador n suficientemente grande, de modo que el intervalo $[0,1/n]$ sea más pequeño que el intervalo $[A, B]$ en cuestión, para que al menos una de las fracciones m/n sea interior a él. No existen, por tanto, intervalos, por pequeños que sean, vacíos de puntos racionales. Resulta también que en todo intervalo debe haber infinitos puntos racionales; puesto que si hubiera solamente un número finito de ellos, el intervalo determinado por dos consecutivos no podría contener puntos racionales, en oposición a lo que acabamos de probar.

II. SEGMENTOS INCONMENSURABLES, NÚMEROS IRRACIONALES Y CONCEPTO DE LÍMITE

1. Introducción.—Cuando se comparan las longitudes de dos segmentos rectilíneos a y b, puede ocurrir que a esté contenido un número r exacto de veces en b. En este caso podemos expresar la medida del segmento b tomando como unidad a y diciendo que la longitud de b es r veces la de a. Pero puede ocurrir que, mientras que ningún múltiplo entero de a sea igual a b, se pueda dividir a en un cierto número de partes iguales, p. ej., n, cada una de longitud a/n y tales que un múltiplo entero m del segmento a/n sea igual a b:

$$b = \frac{m}{n} a. \qquad [1]$$

Cuando se tiene una igualdad de la forma [1] diremos que los dos segmentos a y b son *conmensurables*, dado que tienen una medida común: el segmento a/n está contenido n veces en a y m veces en b. El conjunto de todos los segmentos conmensurables con a estará constituído por aquellos segmentos cuya longitud puede ser expresada en la forma [1], para enteros m y n convenientes ($n \neq 0$). Si tomamos a como segmento unidad [0,1], en la figura 9, los segmentos conmensu-

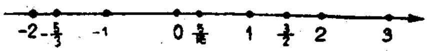


FIG. 9.—Los puntos racionales.

rables con el segmento unidad corresponderán a todos los puntos racionales m/n sobre la recta numérica. Para todas las cuestiones prácticas relacionadas con la medida, los números racionales son suficientes. Incluso desde un punto de vista teórico, como los puntos racionales cubren la recta densamente, podría pensarse que todos los puntos de la recta fueran racionales. Si esta sospecha fuese cierta, todos los segmentos serían conmensurables con la unidad. Uno de los descubrimientos más sorprendentes de los primeros matemáticos griegos (la escuela pitagórica) fué el de que las cosas no sucedían de modo tan simple. Existen *segmentos inconmensurables* y, si suponemos que a todo segmento corresponde un número, como medida de su longitud con un segmento unidad, existen también *números irracionales*. Este descubrimiento fué un acontecimiento científico de la máxima importancia. Posiblemente señala el origen de lo que puede considerarse como contribución específica de los griegos a los procesos rigurosos de las matemáticas. Es evidente que este hecho afectó profundamente la matemática y la filosofía desde la época griega hasta nuestros días.

La teoría de los inconmensurables de Eudoxio, presentada en forma geométrica en los *Elementos* de Euclides, es una obra maestra de la matemática griega, frecuentemente omitida en las desfiguradas versiones didácticas de los *Elementos*. Dicha teoría no fué apreciada en su justo valor hasta el siglo pasado, después que Dedekind, Cantor y Weierstrass construyeron una teoría rigurosa de los números irracionales. Expondremos aquí la teoría de los inconmensurables en la forma aritmética moderna.

Antes de nada probaremos que *la diagonal del cuadrado es inconmensurable con su lado*. Supongamos que se ha tomado como unidad de longitud el lado del cuadrado y que la diagonal tiene una longitud x. Entonces, por el teorema de Pitágoras, se tendrá

$$x^2 = 1^2 + 1^2 = 2.$$

(Designamos x con el símbolo $\sqrt{2}$.) Si x fuese conmensurable con 1, existirían dos enteros p y q tales que $x = p/q$, y

$$p^2 = 2q^2. \qquad [2]$$

Supongamos p/q irreducible, ya que puede suprimirse todo factor común al numerador y denominador. Puesto que 2 aparece como factor en el segundo miembro, p^2 tiene que ser un número par, de donde resulta que p debe ser par, pues el cuadrado de todo número impar es impar. Podemos, por tanto, escribir $p = 2r$. Al sustituir este valor en [2] se tiene

$$4r^2 = 2q^2, \quad \text{o lo que es lo mismo,} \quad 2r^2 = q^2.$$

Por ser 2 un factor del primer miembro de la última igualdad, q^2 es par y, en consecuencia, también lo es q. Resultan así p y q divisibles por 2, lo que contradice la hipótesis de que p y q no tenían factores comunes; en consecuencia, no se puede tener la igualdad [2]; es decir, x no puede ser un número racional.

Nuestro resultado puede ser expresado por la proposición: no existe ningún número racional igual a $\sqrt{2}$.

Del argumento precedente resulta que, mediante una construcción geométrica muy sencilla, se puede obtener un segmento inconmensurable con el segmento unidad. Si con un compás llevamos dicho segmento sobre la recta numérica, en la forma indicada en la figura 10, el punto obtenido no puede coincidir con ninguno de los puntos racionales: *El sistema de los números racionales*, aunque denso en toda ella, *no cubre toda la recta numérica*. A una mente ingenua debe resultarle ciertamente extraño y paradójico que el conjunto denso de los puntos racionales no llena la recta completa. Nada en nuestra «intuición» puede ayudarnos a «ver» los puntos irracionales como distintos de los racionales. No es de extrañar que el descubrimiento de los inconmensurables produjera gran impresión en los filósofos y matemáticos griegos, y que aún hoy le ofrezca, a quien medite sobre la cuestión, cierta perplejidad.

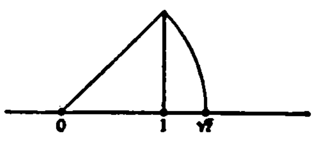


FIG. 10.—Construcción de $\sqrt{2}$.

Es fácil construir tantos segmentos inconmensurables con la unidad como se desee. Los extremos de tales segmentos llevados a partir del 0 de la recta numérica son los llamados *puntos irracionales*. Ahora bien: el principio que sirvió para introducir las fracciones fué el de *medir las longitudes con números*, y deseamos en lo que sigue conservar este principio y tratar de acuerdo con él los segmentos inconmensurables con la unidad. Si queremos que exista una *correspondencia mutua entre números*, de una parte, *y puntos de la recta*, de otra, es preciso introducir los *números irracionales*.

Resumiendo en lo posible la situación, se puede decir que un número irracional representa la longitud de un segmento inconmensurable con la unidad. En las secciones que siguen precisaremos esta definición un poco vaga y completamente geométrica, hasta llegar a otra más satisfactoria desde el punto de vista del rigor lógico. Nuestras primeras consideraciones a este propósito partirán de las propiedades de las fracciones decimales.

Ejercicios:

1. Demuéstrese que $\sqrt[3]{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt[3]{3}$ no son racionales. (*Indicación:* Utilícese el lema de la página 54.)
2. Pruébese que $\sqrt{2}+\sqrt{3}$ y $\sqrt{2}+\sqrt[3]{2}$ no son racionales. (*Indicación:* Si, p. ej., el primero de estos números fuera igual a un número racional r, poniendo $\sqrt{3}=r-\sqrt{2}$ y elevando al cuadrado, $\sqrt{2}$ resultaría racional.)
3. Demuéstrese que $\sqrt{2}+\sqrt{3}+\sqrt{5}$ es irracional. Inténtese construir ejemplos análogos y más generales.

2. Fracciones decimales. Decimales de infinitas cifras.—Para cubrir la recta numérica con un conjunto de puntos denso en toda ella no son necesarios *todos* los números racionales; bastan, por ejemplo, los números obtenidos por subdivisión de cada intervalo unidad en 10, luego en 100, 1000, etc., segmentos iguales. Los puntos así obtenidos corresponden a las «fracciones decimales»; p. ej., el punto $0{,}12=1/10+$ $+2/100$ corresponde al punto situado en el primer intervalo unidad, en el segundo subintervalo de longitud 10^{-1}, y en el origen del tercer «sub-sub-» intervalo de longitud 10^{-2}. (a^{-n} significa $1/a^n$.) Si una *fracción decimal* contiene n cifras después de la coma, tiene la forma

$$f = z + a_1 10^{-1} + a_2 10^{-2} + a_3 10^{-3} + \ldots + a_n 10^{-n},$$

donde z es un entero y las a son cifras—0, 1, 2, ..., 9—que indican las décimas, centésimas, y así sucesivamente. El número f se representa en el sistema decimal en la forma abreviada $z{,}a_1a_2a_3\ldots a_n$. Se ve inmediatamente que estas fracciones pueden escribirse en forma de fracción p/q, siendo $q=10^n$; p. ej., $f=1{,}314=1+3/10+1/100+$ $+4/1000=1314/1000$. Si p y q tienen un divisor común, la fracción podrá reducirse a otra cuyo denominador será divisor de 10^n. Por otra parte, ninguna fracción irreducible cuyo denominador no sea divisor de alguna potencia de 10 puede venir representada por una fracción decimal; p. ej., $1/5=2/10=0{,}2$ y $1/250=4/1000=0{,}004$; en cambio, $1/3$ no puede ser escrita como número decimal de n cifras, por grande que sea n, ya que una igualdad de la forma

$$1/3 = b/10^n$$

conduciría a

$$10^n = 3b,$$

lo que es absurdo, ya que 3 no es factor de ninguna potencia de 10.

Tomemos sobre la recta numérica un punto P que no corresponda a ninguna fracción decimal; p. ej., el punto racional 1/3 o el punto irracional $\sqrt{2}$. Entonces, por el proceso de subdivisión del intervalo unidad en diez partes iguales, y luego en cien y así sucesivamente, el punto P no será nunca origen de ninguno de los subintervalos parciales. Sin embargo, P puede ser incluído dentro de intervalos cada vez más pequeños de la subdivisión decimal, con el grado de aproximación que se desee. Este proceso de aproximación puede ser descrito en la forma siguiente: supongamos que P está en el primer intervalo unidad; subdividiendo este intervalo en 10 partes iguales, cada una de longitud 10^{-1}, supongamos que P está en el tercero de tales intervalos. Diremos entonces que P está entre las fracciones decimales 0,2 y 0,3. Subdividimos entonces el intervalo de 0,2 a 0,3 en 10 partes iguales, cada una de longitud 10^{-2}, y supongamos que P está en el cuarto de tales intervalos. Subdividamos éste a su vez y supóngase que P está en el primero de estos intervalos de longitud 10^{-3}. Podremos decir entonces que P está entre 0,230 y 0,231. Este proceso puede continuarse indefinidamente, dando lugar a una sucesión ilimitada de cifras, $a_1, a_2, a_3, \ldots, a_n, \ldots$, con la propiedad siguiente: para todo valor del entero n, el punto P está incluído en el intervalo I_n, cuyo origen es la fracción decimal $0{,}a_1a_2a_3 \ldots a_{n-1}a_n$ y cuyo extremo es $0{,}a_1a_2a_3 \ldots a_{n-1}(a_n + 1)$, siendo 10^{-n} la longitud de I_n. Si elegimos la sucesión $n = 1, 2, 3, 4, \ldots$, vemos que cada uno de los intervalos $I_1, I_2, I_3, \ldots$, está contenido en el precedente, mientras que sus longitudes 10^{-1}, 10^{-2}, 10^{-3}, ..., tienden a cero. Diremos que P está contenido en una sucesión de *intervalos decimales encajados;* p. ej., si P es el punto racional 1/3, todas las cifras $a_1, a_2, a_3, \ldots$ son iguales a 3, y P está contenido en todo intervalo I_n cuyos extremos sean 0,333...33 y 0,333...34; es decir, 1/3 es mayor que 0,333...33 y menor que 0,333...34, donde el número de cifras puede ser arbitrariamente grande. Expresaremos este hecho diciendo que el número decimal de n cifras 0,333 ... 33 «tiende hacia 1/3» al crecer n, y escribiremos

$$1/3 = 0{,}333\ldots;$$

los puntos indican que la fracción decimal debe extenderse «indefinidamente».

El punto irracional $\sqrt{2}$ antes definido conduce también a una fracción decimal que se extiende indefinidamente; sin embargo, en este caso, la ley que determina los valores de las cifras de la sucesión no es sencilla. En efecto, no se conoce ninguna fórmula explícita que determine las cifras de la sucesión, aunque se pueden calcular tantas como se desee:

$$1^2 = 1 < 2 < 2^2 = 4$$
$$(1{,}4)^2 = 1{,}96 < 2 < (1{,}5)^2 = 2{,}25$$
$$(1{,}41)^2 = 1{,}9881 < 2 < (1{,}42)^2 = 2{,}0264$$
$$(1{,}414)^2 = 1{,}999396 < 2 < (1{,}415)^2 = 2{,}002225$$
$$(1{,}4142)^2 = 1{,}99996164 < 2 < (1{,}4143)^2 = 2{,}00024449, \text{ etc.}$$

Como definición general diremos que un punto P que no esté representado por una fracción decimal con un número finito n de cifras, está representado por la *fracción decimal infinita*, $z{,}a_1a_2a_3 \ldots$, si para cualquier valor de n el punto P está situado en el intervalo de longitud 10^{-n} con origen en el punto $z{,}a_1a_2a_3 \ldots a_n$.

De este modo se establece una correspondencia entre los puntos de la recta numérica y todas las fracciones decimales *finitas* e *infinitas*. Esto sugiere la siguiente definición: un «número» es una fracción decimal *finita* o *infinita*. Los decimales infinitos que no representan números racionales serán llamados *números irracionales*.

Hasta mediados del siglo pasado, las consideraciones precedentes eran aceptadas como una exposición satisfactoria del sistema de los números racionales e irracionales, sistema designado con el nombre de *continuo numérico*. El avance enorme de las matemáticas a partir del siglo XVII, en particular el desarrollo de la geometría analítica y del cálculo diferencial e integral, se hace sin riesgo con este concepto de sistema numérico como base. Pero durante el período de examen crítico de los principios y de consolidación de los resultados, fué abriéndose paso la idea de que el concepto de número irracional requería un análisis más preciso. Como preliminar a nuestra exposición de la teoría moderna del continuo numérico, discutiremos en forma más o menos intuitiva el concepto básico de *límite*.

Ejercicio: Calcúlese $\sqrt[3]{2}$ y $\sqrt[3]{5}$ con una aproximación de 10^{-2}.

3. Límites. Progresiones geométricas indefinidas.—Como vimos en la sección precedente, ocurre a veces que un cierto número racional s viene aproximado por una sucesión de otros números racionales s_n, en la cual el índice n toma sucesivamente los valores 1, 2, 3, ... ; p. ej., si es $s = 1/3$, la sucesión de números racionales $s_1 = 0{,}3$, $s_2 = 0{,}33$, $s_3 = 0{,}333$, etc., tiende hacia s. Para tener otro ejemplo, dividamos el intervalo unidad en dos mitades, la segunda mitad en otras dos partes iguales, y así sucesivamente, hasta que los dos menores intervalos obtenidos sean de longitud 2^{-n}, donde n es arbitrariamente grande; es decir, $n = 100$, $n = 100\,000$, o el número que queramos. Sumando entonces todos los intervalos, excepto el último, obtenemos una longitud total igual a

$$s_n = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \cdots + \frac{1}{2^n} \qquad [3]$$

Vemos que s_n difiere de 1 en $(^1/_2)^n$, y que esta diferencia llega a ser arbitrariamente pequeña, o «tiende a cero» cuando n crece indefinidamente. Carece de sentido decir que la diferencia *es* cero cuando n *es* infinito. El infinito aparece únicamente en el *proceso* y no como una *cantidad* efectiva. Podemos describir el comportamiento de s_n diciendo que *la suma* s_n *se aproxima a 1 cuando* n *tiende a infinito*, y escribir

$$1 = \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} + \cdots, \qquad [4]$$

donde en el segundo miembro se tiene una *serie indefinida* o *infinita*. Esta «ecuación» no significa que debamos sumar efectivamente infinitos sumandos; es sólo una expresión abreviada para el hecho de que 1 es el límite de la suma finita s_n cuando n *tiende a* infinito (no que *es* infinito). Así, la ecuación [4], con su símbolo incompleto «$+ \ldots$», es sólo una manera breve de escribir la proposición precisa:

1 = al límite, cuando n tiende hacia infinito, de la cantidad

$$s_n = \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots + \frac{1}{2^n} \qquad [5]$$

En forma más abreviada, pero más expresiva, se puede escribir

$$s_n \to 1 \quad \text{cuando} \quad n \to \infty\,. \qquad [6]$$

Como otro ejemplo de límite, consideremos las potencias de un número q. Si es $-1 < q < 1$; p. ej., $q = 1/3$ ó $q = -4/5$, la sucesión de potencias de q,

$$q,\ q^2,\ q^3,\ q^4, \ldots,\ q^n, \ldots,$$

se aproxima a cero cuando n crece. Si q es negativo, el signo de q^n será alternativamente $+$ ó $-$, y q^n tenderá a cero aproximándose a este valor a derecha e izquierda, alternativamente. Para $q = 1/3$ se tiene $q^2 = 1/9$, $q^3 = 1/27$, $q^4 = 1/81$, ..., mientras que si es $q = -1/2$, se tendrá $q^2 = 1/4$, $q^3 = -1/8$, $q^4 = 1/16$, ... Diremos que el *límite de* q^n, *cuando* n *tiende a infinito, es cero*, o, en símbolos

$$q^n \to 0 \quad \text{cuando} \quad n \to \infty, \quad \text{para} \quad -1 < q < 1. \qquad [7]$$

(Incidentalmente, si $q > 1$ ó $q < -1$, q^n no tiende hacia cero, sino que su valor absoluto crece sin límite.)

Para dar una demostración rigurosa de la proposición contenida en [7] partimos de la desigualdad probada en la página 22, la cual decía que $(1 + p)^n \geqslant 1 + np$ para todo entero positivo n y $p > -1$. Si q es un número fijo entre 0 y 1, p. ej., $q = 9/10$, se tiene $q = 1/(1+p)$, siendo $p > 0$. De ahí resulta

$$\frac{1}{q^n} = (1 + p)^n > 1 + np > np,$$

o (véase la regla 4, Cap. VI, suplemento I, 1)

$$0 < q^n < \frac{1}{p} \cdot \frac{1}{n}$$

Por consiguiente, q^n está comprendido entre el valor fijo 0 y $(1/p) \cdot (1/n)$, que se aproxima a cero al crecer n, puesto que p es fijo. De aquí resulta evidentemente que $q^n \to 0$. Si q es negativo, se tiene $q = -1/(1 + p)$ y, en vez de las cotas anteriores 0 y $(1/p)\,(1/n)$ aparecen ahora, respectivamente, $(-1/p)\,(1/n)$ y $(1/p)\,(1/n)$. Por lo demás, el razonamiento es el mismo.

Consideremos ahora la *progresión geométrica*

$$s_n = 1 + q + q^2 + q^3 + \cdots + q^n. \qquad [8]$$

(El caso $q = 1/2$ fué discutido antes.) Como vimos en la página 20, se puede expresar s_n en una forma concisa y simple. Multiplicando s_n por q, encontramos

$$qs_n = q + q^2 + q^3 + q^4 + \cdots + q^{n+1}, \qquad [8a]$$

y restando [8 a] de [8], vemos que desaparecen todos los términos excepto el 1 y el q^{n+1}, obteniendo

$$(1 - q)s_n = 1 - q^{n+1},$$

o, por división,

$$s_n = \frac{1 - q^{n+1}}{1 - q} = \frac{1}{1 - q} - \frac{q^{n+1}}{1 - q}$$

El concepto de límite interviene al hacer crecer n. Como hemos visto, $q^{n+1} = q \cdot q^n$ tiende a cero si es $-1 < q < 1$, y por paso al límite se obtiene

$$s_n \to \frac{1}{1-q} \text{ cuando } n \to \infty, \text{ para } -1 < q < 1. \qquad [9]$$

Escrito como ***progresión geométrica indefinida (serie)*** resulta

$$1 + q + q^2 + q^3 + \ldots = \frac{1}{1-q}, \text{ para } -1 < q < 1. \qquad [10]$$

Por ejemplo,

$$1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \ldots = \frac{1}{1 - 1/2} = 2,$$

de acuerdo con la ecuación [4], y análogamente

$$\frac{9}{10} + \frac{9}{10^2} + \frac{9}{10^3} + \frac{9}{10^4} + \ldots = \frac{9}{10}\frac{1}{1 - 1/10} = 1,$$

de forma que 0,99999 ... = 1. Del mismo modo se tiene que el número decimal finito 0,2374 y el decimal infinito 0,237399999 ... representan el mismo número.

En el capítulo VI daremos un resumen de una exposición general del concepto de límite dentro del moderno espíritu rigorista.

Ejercicios:

1. Pruébese que $1 - q + q^2 - q^3 + q^4 - \ldots = \dfrac{1}{1+q}$, si es $|q| < 1$.

2. ¿Cuál es el límite de la sucesión $a_1, a_2, a_3, \ldots$, donde es $a_n = n/(n+1)$? (*Indicación:* Escríbase el término a_n en la forma $n/(n+1) = 1 - 1/(n+1)$ y obsérvese que el último término del segundo miembro tiende a cero.)

3. ¿Cuál es el límite de $\dfrac{n^2+n+1}{n^2-n+1}$ para $n \to \infty$? (*Indicación:* Póngase la expresión en la forma

$$\frac{1 + \frac{1}{n} + \frac{1}{n^2}}{1 - \frac{1}{n} + \frac{1}{n^2}})$$

4. Pruébese, para $|q| < 1$, que $1 + 2q + 3q^2 + 4q^3 + \ldots = \dfrac{1}{(1-q)^2}$. (*Indicación:* Utilícese el resultado del ejercicio 3 de la página 25.)

5. ¿Cuál es el límite de la serie indefinida

$$1 - 2q + 3q^2 - 4q^3 + \ldots ?$$

6. ¿Cuál es el límite de $\frac{1+2+3+\ldots+n}{n^2}$, de $\frac{1^2+2^2+\ldots+n^2}{n^3}$ y de $\frac{1^3+2^3+\ldots+n^3}{n^4}$? (*Indicación:* Utilícense los resultados de las páginas 19, 21 y 22.)

4. Números racionales y decimales periódicos.—Aquellos números racionales p/q que no son fracciones decimales finitas pueden ser desarrollados en fracciones decimales indefinidas mediante el proceso de división decimal. En cada paso de este proceso debe haber un resto distinto de cero, ya que de otro modo la fracción decimal sería finita. Todos los restos distintos que aparecen en la división son enteros comprendidos entre 1 y $q-1$, de modo que hay solamente $q-1$ posibilidades para los valores de dichos restos. Esto significa que al cabo de q cifras decimales, a lo sumo, algún resto k deberá repetirse. Pero todos los restos siguientes se repetirán en el mismo orden en que aparecían después de este primer resto k. Esto prueba que la *expresión decimal de cualquier número racional es periódica;* una vez aparecido un cierto conjunto finito de cifras, dicho conjunto se repetirá infinitas veces; p. ej., $1/6 = 0{,}166666666\ldots$; $1/7 = 0{,}142857142857142857\ldots$; $1/11 = 0{,}0909090909\ldots$; $122/1100 = 0{,}1109090909\ldots$; $11/90 = 0{,}12222222\ldots$; etc. (Cabe considerar que los números racionales que pueden ser representados mediante fracciones decimales finitas tienen un desarrollo decimal periódico en el cual la cifra 0 se repite indefinidamente después de un número finito de cifras.) En algunos ejemplos anteriores se ve incidentalmente que ciertos desarrollos tienen una parte no periódica, que precede al período que se repite.

Recíprocamente, se puede probar que *todos los decimales periódicos son números racionales.* Como ejemplo, consideremos el decimal periódico indefinido

$$p = 0{,}3322222\ldots.$$

Se tiene $p = 33/100 + 10^{-3}\cdot 2(1 + 10^{-1} + 10^{-2} + \ldots)$, donde la expresión entre paréntesis es la serie geométrica

$$1 + 10^{-1} + 10^{-2} + 10^{-3} + \ldots = \frac{1}{1-1/10} = \frac{10}{9}$$

Por tanto,

$$p = \frac{33}{100} + 2\cdot 10^{-3}\cdot\frac{10}{9} = \frac{2970+20}{9\cdot 10^3} = \frac{2990}{9000} = \frac{299}{900}$$

La demostración en el caso general es esencialmente la misma, pero requiere una notación más general. En el decimal periódico general

$$p = 0{,}a_1a_2a_3\ldots a_mb_1b_2\ldots b_nb_1b_2\ldots b_nb_1b_2\ldots b_n\ldots$$

pongamos $0,b_1b_2 \ldots b_n = B$, de manera que B represente la parte periódica del decimal. Entonces, p puede escribirse así:

$$p = 0, a_1a_2 \ldots a_m + 10^{-m}B(1 + 10^{-n} + 10^{-2n} + 10^{-3n} + \ldots).$$

La expresión entre paréntesis es una serie geométrica con $q = 10^{-n}$; su suma, de acuerdo con la ecuación [10] de la página 74, es $1/(1-10^{-n})$, y, por tanto, se tiene

$$p = 0, a_1a_2 \ldots a_m + \frac{10^{-m}B}{1 - 10^{-n}}$$

Ejercicios:

1. Desarróllense las fracciones $\frac{1}{11}, \frac{1}{13}, \frac{2}{13}, \frac{3}{13}, \frac{1}{17}, \frac{2}{17}$ en fracciones decimales y determínese el período.

*2. El número 142 857 tiene la propiedad de que multiplicado por cualquiera de los números 2, 3, 4, 5 ó 6 da otro que tiene las mismas cifras en diferente orden. Justifíquese esta propiedad, utilizando el desarrollo de 1/7 en fraccion decimal.

3. Desarróllense los números racionales del ejercicio 1 como fracciones «decimales» en los sistemas de numeración de bases 5, 7 y 12.

4. Desarróllese 1/3 como número diádico.

5. Escríbase 0,11212121 . . . como fracción ordinaria. Hállese el valor de dicho símbolo en los sistemas de numeración de base 3 ó 5.

5. Definición general de los números irracionales mediante encajes de intervalos.—En la página 71 adoptamos como definición provisional la siguiente: un *número* es un decimal finito o infinito, y conveníamos en que aquellos decimales infinitos que no correspondían a números racionales serían llamados números irracionales. Sobre la base de los resultados de la sección precedente podemos ahora formular esta definición en la siguiente forma: *el continuo numérico*, o *sistema de números reales* («real» en oposición a los números «imaginarios» o «complejos» que introduciremos en V) es *la totalidad de los decimales infinitos*. (Los decimales finitos quedan considerados como un caso especial de los infinitos: aquel en que todas las cifras a partir de una de ellas son ceros; otra manera de considerarlos será la de reemplazar la última cifra a por $a - 1$ y hacerla seguir de una infinidad de cifras todas iguales a 9. Esto expresa el hecho de que $0,9999 \ldots = 1$, de acuerdo con la sección 3.) Los números *racionales* son los decimales *periódicos*; los números *irracionales* son los decimales *no-periódicos*. Sin embargo, esta definición no es aún plenamente satisfactoria, puesto que, como hemos visto en el capítulo primero, el sistema decimal no se diferencia de los de otras bases por propiedades intrínsecas del sistema de números. En consecuencia, podíamos muy bien haber seguido los razonamientos de las secciones precedentes utilizando el sistema diádico u otro cualquiera. Por esta razón es de desear una definición más general del continuo numérico, independiente de especiales referencias al sistema de base diez. Quizá la más sencilla sea la siguiente:

Consideremos una sucesión cualquiera de intervalos $I_1, I_2, ..., I_n, ...$ de la recta numérica, cuyos extremos sean puntos racionales, cada uno de los cuales esté contenido en el precedente, y tal que la longitud del intervalo n-ésimo I_n tienda a cero al crecer n. A una tal sucesión la llamaremos *sucesión de intervalos encajados* o *encaje de intervalos*. En el caso de intervalos decimales, la longitud de I_n era 10^{-n}; pero en el caso general puede ser muy bien 2^{-n}, o estar simplemente sujetos a la restricción de ser menores que $1/n$. En estas condiciones vamos a formular un postulado fundamental en geometría: *en correspondencia con cada sucesión de intervalos encajados existe precisamente un punto de la recta numérica que está contenido en todos los intervalos.* (Se ve directamente que no puede haber más de *un* punto común a todos los intervalos, puesto que las longitudes de éstos tienden a cero y dos puntos no pueden estar contenidos en un intervalo de longitud menor que su distancia.) El punto a que se refiere el postulado es por definición un *número real*; si no es un punto racional, se dice que es un *número irracional*. Mediante esta definición establecemos una correspondencia perfecta entre puntos y números. Con ella damos una formulación más general a lo que expresábamos con la definición que utilizaba los decimales infinitos.

Al llegar a este punto quizá el lector se sienta inquietado por una duda completamente legítima: ¿cuál *es* el «punto» de la recta numérica que hemos supuesto pertenecía a todos los intervalos de la sucesión, en el caso de que no se trate de un punto racional? Nuestra respuesta es: la existencia, en la recta numérica, de un punto contenido en cualquier encaje de intervalos cuyos extremos sean puntos racionales es un *postulado fundamental de la geometría.* No es, por tanto, precisa la reducción lógica de esta proposición a otros hechos matemáticos. La aceptamos, lo mismo que aceptamos otros axiomas o postulados de la matemática, a causa de que es plausible de modo intuitivo, y también en virtud de su utilidad para la construcción de un sistema no contradictorio del proceso matemático. Desde un punto de vista puramente formal se podía haber partido de una recta constituída únicamente por puntos racionales y luego *definir* como punto irracional un *símbolo que representa determinadas sucesiones de intervalos racionales encajados.* Un punto irracional queda así perfectamente determinado por la sucesión de intervalos en cuestión. Resulta, por tanto, que nuestro postulado equivale a una definición. Establecer esta definición después de haber llegado a los encajes de intervalos racionales, gracias al sentimiento intuitivo de que los puntos irracionales «existen», equivale a prescindir de los apoyos intuitivos con los que nuestro razonamiento está acostumbrado a proceder y darse cuenta de que todas las *propiedades matemáticas* de los puntos irracionales pueden venir expresadas como propiedades de los encajes de intervalos racionales.

Tenemos aquí un ejemplo típico de la posición filosófica descrita en la introducción de este libro; prescindir del ingenuo punto de vista «realista», que considera los objetos matemáticos como *cosas en sí* de

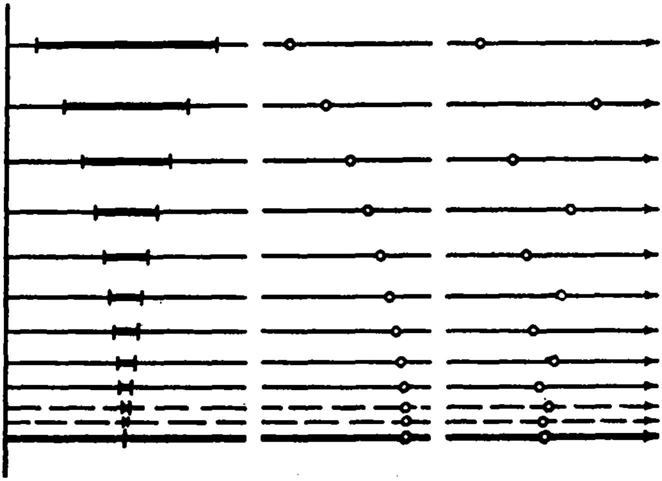


FIG. 11.—Encaje de intervalos. Límites de sucesiones.

las cuales pretendemos modestamente determinar las propiedades, y, en cambio, comprobar que el único modo de existir de los objetos matemáticos que nos importa reside en sus propiedades matemáticas y en las relaciones que los ligan. Estas propiedades y relaciones agotan todos los aspectos posibles bajo los cuales puede intervenir un objeto en el mundo de la actividad matemática. Dejamos de lado la «cosa en sí» matemática, del mismo modo que los físicos dejan de lado el inobservable éter; éste es el significado de la definición *intrínseca* de un número irracional como encaje de intervalos racionales.

La cuestión matemática importante a este respecto es la de que para los números irracionales así definidos, se pueden generalizar de modo inmediato las operaciones de adición, multiplicación, etc., y las relaciones de «menor que» y «mayor que» establecidas para los números racionales, siendo dicha generalización de tal naturaleza que las reglas y leyes válidas para los números racionales se conservan para los nuevos números; p. ej., la adición de dos números irracionales α y β puede venir dada por medio de los dos encajes de intervalos que sirvieron para definir α y β. Se construye una tercera sucesión de intervalos encajados sumando los valores de los orígenes y los de los extremos de los intervalos correspondientes a los dos encajes que definen α y β, y la nueva sucesión de intervalos encajados define $\alpha + \beta$. Análogamente se pueden definir el producto $\alpha\beta$, la diferencia $\alpha - \beta$ y el cociente α/β. Sobre la base de estas definiciones se prueba que las leyes aritméticas que discutimos anteriormente en este capítulo continúan siendo válidas para los números irracionales. Sin embargo, no daremos aquí los detalles de tales demostraciones.

La comprobación de las leyes anteriores es simple y fácil, aunque resulta a veces enojosa para el principiante, que desea más bien aprender las matemáticas como instrumento que analizar sus fundamentos lógicos. Algunos de los textos modernos de matemáticas repelen a numerosos estudiantes, debido a que comienzan con un análisis completo del sistema de los números reales, análisis que resulta un poco pedante. El lector que prescinde simplemente de esa introducción procede con el mismo espíritu con que, hasta fines del siglo pasado, hicieron sus descubrimientos los más grandes matemáticos sobre la base del concepto «ingenuo» del sistema numérico que les proporcionaba su intuición.

Desde el punto de vista físico, la definición de un número irracional mediante un encaje de intervalos corresponde a la determinación de una cantidad observable por una sucesión de medidas de aproximación creciente. Toda operación de determinación, p. ej., de una longitud, tiene significación práctica dentro de los límites de un cierto error posible, error que mide la precisión de la operación. Puesto que los números racionales forman un conjunto denso en la recta, resulta imposible determinar para toda operación física, cualquiera que sea su precisión, si una longitud dada es racional o irracional. De aquí podría parecer que los números irracionales son superfluos para una adecuada descripción de los fenómenos físicos; sin embargo, como veremos más claramente en el capítulo VI, la ventaja efectiva que la introducción de los números irracionales aporta a la descripción matemática de los fenómenos físicos es la de que dicha descripción se simplifica de modo notable, gracias a la posibilidad de utilizar libremente el concepto de límite, para el cual es fundamental el continuo numérico.

***6. Otros métodos de definición de números irracionales. Cortaduras de Dedekind.**—Otra manera de definir los números irracionales fué dada por Richard Dedekind (1831-1916), uno de los grandes iniciadores del análisis lógico y filosófico de los fundamentos de la matemática. Sus obras *Stetigkeit und irrationale Zahlen* (1872) y *Was sind und was sollen die Zahlen?* (1887) ejercieron una profunda influencia en los estudios sobre los fundamentos de la matemática. Dedekind prefería operar con ideas generales abstractas a hacerlo con sucesiones determinadas de encajes de intervalos. Su método está basado en la definición de «cortadura» que vamos a exponer brevemente.

Supongamos que se ha dado un cierto método para dividir el conjunto de *todos los números racionales* en dos clases, A y B, tales que todo número b de la clase B es mayor que todo elemento a de la clase A. Toda clasificación de este tipo se llama una *cortadura* en el campo de los números racionales. Para una cortadura hay precisamente tres posibilidades, que se excluyen mutuamente:

1) *Hay en* A *un elemento máximo* a*. Este es, p. ej., el caso cuando A está formada por todos los números racionales $\leqslant 1$ y B por todos los números racionales >1.

2) *Hay en* B *un elemento mínimo* b*. Así sucede, p. ej., si A está constituída por todos los números racionales < 1 y B por todos los números racionales $\geqslant 1$.

3) *No hay elemento máximo en* A *ni elemento mínimo en* B. Se tiene, en particular, este caso cuando A está formada por todos los números racionales negativos, el 0, y todos los números racionales positivos cuyo cuadrado es menor que 2, y B por todos los números racionales positivos cuyo cuadrado es mayor que 2. A y B, reunidas, comprenden todos los números racionales, puesto que hemos probado que no hay ningún número racional cuyo cuadrado sea igual a 2.

El caso en que A tuviera un elemento máximo a^* y B un elemento mínimo b^* es imposible, puesto que en dicho caso el número racional $(a^* + b^*)/2$, que está comprendido entre a^* y b^*, sería mayor que el elemento máximo de A y más pequeño que el elemento mínimo de B, y no pertenecería a ninguna de las dos clases.

En el tercer caso, aquel en el que no hay elemento máximo en A ni elemento mínimo en B, la cortadura, según Dedekind, define o simplemente *es* un número irracional. Es fácil ver que esta definición concuerda con la dada mediante encajes de intervalos; cualquier sucesión I_1, I_2, I_3, ... de intervalos encajados define una cortadura, si colocamos en la clase A todos los números racionales que son menores que el origen de al menos uno de los intervalos I_n, y en B todos los demás números racionales.

Desde un punto de vista filosófico, la definición de Dedekind de números irracionales representa un mayor grado de abstracción, puesto que no impone restricción alguna a la ley matemática que define las dos clases A y B. Un método más concreto de definir el continuo numérico real se debe a Georg Cantor (1845-1918). Aunque a primera vista parece completamente diferente del método de los encajes de intervalos y del de las cortaduras, en realidad es equivalente a ambos, en el sentido de que los sistemas numéricos definidos de las tres maneras gozan de las mismas propiedades. La idea de Cantor aparece sugerida por los dos hechos siguientes: 1) los números reales pueden considerarse como decimales de infinitas cifras, y 2) los decimales infinitos son límites de fracciones decimales finitas.

Prescindiendo de la dependencia del sistema decimal se puede decir, siguiendo a Cantor, que toda sucesión $a_1, a_2, a_3, \ldots$ de números racionales define un *número real* si dicha sucesión «converge». La convergencia significa que la diferencia $(a_m - a_n)$ entre dos números cualesquiera de la sucesión tiende a cero cuando a_m y a_n ocupan lugares suficientemente avanzados en la sucesión; es decir, cuando m y n tienden a infinito. (Las sucesivas aproximaciones decimales de todo número gozan de dicha propiedad, puesto que dos números posteriores al n-ésimo difieren en menos de 10^{-n}.) Dado que existen muchas formas de aproximarse al mismo número real mediante sucesiones de números racionales, diremos que dos sucesiones convergentes de números racionales $a_1, a_2, a_3, \ldots$ y $b_1, b_2, b_3, \ldots$ definen el mismo número real si $a_n - b_n$ tiende a cero cuando n crece indefinidamente. Es fácil definir, para tales sucesiones, las operaciones de adición, multiplicación, etc.

III. OBSERVACIONES SOBRE GEOMETRÍA ANALÍTICA [1]

1. El principio fundamental.—El continuo numérico, aceptado como cosa inmediata o bien después de un examen crítico, ha constituído la base de las matemáticas—y en particular de la geometría analítica y del cálculo—desde el siglo XVII.

La introducción del continuo numérico hace posible asociar a cada segmento rectilíneo un determinado número real que da su longitud. Pero aún se puede ir más lejos: no sólo las longitudes, sino también *todo objeto geométrico y toda operación geométrica, pueden ser referidos al reino de los números*. Los pasos decisivos en esta aritmetización de la geometría fueron dados por Fermat (1601-1655) en 1629 y por Descartes (1596-1650) en 1637. La idea fundamental de la geometría analítica es la introducción de «coordenadas»; esto es, de *números* ligados o coordinados con un *objeto geométrico* y que caracterizan completamente a éste. La mayor parte de los lectores conocen, sin duda, las llamadas coordenadas cartesianas rectangulares, que sirven para caracterizar la posición de un punto P en un plano. Se parte de dos rectas fijas perpendiculares del plano, el «eje x» y el «eje y», a las que se refiere todo punto. Estas rectas se consideran como rectas numéri-

[1] El lector que no conozca suficientemente esta materia encontrará en el Apéndice del final del libro una serie de ejercicios sobre los elementos de geometría analítica.

cas orientadas, y se miden con la misma unidad. A cada punto P (Fig. 12) se le asignan dos coordenadas x e y. Estos números se obtienen de la siguiente forma: consideremos el segmento dirigido desde el «origen» O al punto P, y proyectemos este segmento orientado, que a veces se llama «vector de posición» de P, perpendicularmente sobre

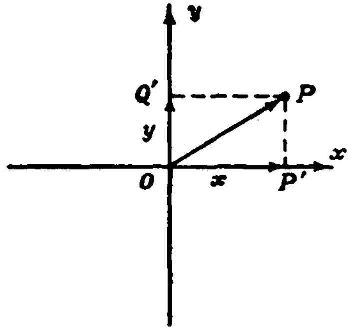


FIG. 12.—Coordenadas rectangulares de un punto.

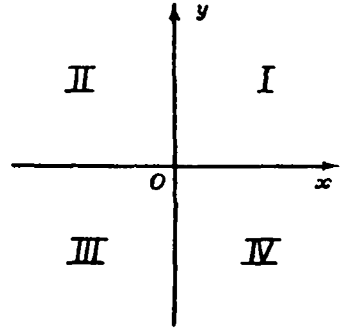


FIG. 13.—Los cuatro cuadrantes.

los dos ejes; de este modo se obtiene el segmento orientado OP' sobre el eje x, con el número x como medida de su longitud orientada a partir de O, y del mismo modo el segmento orientado OQ' sobre el eje y, con el número y como medida de su longitud orientada a partir de O. Los dos números x, y son las *coordenadas* de P. Recíprocamente: si x, y son dos números arbitrarios dados, el punto P correspondiente está unívocamente determinado. Si x, y son los dos positivos, P está en el *primer cuadrante* del sistema de coordenadas (Fig. 13); si los dos son negativos, P está en el tercer cuadrante; si x es positivo e y negativo, P estará en el cuarto cuadrante y, finalmente, si x es negativo e y positivo, P se hallará en el segundo cuadrante.

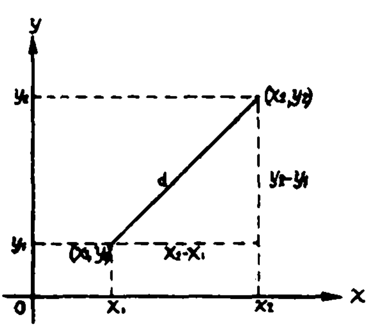


FIG. 14.—Distancia entre dos puntos.

La distancia entre el punto P_1, de coordenadas x_1, y_1, y el punto P_2, de coordenadas x_2, y_2, viene dada por la fórmula

$$d^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2, \qquad [1]$$

la cual se obtiene inmediatamente por el teorema de Pitágoras, como resulta de la figura 14.

***2. Ecuaciones de rectas y curvas.**—Si C es un punto fijo de coordenadas $x = a$, $y = b$, el lugar de todos los puntos P que están a una distancia r dada de C es una circunferencia con centro C y radio r. De la fórmula [1], que da la distancia entre dos puntos, resulta que los puntos de dicha circunferencia tienen coordenadas x, y que satisfacen la ecuación

$$(x - a)^2 + (y - b)^2 = r^2. \qquad [2]$$

Ésta es la llamada *ecuación de la circunferencia*, ya que expresa la condición completa (necesaria y suficiente) que han de cumplir las coordenadas x, y de un punto P para estar sobre la circunferencia de centro C y radio r. Si se desarrollan los paréntesis de [2], dicha ecuación toma la forma

$$x^2 + y^2 - 2ax - 2by = k, \qquad [3]$$

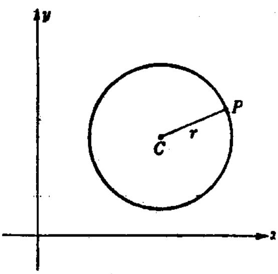


FIG. 15.—La circunferencia.

donde $k = r^2 - a^2 - b^2$. Recíprocamente: si se tiene una ecuación de la forma [3], siendo a, b y k constantes arbitrarias tales que $k + a^2 + b^2$ es positivo, mediante el proceso algebraico de «completar los cuadrados», podemos escribir la ecuación en la forma

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

donde es $r^2 = k + a^2 + b^2$. Resulta, en consecuencia, que la ecuación [3] define una circunferencia de radio r, que tiene su centro en el punto C de coordenadas a y b.

Las ecuaciones de las rectas tienen una forma todavía más sencilla; p. ej., el eje x tiene como ecuación $y = 0$, puesto que $y = 0$ se verifica para todos los puntos del eje x y sólo para ellos. El eje y tiene la ecuación $x = 0$. Las rectas que pasan por el origen y bisecan los ángulos formados por los ejes tienen como ecuaciones $x = y$ y $x = -y$. Es fácil probar que toda recta tiene una ecuación de la forma

$$ax + by = c, \qquad [4]$$

donde a, b y c son constantes que caracterizan la recta. La significación de la ecuación [4] es la de que todos los pares de valores x, y que la satisfacen son coordenadas de puntos de la recta, y recíprocamente.

Es posible que el lector sepa que la ecuación

$$\frac{x^2}{p^2} + \frac{y^2}{q^2} = 1 \qquad [5]$$

representa una elipse (Fig. 16). Esta curva corta al eje x en los puntos $A(p, 0)$ y $A'(-p, 0)$, y al eje y en $B(0, q)$ y $B'(0, -q)$. (Usaremos la notación $P(x, y)$ o simplemente (x, y) para designar brevemente «el punto P con coordenadas x, y».) Si es $p > q$, el segmento AA', de longitud $2p$, se llama eje mayor de la elipse, mientras que el segmento BB', de longitud $2q$, se llama eje menor. La elipse es el lugar de todos los puntos P cuya suma de distancia a los puntos $F(\sqrt{p^2-q^2}, 0)$

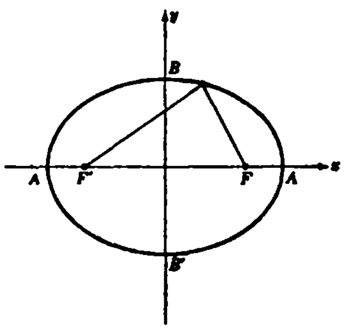


FIG. 16.—La elipse; F y F' son los focos.

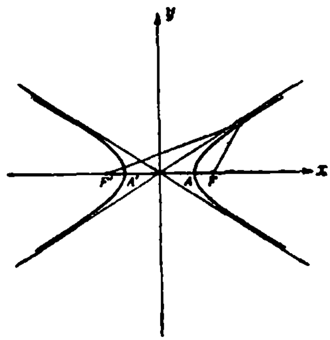


FIG. 17.—La hipérbola; F y F' son los focos.

y $F'(-\sqrt{p^2-q^2}, 0)$ es $2p$. El lector puede comprobar esto, como ejercicio, utilizando la fórmula [1]. Los puntos F y F' se llaman *focos* de la elipse, y el cociente $e = \dfrac{\sqrt{p^2-q^2}}{p}$ se denomina *excentricidad* de la misma.

Una ecuación de la forma

$$\frac{x^2}{p^2} - \frac{y^2}{q^2} = 1 \qquad [6]$$

representa una hipérbola. Esta curva (Fig. 17) está formada por dos ramas que cortan al eje x en los puntos $A(p, 0)$ y $A'(-p, 0)$, respectivamente. El segmento AA', de longitud $2p$, se llama eje transversal de la hipérbola. La hipérbola se aproxima indefinidamente a las dos rectas $qx \pm py = 0$ a medida que se aleja del origen, sin llegar nunca a tocarlas; dichas rectas se llaman *asíntotas* de la hipérbola. La hipérbola es el lugar de todos los puntos P cuya *diferencia* de distancias a los dos puntos $F(\sqrt{p^2 + q^2}, 0)$ y $F'(-\sqrt{p^2 + q^2}, 0)$ es $2p$. Estos dos puntos se llaman focos de la hipérbola; la excentricidad de la curva viene dada por el cociente $e = \dfrac{\sqrt{p^2 + q^2}}{p}$.

La ecuación

$$xy = 1 \tag{7}$$

define también una hipérbola cuyas asíntotas son los ejes coordenados (Fig. 18). La ecuación de esta hipérbola «equilátera» indica que el área del rectángulo determinado por P y los ejes (Fig. 18) es igual a 1 para todo punto P de la curva.

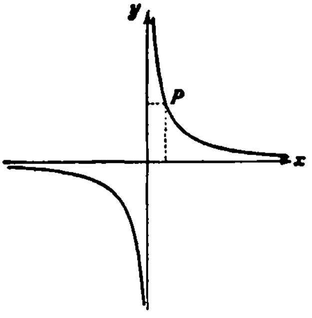


FIG. 18.—La hipérbola equilátera $xy = 1$. El área xy del rectángulo determinado por el punto P (x, y) es igual a 1.

Una hipérbola equilátera cuya ecuación sea

$$xy = c, \tag{7a}$$

siendo c una constante, es sólo un caso particular de hipérbola, del mismo modo que la circunferencia es un caso particular de la elipse. La particularidad de la hipérbola equilátera reside en el hecho de que sus asíntotas (en el caso presente, los ejes) son perpendiculares entre sí.

Para nosotros, la cuestión fundamental es la idea de que los objetos geométricos pueden ser representados de modo completo mediante elementos aritméticos y algébricos, y que lo mismo sucede con las operaciones geométricas; p. ej., si queremos determinar el punto de intersección de dos rectas, consideraremos las dos ecuaciones

$$\begin{aligned} ax + by &= c \\ a'x + b'y &= c'. \end{aligned} \tag{8}$$

El punto común a las rectas se hallará determinando sus coordenadas, que no son otra cosa que la solución x, y del sistema [8]. Análogamente, los puntos de intersección de dos líneas, tales como la circunferencia $x^2 + y^2 - 2ax - 2by = k$ y la recta $ax + by = c$, se hallarían resolviendo el sistema formado por las ecuaciones de ambas líneas.

IV. ANÁLISIS DEL CONCEPTO MATEMÁTICO DE INFINITUD

1. Conceptos fundamentales.—La sucesión de los enteros positivos

$$1, 2, 3, \ldots$$

es el primer y mas importante ejemplo de conjunto infinito. No hay ningún misterio en el hecho de que esta sucesión no tiene fin; puesto que, por grande que sea el entero n, siempre se puede formar el entero siguiente $n + 1$. Pero el paso del *adjetivo* «infinito», que significa simplemente «sin fin», al *sustantivo* «infinito» no debe hacernos pensar que «infinito», representado generalmente con el símbolo ∞, puede considerarse como si fuera un *número* ordinario. No es posible incluir el símbolo ∞ en el sistema de los números reales y conservar al mismo tiempo las leyes fundamentales de la aritmética. Sin embargo, el concepto de infinito invade toda la matemática, ya que los objetos matemáticos son considerados habitualmente, no como individuos, sino como miembros de clases o conjuntos que contienen una infinidad de objetos del mismo tipo, tales como el conjunto de todos los enteros, o el de los números reales, o el de los triángulos de un plano. Por esta razón es necesario analizar el infinito matemático de una manera precisa. La teoría moderna de conjuntos, creada por Georg Cantor y su escuela a fines del siglo pasado, obtuvo brillantes resultados en tal cometido. La teoría de conjuntos de Cantor ha penetrado y ejercido enorme influjo en varios campos de la matemática, y ha llegado a ser de importancia fundamental en el estudio de las bases lógicas y filosóficas de dicha ciencia. El punto de partida es el concepto general de *conjunto* o *agregado*. En este concepto se comprende toda colección de objetos definida por una regla determinada que especifica exactamente qué objetos pertenecen a la colección. Como ejemplos podemos considerar el conjunto de todos los enteros positivos; el de todos los decimales periódicos; el conjunto de todos los números reales, o el de todas las rectas del espacio de tres dimensiones.

Para comparar la «magnitud» de dos conjuntos diferentes es fundamental la noción de «equivalencia». Si los elementos de dos conjuntos A y B pueden ser apareados, de modo que a todo elemento de A corresponda un elemento (y sólo uno) de B y a cada elemento de B corresponda un elemento de A, y uno solo, la correspondencia entre A y B se llama *biunívoca*, y dichos conjuntos se dicen *equivalentes* o *coordinables*. La noción de equivalencia para conjuntos *finitos* coincide con la noción ordinaria de *igualdad de números*, puesto que dos conjuntos finitos tienen el mismo número de elementos cuando (y sólo entonces) se pueden poner en correspondencia biunívoca. Ésta es, en realidad, la verdadera idea que interviene en la operación de contar, ya que cuando contamos un conjunto finito de objetos lo que hacemos es establecer una correspondencia biunívoca entre dichos objetos y el conjunto de símbolos numéricos 1, 2, 3, ... , n.

No es necesario siempre contar los objetos de dos conjuntos finitos para comprobar su equivalencia; p. ej., se puede afirmar, sin necesidad de contar, que todo conjunto finito de circunferencia de radio 1 es coordinable con el conjunto de sus centros.

La idea de Cantor fué la de extender el concepto de equivalencia a los conjuntos infinitos para poder de este modo definir una «aritmética» de los infinitos. El conjunto de todos los números reales y el conjunto de todos los puntos de una recta son equivalentes, puesto que la elección del origen y del segmento unidad permite asociar de modo biunívoco cada punto P de la recta con un número real x determinado, su abscisa:

$$P \longleftrightarrow x.$$

Los *enteros pares* forman un subconjunto propio del conjunto de *todos los enteros*, y los *enteros* forman un subconjunto propio del conjunto de todos los *números racionales*. (Con la frase *subconjunto propio* de un conjunto S designamos un conjunto S' formado por algunos, *no todos*, de los objetos de S). Evidentemente, *si un conjunto es finito*, es decir, si contiene un cierto número n de elementos, *no puede ser equivalente a ninguno de sus subconjuntos propios*, ya que cualquier subconjunto puede contener a lo sumo $n-1$ elementos. En cambio, *si un conjunto contiene infinitos objetos* se verifica, lo que a primera vista parece paradójico, *que es equivalente a algunos de sus subconjuntos propios;* p. ej., la coordinación

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & \dots & n & \dots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \\ 2 & 4 & 6 & 8 & 10 & \dots & 2n & \dots \end{array}$$

establece una correspondencia biunívoca entre el conjunto de los *enteros positivos* y su subconjunto propio formado por los *enteros pares*, y, por tanto, ambos conjuntos son equivalentes. Esta contradicción con el familiar axioma «el todo es mayor que cualquiera de sus partes» muestra qué sorpresas pueden presentarse en el dominio del infinito.

2. La numerabilidad de los números racionales y la no-numerabilidad del continuo.—Uno de los primeros descubrimientos de Cantor en su análisis del infinito fué el de que el conjunto de los *números racionales* (que contiene el conjunto infinito de los enteros y que, por consiguiente, es infinito) es equivalente al *conjunto de los enteros*. A primera vista resulta bastante extraño que el conjunto denso en la recta de los números racionales pueda ser equivalente al disperso conjunto de los enteros. Ciertamente, no se pueden colocar los números positivos racionales *en orden de magnitud* (como ocurre con los enteros), de modo que haya un a que sea el primer número racional, b el inmediato mayor, y así sucesivamente, puesto que existen infinitos números racionales entre dos cualesquiera dados, y, por consiguiente, carece de sentido la expresión «el inmediato mayor». Pero, como observó Cantor, prescindiendo de la relación de magnitud entre los elementos consecutivos, es posible colocar los números racionales en una sucesión r_1, r_2, r_3, ..., análoga a la de los enteros. En dicha sucesión habrá un primer número racional, un segundo, un tercero y así sucesivamente, y todo número racional aparecerá precisamente una vez. Una ordenación de los elementos de un conjunto en una sucesión análoga a la de los enteros se llama una *enumeración* del conjunto. Construyendo una enumeración del conjunto de los números racionales, Cantor probó que dicho conjunto es equivalente al de los números enteros, ya que la correspondencia

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & \cdots & n & \cdots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \\ r_1 & r_2 & r_3 & r_4 & \cdots & r_n & \cdots \end{array}$$

es biunívoca. Vamos a describir una manera efectiva de enumeración de los números racionales.

Todo número racional puede escribirse en la forma a/b, donde a y b son enteros, y todos aquellos números pueden disponerse en un cuadro, con a/b en la fila a y en la columna b; p. ej., 3/4 estará en la tercera fila y en la cuarta columna. Entonces, todos los números racionales positivos pueden ser ordenados según el esquema siguiente: en el cuadro anterior trazamos una línea quebrada continua que pase por todos los números del cuadro en la forma indicada en la figura 19. Partiendo del 1, vamos horizontalmente hasta el primer lugar a la derecha, obteniendo el 2 como segundo término de la sucesión; vamos entonces diagonalmente hacia abajo, a la izquierda, hasta la primera columna, a alcanzar la posición ocupada por el 1/2; luego, verticalmente, hacia abajo, un lugar, hasta el 1/3; después, diagonalmente hacia arriba y a la derecha, alcanzamos el 3: de ahí pasamos al 4 y después, diagonalmente, hasta el 1/4, y así sucesivamente. A través de esta línea quebrada se obtiene la sucesión 1, 2, 1/2, 1/3, 2/2, 3, 4, 3/2, 2/3, 1/4, 1/5, 2/4, 3/3, 4/2, 5. ... que contiene los números racionales en el orden en que aparecen en la línea quebrada. En dicha sucesión suprimimos aquellos números a/b para los cuales a y b tienen un factor común, de modo que cada número racional aparezca una sola vez, representado por una fracción irreducible. Se obtiene así la sucesión

$$\begin{array}{cccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & \cdots \\
\frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \frac{4}{2} & \frac{5}{2} & \frac{6}{2} & \frac{7}{2} & \cdots \\
\frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \frac{4}{3} & \frac{5}{3} & \frac{6}{3} & \frac{7}{3} & \cdots \\
\frac{1}{4} & \frac{2}{4} & \frac{3}{4} & \frac{4}{4} & \frac{5}{4} & \frac{6}{4} & \frac{7}{4} & \cdots \\
\frac{1}{5} & \frac{2}{5} & \frac{3}{5} & \frac{4}{5} & \frac{5}{5} & \frac{6}{5} & \frac{7}{5} & \cdots \\
\frac{1}{6} & \frac{2}{6} & \frac{3}{6} & \frac{4}{6} & \frac{5}{6} & \frac{6}{6} & \frac{7}{6} & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots
\end{array}$$

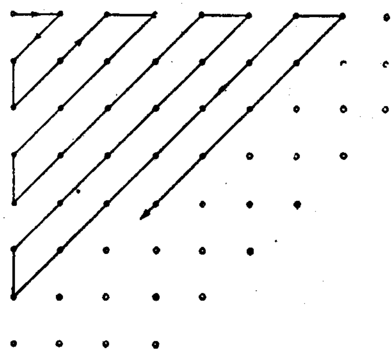


FIG. 19.—El conjunto de los números racionales es numerable.

1, 2, 1/2, 1/3, 3, 4, 3/2, 2/3, 1/4, 1/5, 5, ... la cual contiene cada número racional una sola vez. Resulta así la numerabilidad del conjunto de los números racionales. Como consecuencia de la correspondencia biunívoca entre los números racionales y los puntos racionales de una recta, se tiene la numerabilidad del conjunto de los puntos racionales de la recta.

Ejercicios:

1. Pruébese que el conjunto de todos los enteros positivos y negativos es numerable. Pruébese que el conjunto de los números racionales positivos y negativos es numerable.
2. Pruébese que el conjunto $S + T$ (véase pág. 120) es numerable si S y T son numerables. Pruébese el mismo hecho para el caso de una suma de tres, cuatro o cualquier número n de conjuntos, y, finalmente, para un conjunto numerable de conjuntos numerables.

Habiendo demostrado que el conjunto de números racionales es numerable, podría esperarse que *todo* conjunto infinito fuera también numerable, con lo que se tendría el resultado final del análisis del infinito. La realidad de los hechos es muy distinta. El mismo Cantor obtuvo el notable resultado de que el *conjunto de los números reales*, racionales e irracionales, *no es numerable*. En otros términos, el conjunto de los números reales presenta una diferencia radical y, por así decirlo, un tipo superior de infinitud que el de los enteros o el de los números racionales. La ingeniosa demostración indirecta de este hecho, debida a Cantor, ha quedado como modelo para un cierto tipo de demostraciones matemáticas. Las líneas principales de dicha demostración son las siguientes: se parte de la hipótesis de que todos los números reales pueden ser efectivamente enumerados y dispuestos en una sucesión, y se construye luego un número real que no figura en dicha sucesión. De ahí resulta una contradicción con la hipótesis inicial, que suponía que *todos* los números reales estaban incluídos en la sucesión; la hipótesis de que la enumeración de los números reales es posible resulta absurda y, en consecuencia, la hipótesis contraria, es decir, la proposición de Cantor de que el conjunto de los números reales no es numerable queda demostrada.

Para llevar a cabo el programa indicado, supongamos que hemos enumerado todos los números reales colocándolos en una tabla de decimales infinitos

1.^{er} número	$N_1,a_1a_2a_3a_4a_5 \cdots$
2.^{o} número	$N_2,b_1b_2b_3b_4b_5 \cdots$
3.^{er} número	$N_3,c_1c_2c_3c_4c_5 \cdots$
. . . . . .	. . . .

donde las N designan la parte entera y las letras minúsculas las cifras decimales. Supongamos que esta sucesión de fracciones decimales contiene *todos* los números reales. El punto esencial de la demostración consiste en construir, por un «proceso diagonal», un número del que se demuestra que no puede estar en la sucesión. Para ello, comencemos por elegir una cifra a distinta de a_1 y de 0 y 9 (las últimas exigencias se hacen para evitar ambigüedades que puedan resultar de igualdades análogas a la $0,9999 \ldots = 1,0000 \ldots$); luego, una cifra b distinta de b_2, de 0 y de 9; después, una c diferente de c_3, de 0 y de 9, y así sucesivamente. (P. ej., se puede elegir $a = 1$, a no ser que sea $a_1 = 1$, en cuyo caso tomaríamos $a = 2$, y análogamente para las cifras $b, c, d, e, \ldots$.) Consideremos entonces el decimal infinito

$$z = 0,abcde \cdots .$$

Este nuevo número z es ciertamente distinto de cualquiera de los que están en la tabla anterior; no puede ser igual al primero, puesto que difiere de él en la primera cifra decimal; no puede ser igual al segundo, porque tiene distinta la segunda cifra decimal; y, en general, no puede ser igual al que ocupa el lugar n, porque difiere de él en la n-ésima cifra decimal. Esto prueba que dicha tabla, en la que hemos dispuesto una sucesión de números reales, *no* puede contener todos los números reales. El conjunto de estos números no es, por tanto, numerable.

Quizá pueda sospechar el lector que la razón de la no-numerabilidad del continuo numérico esté en el hecho de que la recta se extiende infinitamente, y que posiblemente pueda ser numerable el conjunto de los puntos de un segmento finito de recta. Se comprueba fácilmente que no es éste el caso viendo que el continuo numérico es equivalente a cualquier segmento finito; p. ej., al (0,1), del que se han excluído los extremos. La correspondencia biunívoca deseada se puede obtener formando con dicho segmento una quebrada de tres lados de

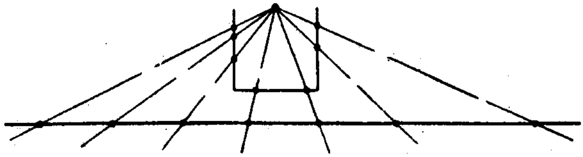


FIG. 20.—Correspondencia biunívoca entre los puntos de una poligonal y los de la recta completa.

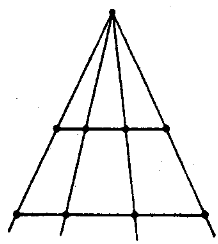


FIG. 21.—Correspondencia biunívoca entre los puntos de dos segmentos de distinta longitud.

longitud igual a 1/3 y proyectando desde un punto conveniente, como se indica en la figura 20. Resulta, por tanto, que también un segmento finito de la recta numérica contiene una infinidad no-numerable de puntos.

Ejercicio: Pruébese que cualquier intervalo $[A, B]$ de la recta numérica es equivalente a otro intervalo cualquiera $[C, D]$.

Vale la pena indicar otra demostración, quizá más intuitiva, de la no-numerabilidad del continuo numérico. Apoyándonos en lo que acabamos de decir, será suficiente que nos ocupemos del conjunto de puntos comprendidos entre 0 y 1. La nueva demostración será también por reducción al absurdo. Supongamos que el conjunto de todos los puntos de la recta comprendidos entre 0 y 1 puede ser ordenado en una sucesión

$$a_1, a_2, a_3, \cdots . \qquad [1]$$

Incluyamos el punto a_1 en un intervalo de longitud $1/10$, el punto a_2 en un intervalo de longitud $1/10^2$, y así sucesivamente. Si todos los puntos del intervalo (0,1) estuvieran en la sucesión [1], el intervalo unidad aparecería completamente recubierto, en parte quizá por intervalos superpuestos, por la sucesión de intervalos de longitudes $1/10$, $1/10^2$, ... que hemos construído. (El hecho de que alguno de los intervalos pueda extenderse fuera del segmento unidad no influye en la demostración.) La suma de las longitudes de dichos intervalos viene dada por la serie geométrica

$$1/10 + 1/10^2 + 1/10^3 + \dots = \frac{1}{10}\left[\frac{1}{1-\frac{1}{10}}\right] = \frac{1}{9}$$

Así, la hipótesis de que la sucesión [1] contiene todos los números reales comprendidos entre 0 y 1 que llenan el intervalo completo de longitud 1 conduce a la contradicción de que dicho intervalo puede ser recubierto por un conjunto de intervalos de longitud total igual a 1/9, lo cual es intuitivamente absurdo. Aceptaremos esta contradicción como una demostración, aunque desde un punto de vista lógico requeriría un análisis más detallado.

El razonamiento del párrafo anterior sirve para establecer un teorema de gran importancia en la teoría moderna de la *medida*. Reemplazando los intervalos anteriores por otros más pequeños de longitud $\varepsilon/10^n$, donde ε es un número positivo arbitrariamente pequeño, se ve que los puntos de todo conjunto numerable de la recta pueden ser incluídos en un conjunto de intervalos de longitud total igual a $\varepsilon/9$. Puesto que ε es arbitrario, dicha longitud total puede ser tan pequeña como se quiera. En la terminología de la teoría de la medida expresaremos este hecho diciendo que un conjunto numerable de puntos tiene *medida nula*.

Ejercicio: Demuéstrese que el mismo resultado tiene lugar para un conjunto numerable de puntos de un plano, reemplazando las longitudes de los intervalos por áreas de cuadrados.

3. «Números cardinales» de Cantor.—Resumiendo los resultados expuestos hasta ahora, se tiene: el número de elementos de un conjunto *finito* A no puede ser igual al número de elementos de un conjunto finito B, si A contiene *más* elementos que B. Si reemplazamos el concepto de «conjuntos con el mismo número (finito) de elementos» por el concepto más general de *conjuntos equivalentes*, se tiene que para conjuntos infinitos no es válida la proposición anterior; el conjunto de todos los enteros contiene más elementos que el conjunto de los números pares, y el conjunto de los números racionales más que el de enteros y, sin embargo, estos tres conjuntos son equivalentes. Esto podría hacer sospechar que *todos* los conjuntos infinitos fueran equivalentes y que toda otra distinción que la de conjuntos finitos e infinitos resultaría superflua; pero hemos visto que los resultados de Cantor contradicen tal sospecha; existe un conjunto, el continuo numérico real, que no es equivalente a ningún conjunto numerable.

Así resulta que hay al menos dos tipos diferentes de «infinitud»: el infinito numerable de los enteros y el infinito no-numerable del continuo. Si dos conjuntos, finitos o infinitos, son equivalentes, diremos que tienen el *mismo número cardinal.* Esta propiedad se reduce a la noción ordinaria de *igual número natural* si A y B son finitos, y puede considerarse como una generalización de este concepto. Por otra parte, si un conjunto A es equivalente con algún subconjunto de B, mientras que B no es equivalente con A ni con ninguno de sus subconjuntos, diremos, siguiendo a Cantor, que el conjunto B tiene un *número cardinal mayor* que el del conjunto A. El uso de la palabra «número» está también en este caso de acuerdo con la noción de «número mayor» para conjuntos finitos. El conjunto de los enteros es un subconjunto del conjunto de los números reales, mientras que el conjunto de los números reales no es equivalente con el de los enteros ni con ninguno de los subconjuntos de éste (es decir, el conjunto de los números reales no es numerable ni finito); por tanto, de acuerdo con nuestra definición, el continuo de los números reales tiene un número cardinal mayor que el conjunto de los enteros.

*Se debe indicar que Cantor demostró realmente cómo construir una sucesión de conjuntos infinitos de números cardinales crecientes. Partiendo de los números enteros positivos, es suficiente probar que *dado un conjunto* A *cualquiera, es posible construir otro conjunto* B *de mayor número cardinal que aquél.* A causa de la gran generalidad de este teorema su demostración resulta bastante abstracta. Definimos el conjunto B como el conjunto de todos los distintos subconjuntos de A. En el término «subconjunto» debemos incluir no solamente los subconjuntos propios de A, sino también A mismo y el «subconjunto vacío», 0, que no contiene ningún elemento. (Así, en el caso en que A esté formado por los enteros 1, 2, 3, B consta de los 8 elementos diferentes $\{1, 2, 3\}$, $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$, $\{1\}$, $\{2\}$, $\{3\}$ y 0.) Los elementos de B son a su vez *conjuntos* formados por elementos de A. Supongamos que B es equivalente a A o a algún subconjunto de A; es decir, que existe una ley que coordina de manera biunívoca los elementos de A o de uno de sus subconjuntos con todos los elementos de B; esto es, con los subconjuntos de A:

$$a \longleftrightarrow S_a, \qquad [2]$$

donde designamos con S_a el subconjunto de A que corresponde al elemento a de A. Llegaremos a una contradicción construyendo un elemento de B (es decir, un subconjunto de A) al que no le corresponde ningún elemento a de A. En la construcción de este subconjunto se observa que existen dos posibilidades para todo elemento x de A: o bien el conjunto S_x asignado a x por la correspondencia [2] contiene al elemento x, o S_x no contiene a x. *Definamos* T *como el subconjunto de* A *formado por los elementos* x *tales que* S_x *no contiene* a x. Este subconjunto T difiere de cualquier S_a al menos en el elemento a, puesto que si S_a contiene a a, T no debe contenerlo, mientras que si S_a no contiene a a, T debe contenerlo. En consecuencia, T no está incluído en la correspondencia [2]. Esto prueba que no se puede establecer una correspondencia biunívoca entre los elementos de A, o de un subconjunto de A, y los de B. Sin embargo, la coordinación

$$a \longleftrightarrow \{a\}$$

define una correspondencia biunívoca entre los elementos de A y el subconjunto de B formado por los subconjuntos de A que constan de un solo elemento. En consecuencia, de acuerdo con la definición del último párrafo, B tiene un número cardinal mayor que el de A.

***Ejercicio:** Si A contiene n elementos, siendo n un entero positivo, pruébese que B, tal como ha sido definido antes, contiene 2^n elementos. Si A es el conjunto de todos los enteros positivos, demuéstrese que B es equivalente al continuo numérico entre 0 y 1. (*Indicación:* Represéntese todo subconjunto de A en el primer caso por una sucesión finita y en el segundo por una sucesión infinita de las cifras 0 y 1,

$$a_1a_2a_3\cdots$$

siendo $a_n = 1$ ó 0, según que el n-ésimo elemento de A pertenezca o no al subconjunto en cuestión.)

Podría pensarse que es fácil encontrar un conjunto de *puntos* con número cardinal mayor que el conjunto de los números reales entre 0 y 1. Puesto que, a primera vista, un cuadrado, siendo de «dimensión 2», parece contener «más» puntos que un segmento «unidimensional». Paradójicamente, las cosas no ocurren de ese modo: *el número cardinal del conjunto de puntos de un cuadrado es el mismo que el del conjunto de puntos de un segmento.* Para probar esta afirmación, estableceremos la correspondencia siguiente:

Si (x, y) es un punto de un cuadrado de lado unidad, x e y pueden ser escritos en forma decimal

$$x = 0{,}a_1a_2a_3a_4\cdots,$$
$$y = 0{,}b_1b_2b_3b_4\cdots,$$

donde para evitar ambigüedades escribiremos, p. ej., 0,250000... en vez de 0,249999··· para el número racional 1/4. Al punto (x, y) del cuadrado le hacemos corresponder el punto

$$z = 0{,}a_1b_1a_2b_2a_3b_3a_4b_4\cdots$$

del segmento entre 0 y 1. Evidentemente, a puntos distintos (x, y) y (x', y') del cuadrado les corresponderán puntos distintos z y z' del segmento, de modo que el número cardinal del cuadrado no puede exceder del cardinal del segmento.

(En realidad, la correspondencia que acabamos de establecer es biunívoca entre el conjunto de todos los puntos del cuadrado y un subconjunto propio del segmento unidad; puesto que ningún punto del cuadrado corresponde al punto 0,21409090909··· del segmento, ya que, como hemos indicado, tomamos la forma 0,250000··· y no la 0,2499999··· para representar el número 1/4. Sin embargo, es posible modificar un poco la correspondencia, de modo que se tenga la biunivocidad entre el cuadrado y el segmento, los cuales resultan así con el mismo número cardinal.)

Un razonamiento análogo al anterior mostraría que el número cardinal de los puntos de un cubo es igual al número cardinal del segmento unidad.

Aunque estos resultados parecen contradecir la noción intuitiva de dimensión, debemos recordar que la correspondencia que hemos definido no es «continua»; si recorremos el segmento de 0 a 1 de modo continuo, los puntos correspondientes del cuadrado no forman una curva continua, sino que aparecen en un orden completamente caótico. La dimensión de un conjunto de puntos depende, no solamente del número cardinal del conjunto, sino también del modo como los puntos aparecen distribuídos en el espacio. En el capítulo V volveremos a ocuparnos de esta cuestión.

4. El método de demostración indirecta (demostraciones por reducción al absurdo).—La teoría de los números cardinales no es más que un aspecto de la teoría general de conjuntos, creada por Cantor en lucha con las severas críticas de algunos de los más distinguidos matemáticos de su tiempo. Algunos de estos críticos, tales como Kronecker y Poincaré, le reprochaban la vaguedad del concepto general de «conjunto» y el carácter no constructivo de los razonamientos utilizados para definir algunos conjuntos.

Las objeciones a los razonamientos no constructivos se refieren a las que podemos llamar *pruebas indirectas* o *demostraciones por reducción al absurdo.* Las demostraciones indirectas constituyen un tipo habitual de razonamiento matemático: para establecer la verdad de una proposición A, se hace la hipótesis de que la proposición A', contraria de la A, es cierta. Entonces, mediante una cadena de razonamientos, se llega a una contradicción con A', lo que prueba lo absurdo de A'. En consecuencia, apoyándose en el principio lógico fundamental del *tertio excluso,* la falsedad de A' establece la verdad de A.

A lo largo de este libro encontraremos ejemplos de demostraciones indirectas que pueden convertirse en demostraciones directas, si bien la forma indirecta presenta las ventajas de la brevedad y de prescindir de detalles que no son necesarios para el objetivo inmediato. Existen, sin embargo, teoremas para los cuales no ha sido posible dar más demostración que la indirecta; aún más: hay teoremas que se pueden demostrar por el método indirecto, para los cuales no sería posible ni siquiera en principio dar una demostración directa constructiva, a causa de la naturaleza misma del teorema. Tal es, p. ej., el teorema dado en la página 90. En distintas ocasiones de la historia de las matemáticas, en las que los esfuerzos de los matemáticos se dirigían hacia la obtención de soluciones *constructivas* para determinados problemas, con vistas a mostrar la posibilidad de solución, se llegó a la construcción gracias a haberse encontrado una demostración indirecta y no constructiva.

Existe una diferencia esencial entre probar la existencia de un objeto de cierto tipo mediante la construcción de un ejemplo tangible de tal objeto y demostrar que la no existencia de dicho objeto conduciría a una contradicción. En el primer caso se tiene un objeto tangible, mientras que en el segundo no se tiene más que una contradicción. Algunos matemáticos destacados han propugnado en tiempos recientes la supresión más o menos completa de las demostraciones no constructivas de la matemática. Aun en el caso en que se considere deseable este programa, en el estado actual de la matemática supondría una gran complicación y también la parcial destrucción del edificio matemático actual. Por esta razón no es de extrañar que la escuela «intuicionista», que es la que ha adoptado tal programa, haya encontrado fuerte resistencia, y que los intuicionistas más puros no puedan en ocasiones permanecer fieles a sus principios.

5. Las paradojas del infinito.—Aunque la posición irreducible de los intuicionistas parece demasiado extremista a la mayor parte de los matemáticos, la aparición de paradojas lógicas en la teoría de los conjuntos infinitos representó una seria amenaza para dicha teoría. Pronto se observó que la utilización sin restricciones del concepto de «conjunto» podía conducir a contradicciones. Una de las paradojas, presentada por Bertrand Russell, puede ser formulada como sigue: la mayor parte de los conjuntos no se contienen a sí mismos como elementos; p. ej., el conjunto A de los números enteros contiene como elementos únicamente números enteros; como A no es un entero, sino un *conjunto de enteros*, no se contiene a sí mismo como elemento. Un conjunto de este tipo se llamará «ordinario». Sin embargo, es posible que un conjunto se contenga a sí mismo como elemento; p. ej., el conjunto S, definido por la frase «S contiene como elementos los conjuntos que se pueden definir en castellano con una frase de menos de treinta palabras», es un conjunto que se contiene a sí mismo como elemento. A estos conjuntos los llamaremos «extraordinarios». En todo caso, la mayor parte de los conjuntos son ordinarios y podemos excluir el comportamiento extraño de los conjuntos «extraordinarios», limitando nuestra atención al *conjunto de todos los conjuntos ordinarios*. Llamemos C a dicho conjunto. Cualquier elemento de C es a su vez un conjunto; en realidad un conjunto ordinario. Ahora se plantea la cuestión de saber si el conjunto C es ordinario o extraordinario. Debe ser de uno o del otro tipo; si C es ordinario, debe contenerse a sí mismo como elemento, puesto que hemos definido C por la propiedad de contener a *todos* los conjuntos ordinarios; pero si es así, C debe ser extraordinario, ya que hemos llamado extraordinarios a los conjuntos que se contienen a sí mismos como elementos. Se tiene en consecuencia una contradicción; por tanto, C debe ser extraordinario. Pero entonces C, que se contiene a sí mismo por ser extraordinario, contendrá un conjunto extraordinario (el mismo C), en contradicción con la definición que dimos de C como conjunto que contiene únicamente conjuntos ordinarios. Vemos así que, en cualquiera de las dos hipótesis, la mera existencia de C conduce a una contradicción.

6. Los fundamentos de la matemática.—Paradojas análogas a la precedente condujeron a Russell y a otros matemáticos a un estudio sistemático de los fundamentos de la matemática y de la lógica. El objeto final de sus esfuerzos es el de dar al razonamiento matemático una base lógica, la cual se pueda probar que está libre de contradicción, y que al mismo tiempo incluya todo lo que es considerado como importante por todos (o algunos de) los matemáticos. Aunque esta meta ambiciosa no ha sido alcanzada y quizá no pueda ser alcanzada nunca, el tema de la lógica matemática ha atraído la atención de un número creciente de estudiosos. Muchas de las cuestiones en este dominio que pueden ser enunciadas en forma simple presentan grandes dificultades para su solución. Como ejemplo, citaremos la llamada *hipótesis del continuo*, que supone la no existencia de ningún conjunto cuyo número cardinal sea mayor que el de los conjuntos numerables y menor que el del continuo numérico correspondiente al conjunto de los números reales. De esta hipótesis pueden deducirse muchas consecuencias interesantes; pero hasta ahora no ha sido demostrada ni refutada, si bien recientemente Kurt Gödel ha probado que si el sistema de postulados sobre los que se funda la teoría de conjuntos no es contradictorio, tampoco lo es el sistema ampliado obtenido al añadir la hipótesis del continuo. Cuestiones tales como éstas se reducen en última instancia a saber lo que se quiere significar por el concepto de *existencia matemática*. Afortunadamente, la existencia de la matemática no depende de una respuesta satisfactoria. La escuela de los «formalistas», dirigida por el gran matemático Hilbert, afirma que, en matemática, «existencia» significa simplemente «libre de contradicción». Resulta entonces necesario construir un sistema de postulados del que pueda deducirse toda la matemática por razonamiento puramente formal, y demostrar que este sistema de postulados no puede llevar nunca a contradicción. Los resultados recientes obtenidos por Gödel y otros parecen probar que este programa, al menos como fué concebido originalmente por Hilbert, no puede realizarse. Es significativo que la teoría de Hilbert acerca de la estructura formal de las matemáticas esté basada en esencia en un proceso intuitivo. De una forma u otra, explícita o implícitamente, aun bajo el más inflexible aspecto formalista, lógico o postulatorio, la intuición constructiva continúa siendo el elemento vital en matemáticas.

V. NÚMEROS COMPLEJOS

1. Origen de los números complejos.—Por muchas razones el concepto de número ha tenido que ser extendido más allá del continuo numérico real mediante la introducción de los llamados *números complejos*. Debe observarse que en el desarrollo histórico y psicológico de las matemáticas, todas estas generalizaciones y nuevas invenciones no han sido en forma alguna resultado de algún esfuerzo individual, sino que más bien aparecen como el desenlace de una evolución gradual y cautelosa que no puede atribuirse a una sola persona determinada. Fué la necesidad de una mayor libertad en el cálculo formal lo que llevó a la utilización de los números racionales negativos, y sólo al final de la Edad Media empezaron los matemáticos a perder el temor de usar estos conceptos que no tenían el mismo carácter concreto e intuitivo de los números naturales. Hasta la mitad del siglo XIX los matemáticos no percibieron de una forma completamente clara que la base esencial lógico-filosófica de las operaciones en un conjunto numérico ampliado es formalista, y que las ampliaciones han de hacerse mediante definiciones que, como tales, son libres, pero resultan inútiles si no son hechas de manera que las leyes y propiedades válidas en el campo numérico original se conserven al ampliar éste. El hecho de que estas ampliaciones puedan estar a veces relacionadas con objetos «reales», y que de esta forma procuren una herramienta para nuevas aplicaciones, es de la mayor importancia, si bien esto es sólo una justificación, pero no constituye una prueba lógica de la validez de la ampliación.

El primer problema que requiere el uso de los números complejos es el de la *resolución de las ecuaciones cuadráticas*. Recordemos el concepto de ecuación lineal $ax = b$, en la cual hay que determinar la incógnita x. La solución es simplemente $x = \frac{b}{a}$, y la exigencia de que toda ecuación de coeficientes enteros $a \neq 0$ y b tenga solución, precisa de la introducción de los números racionales. Ecuaciones tales como

$$x^2 = 2, \tag{1}$$

que carecen de solución en el campo de los números racionales, nos llevan a construir el campo más amplio de los números reales, en el cual existe solución. Pero incluso el campo de los números reales no es suficientemente amplio para procurarnos una teoría completa de las ecuaciones cuadráticas. Una ecuación sencilla tal como

$$x^2 = -1 \tag{2}$$

carece de solución real, pues el cuadrado de cualquier número real no es nunca negativo.

Podemos contentarnos con la afirmación de que esta sencilla ecuación no es resoluble, o bien seguir el camino usual de extender nuestro concepto de número mediante la introducción de números que permitan resolver la ecuación. Exactamente esto es lo que se hace al introducir el nuevo símbolo i por la definición $i^2 = -1$. Naturalmente, este objeto i, la «unidad imaginaria», no tiene nada que ver con el concepto de número tal como resulta de la operación de *contar*. Es puramente un *símbolo*, sometido a la regla fundamental $i^2 = -1$, y su valor dependerá por completo de si mediante su introducción se ha conseguido una extensión del sistema numérico que resulte útil y manejable.

Puesto que deseamos sumar y multiplicar con el símbolo i en igual forma que con los números reales ordinarios, deberemos ser capaces de formar símbolos tales como $2i$, $3i$, $-i$, $2 + 5i$ o, más en general, $a + bi$, donde a y b son dos números reales cualesquiera. Si estos símbolos han de obedecer a las familiares leyes conmutativa, asociativa y distributiva de la suma y del producto, se tendrá, p. ej.,

$$\begin{aligned}(2 + 3i) + (1 + 4i) &= (2 + 1) + (3 + 4)i = 3 + 7i,\\ (2 + 3i)(1 + 4i) &= 2 + 8i + 3i + 12i^2 =\\ &= (2 - 12) + (8 + 3)i = -10 + 11i.\end{aligned}$$

Guiados por estas consideraciones, comenzamos nuestra exposición sistemática haciendo la siguiente *definición*: llamaremos *número complejo de parte real* a y *parte imaginaria* b a un símbolo de la forma $a + bi$, donde a y b representan dos números reales cualesquiera. Con estos símbolos pueden realizarse las operaciones de adición y multiplicación en igual forma que si i fuera un número real ordinario, salvo que i^2 debe ser sustituído siempre por -1; con mayor precisión, definimos la adición y multiplicación de números complejos mediante las reglas

$$\begin{aligned}(a + bi) + (c + di) &= (a + c) + (b + d)i,\\ (a + bi)(c + di) &= (ac - bd) + (ad + bc)i.\end{aligned} \qquad [3]$$

En particular, se tiene:

$$(a + bi)(a - bi) = a^2 - abi + abi - b^2i^2 = a^2 + b^2. \qquad [4]$$

Mediante estas definiciones se comprueba fácilmente que subsisten para los números complejos las leyes conmutativa, asociativa y distributiva. Además, no solamente la adición y multiplicación, sino también la sustracción y división de dos números complejos, dan lugar a números de la forma $a + bi$, de modo que los números complejos forman un *cuerpo* (véase pág. 64).

$$(a + bi) - (c + di) = (a - c) + (b - d)i,$$

$$\frac{a + bi}{c + di} = \frac{(a + bi)}{(c + di)} \frac{(c - di)}{(c - di)} = \left(\frac{ac + bd}{c^2 + d^2}\right) + \left(\frac{bc - ad}{c^2 + d^2}\right) i. \qquad [5]$$

(La segunda ecuación carece de significado cuando $c + di = 0 + 0i$, pues en este caso $c^2 + d^2 = 0$. Así que de nuevo *debemos excluir la división por cero*; es decir, por $0 + 0i$.) P. ej.:

$$(2 + 3i) - (1 + 4i) = 1 - i,$$

$$\frac{2 + 3i}{1 + 4i} = \frac{2 + 3i}{1 + 4i} \cdot \frac{1 - 4i}{1 - 4i} = \frac{2 - 8i + 3i + 12}{1 + 16} = \frac{14}{17} - \frac{5}{17} i.$$

El cuerpo de los números complejos incluye el cuerpo de los números reales como un subcuerpo de él, pues el número complejo $a + 0i$ puede considerarse igual al número real a. Por otra parte, un número complejo de la forma $0 + bi$ se llama imaginario puro.

Ejercicios:

1. Exprésese $\dfrac{(1 + i)(2 + i)(3 + i)}{(1 - i)}$ en la forma $a + bi$.

2. Exprésese $\left(-\dfrac{1}{2} + i\dfrac{\sqrt{3}}{2}\right)^3$ en la forma $a + bi$.

3. Exprésense en la forma $a + bi$:

$$\frac{1 + i}{1 - i}, \quad \frac{1 + i}{2 - i}, \quad \frac{1}{i^5}, \quad \frac{1}{(-2 + i)(1 - 3i)}, \quad \frac{(4 - 5i)^2}{(2 - 3i)^2}$$

4. Calcúlese $\sqrt{5 + 12i}$. (*Indicación:* Escríbase $\sqrt{5 + 12i} = x + yi$, elévese al cuadrado e iguálense partes reales e imaginarias.)

Mediante la introducción del símbolo i hemos extendido el cuerpo de los números reales al cuerpo de los símbolos $a + bi$, en el cual la ecuación cuadrática especial

$$x^2 = -1$$

tiene las dos soluciones $x = i$ y $x = -i$. En efecto, por definición, $i \cdot i = (-i)(-i) = i^2 = -1$. En realidad, hemos conseguido mucho más, pues es fácil comprobar que ahora *toda ecuación cuadrática*, que podemos escribir en la forma

$$ax^2 + bx + c = 0, \qquad [6]$$

tiene solución. En efecto, de [6] resulta

$$x^2 + \frac{b}{a}x = -\frac{c}{a},$$

$$x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} = \frac{b^2}{4a^2} - \frac{c}{a},$$

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2},$$

$$x + \frac{b}{2a} = \frac{\pm\sqrt{b^2 - 4ac}}{2a},$$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \qquad [7]$$

Ahora bien: si $b^2 - 4ac \geqslant 0$, $\sqrt{b^2 - 4ac}$ es un número real ordinario y las soluciones [7] son reales, mientras que si $b^2 - 4ac < 0$, entonces $4ac - b^2 > 0$ y $\sqrt{b^2 - 4ac} = \sqrt{-(4ac - b^2)} = i\sqrt{4ac - b^2}$, de forma que las soluciones [7] son números complejos; p. ej., las soluciones de la ecuación

$$x^2 - 5x + 6 = 0,$$

son $x = (5 \pm \sqrt{25 - 24})/2 = (5 \pm 1)/2 = 2$ y 3; en tanto que las soluciones de la ecuación

$$x^2 - 2x + 2 = 0,$$

son $x = (2 \pm \sqrt{4 - 8})/2 = (2 \pm 2i)/2 = 1 + i$ y $1 - i$.

2. Interpretación geométrica de los números complejos.—Ya en el siglo XVI los matemáticos se vieron obligados a introducir símbolos para representar las raíces cuadradas de los números negativos y poder resolver todas las ecuaciones cuadráticas y cúbicas. Sin embargo, no fueron capaces de explicar el significado exacto de estos símbolos, que eran considerados con cierto temor supersticioso. El nombre de «imaginarios» es todavía un vestigio del hecho de que estas expresiones fueran consideradas como algo ficticio e irreal. Por fin, a principios del siglo XIX, al ponerse de manifiesto la importancia de estos números en muchas ramas de las matemáticas, una sencilla interpretación geométrica de las operaciones con los números complejos fué suficiente para hacer desaparecer las dudas acerca de su validez. Por supuesto que tal interpretación es innecesaria desde el punto de vista moderno, de acuerdo con el cual la justificación del cálculo formal con los números complejos está basada directamente sobre las definiciones formales de adición y multiplicación. Pero la interpretación geométrica, que fué dada casi al mismo tiempo por Wessel (1745-1818), Argand (1768-1822) y Gauss, hizo que estas operaciones resultaran más naturales desde un punto de vista intuitivo, habiendo resultado, por otra parte, de la mayor importancia en las aplicaciones de los números complejos a la matemática y a las ciencias físicas.

Esta interpretación geométrica consiste simplemente en representar el número complejo $z = x + yi$ por el punto del plano de coordenadas rectangulares x, y. Así, la parte real de z es su coordenada x, y la parte imaginaria su coordenada y. Con ello queda establecida una correspondencia entre los números complejos y los puntos del «plano numérico», en forma análoga a la correspondencia establecida en II entre los números reales y los puntos de una recta, la recta numérica. Los puntos del eje x del plano numérico corresponden a los números reales $z = x + 0i$, mientras los puntos del eje y corresponden a los números imaginarios puros $z = 0 + yi$.

Si

$$z = x + yi$$

es un número complejo cualquiera, al número complejo

$$\bar{z} = x - yi$$

lo llamaremos *conjugado* de $\bar{z}$. El punto $\bar{z}$ se representa en el plano numérico por el simétrico del punto z respecto al eje x. Si designamos la distancia desde el origen al punto z por ρ, entonces, por el teorema de Pitágoras

$$\rho^2 = x^2 + y^2 = (x + yi)(x - yi) = z \cdot \bar{z}.$$

El número real $\rho = \sqrt{x^2 + y^2}$ se llama *módulo* de z, y se escribe

$$\rho = |z|.$$

Si z está sobre el eje real, su módulo es su valor absoluto ordinario. Los números complejos de módulo 1 están sobre la «circunferencia unidad», con centro en el origen y radio 1.

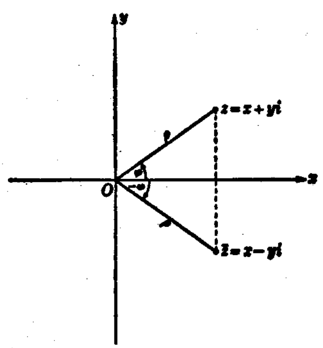


FIG. 22.—Representación geométrica de los números complejos. El punto z tiene como coordenadas rectangulares x e y.

Si $|z| = 0$ *entonces* $z = 0$. Esto resulta de la definición de $|z|$ como distancia de z al origen. Además, *el módulo del producto de dos* *números complejos es igual al producto de sus módulos:*

$$|z_1 \cdot z_2| = |z_1| \cdot |z_2|.$$

Esta propiedad resulta de un teorema más general que será demostrado en la página 105.

Ejercicios:

1. Demuéstrese este teorema basándose directamente en la definición de producto de dos números complejos $z_1 = x_1 + y_1 i$ y $z_2 = x_2 + y_2 i$.

2. Basándose en el hecho de que el producto de dos números *reales* únicamente es 0 si uno de los factores es 0, demuéstrese el teorema correspondiente para los números *complejos*. (Hágase uso de los dos teoremas que se acaban de enunciar.)

De la definición de suma de dos números complejos, $z_1 = x_1 + y_1 i$ y $z_2 = x_2 + y_2 i$, se tiene

$$z_1 + z_2 = (x_1 + x_2) + (y_1 + y_2)i.$$

Por tanto, el punto $z_1 + z_2$ está representado en el plano numérico por el cuarto vértice de un paralelogramo cuyos otros tres vértices son los puntos 0, z_1, z_2. Esta sencilla construcción geométrica de la suma de dos números complejos es de gran importancia en muchas aplicaciones; de ella puede deducirse la consecuencia importante de que *el módulo de la suma de dos números complejos no excede nunca a la suma de los módulos* (véase la pág. 66):

$$|z_1 + z_2| \leq |z_1| + |z_2|.$$

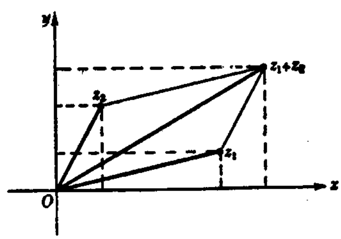


FIG. 23.—Construcción geométrica de la suma de dos números complejos.

Esta propiedad resulta del hecho de ser la longitud de un lado cualquiera de un triángulo menor que la suma de las longitudes de los otros dos.

Ejercicio: ¿En qué caso tiene lugar la igualdad $|z_1 + z_2| = |z_1| + |z_2|$?

El ángulo formado por la dirección positiva del eje x y la recta Oz se llama *argumento* de z, y se representa por φ (Fig. 22). El módulo de $\bar{z}$ es el mismo que el de z

$$|\bar{z}| = |z|,$$

pero el argumento de $\bar{z}$ es opuesto al de z; esto es,

$$\bar{\varphi} = -\varphi.$$

Naturalmente, el argumento de z no está determinado unívocamente, ya que puede sumarse o restarse a un ángulo cualquier múltiplo entero de 360°, sin que esto afecte a la posición gráfica de sus lados. Así, p. ej.,

$$\varphi,\ \varphi + 360^\circ,\ \varphi + 720^\circ,\ \varphi + 1080^\circ, \cdots,$$
$$\varphi - 360^\circ,\ \varphi - 720^\circ,\ \varphi - 1080^\circ, \cdots$$

representan todos gráficamente el mismo ángulo. Utilizando el módulo ρ y el argumento φ, el número complejo z puede escribirse en la forma

$$z = x + yi = \rho(\cos\varphi + i \operatorname{sen}\varphi); \qquad [8]$$

en efecto, por definición de seno y coseno (véase Cap. VI, I, 2),

$$x = \rho \cos\varphi, \qquad y = \rho \operatorname{sen}\varphi.$$

Por ejemplo, para $z = i$, $\rho = 1$, $\varphi = 90^\circ$, de manera que $i = 1\,(\cos 90^\circ + i \operatorname{sen} 90^\circ)$;

para $z = 1 + i$, $\rho = \sqrt{2}$, $\varphi = 45^\circ$, de modo que
$$1 + i = \sqrt{2}\,(\cos 45^\circ + i \operatorname{sen} 45^\circ);$$
para $z = 1 - i$, $\rho = \sqrt{2}$, $\varphi = -45^\circ$, de modo que
$$1 - i = \sqrt{2}\,[\cos(-45^\circ) + i \operatorname{sen}(-45^\circ)];$$
para $z = -1 + \sqrt{3}\,i$, $\rho = 2$, $\varphi = 120^\circ$, de forma que
$$-1 + \sqrt{3}\,i = 2\,(\cos 120^\circ + i \operatorname{sen} 120^\circ).$$

El lector puede comprobar estas igualdades por sustitución de los valores de las funciones trigonométricas.

La representación trigonométrica [8] es de gran interés en el caso de la multiplicación de números complejos. Pues si

$$z = \rho(\cos\varphi + i \operatorname{sen}\varphi),$$

y

$$z' = \rho'(\cos\varphi' + i \operatorname{sen}\varphi'),$$

se tiene

$$zz' = \rho\rho'\{(\cos\varphi\cos\varphi' - \operatorname{sen}\varphi\operatorname{sen}\varphi') + i(\cos\varphi\operatorname{sen}\varphi' + \operatorname{sen}\varphi\cos\varphi')\}$$

Ahora bien: por los teoremas de adición del seno y del coseno,

$$\cos\varphi\cos\varphi' - \operatorname{sen}\varphi\operatorname{sen}\varphi' = \cos(\varphi + \varphi'),$$
$$\cos\varphi\operatorname{sen}\varphi' + \operatorname{sen}\varphi\cos\varphi' = \operatorname{sen}(\varphi + \varphi').$$

Por consiguiente,

$$zz' = \rho\rho'\{\cos(\varphi + \varphi') + i \operatorname{sen}(\varphi + \varphi')\}. \qquad [9]$$

Esta es la forma trigonométrica del número complejo de módulo $\rho\rho'$ y argumento $\varphi + \varphi'$. En otras palabras, *para multiplicar dos números complejos se multiplican sus módulos y se suman sus argumentos* (figura 24). Vemos así que la multiplicación de números complejos está relacionada con la operación geométrica de *rotación*. Con más precisión, denominemos al segmento dirigido que une el origen con el punto z *vector* z; la longitud de éste será $\rho = |z|$. Sea z' un número sobre la circunferencia unidad, es decir, $\rho' = 1$; entonces, al multiplicar z por z' el vector z gira un ángulo igual a φ'. Si $\rho' \neq 1$, la longitud del vector ha de ser multiplicada por ρ' una vez efectuada la rotación. El lector puede comprobar gráficamente estos hechos, haciendo el producto de varios números por $z_1 = i$ (giro de 90°); $z_2 = -i$ (giro de 90° en sentido opuesto); $z_3 = 1 + i$, y $z_4 = 1 - i$.

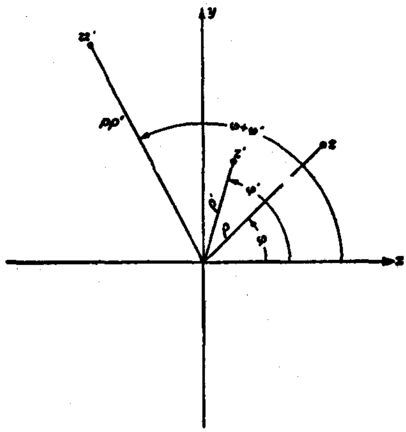


FIG. 24.—Multiplicación de dos números complejos; los argumentos se suman y los módulos se multiplican.

La fórmula [9] tiene una consecuencia particularmente importante cuando $z = z'$, pues en este caso resulta

$$z^2 = \rho^2(\cos 2\varphi + i \operatorname{sen} 2\varphi).$$

Al multiplicar de nuevo por z obtenemos

$$z^3 = \rho^3(\cos 3\varphi + i \operatorname{sen} 3\varphi),$$

y si se continúa indefinidamente en esta forma,

$$z^n = \rho^n(\cos n\varphi + i \operatorname{sen} n\varphi) \qquad \text{para cualquier entero } n. \qquad [10]$$

En particular, si z es un punto de la *circunferencia unidad*, $\rho = 1$, obtenemos la fórmula dada a conocer por el matemático inglés A. De Moivre (1667-1754):

$$(\cos \varphi + i \operatorname{sen} \varphi)^n = \cos n\varphi + i \operatorname{sen} n\varphi. \qquad [11]$$

Esta fórmula es una de las más notables y útiles de las matemáticas elementales, según vamos a poner de manifiesto con un ejemplo.

Si aplicamos la fórmula para $n = 3$ y desarrollamos el primer miembro por la fórmula del binomio

$$(u + v)^3 = u^3 + 3u^2v + 3uv^2 + v^3.$$

se obtiene la relación

$$\cos 3\varphi + i \operatorname{sen} 3\varphi = \cos^3 \varphi - 3 \cos \varphi \operatorname{sen}^2 \varphi + i(3 \cos^2 \varphi \operatorname{sen} \varphi - \operatorname{sen}^3 \varphi).$$

Una sola ecuación, tal como ésta, *entre dos números complejos equivale a un par de ecuaciones entre números reales*, pues la igualdad de dos números complejos exige la igualdad de sus partes reales e imaginarias, respectivamente. En consecuencia podemos escribir

$$\cos 3\varphi = \cos^3 \varphi - 3 \cos \varphi \operatorname{sen}^2 \varphi, \qquad \operatorname{sen} 3\varphi = 3 \cos^2 \varphi \operatorname{sen} \varphi - \operatorname{sen}^3 \varphi.$$

Si utilizamos la igualdad

$$\cos^2 \varphi + \operatorname{sen}^2 \varphi = 1,$$

se obtiene finalmente

$$\begin{aligned} \cos 3\varphi &= \cos^3 \varphi - 3 \cos \varphi(1 - \cos^2 \varphi) = 4 \cos^3 \varphi - 3 \cos \varphi, \\ \operatorname{sen} 3\varphi &= -4 \operatorname{sen}^3 \varphi + 3 \operatorname{sen} \varphi. \end{aligned}$$

Fácilmente pueden obtenerse fórmulas análogas para cualquier valor entero n que expresen $\operatorname{sen} n\varphi$ y $\cos n\varphi$ en función de las potencias de $\operatorname{sen} \varphi$ y $\cos \varphi$, respectivamente.

Ejercicios:

1. Hállense las fórmulas correspondientes para $\operatorname{sen} 4\varphi$ y $\cos 4\varphi$.
2. Demuéstrese que para un punto, $z = \cos \varphi + i \operatorname{sen} \varphi$, de la circunferencia unidad, $1/z = \cos \varphi - i \operatorname{sen} \varphi$.
3. Pruébese, sin efectuar cálculos, que $(a + bi)/(a - bi)$ tiene siempre módulo 1.
4. Si z_1 y z_2 son dos números complejos, demuéstrese que el argumento de $z_1 - z_2$ es igual al ángulo formado por el eje real y el vector dirigido de z_2 a z_1.
5. Interprétese el argumento del número complejo $(z_1 - z_2)/(z_1 - z_3)$ en el triángulo formado por los puntos z_1, z_2 y z_3.
6. Demuéstrese que el cociente de dos números complejos del mismo argumento es real.
7. Demuéstrese que si dados cuatro números complejos z_1, z_2, z_3, z_4, los argumentos de $(z_3 - z_1)/(z_3 - z_2)$ y $(z_4 - z_1)/(z_4 - z_2)$ son iguales, los cuatro puntos están sobre una circunferencia o una recta, y recíprocamente.
8. Demuéstrese que la condición necesaria y suficiente para que los cuatro puntos z_1, z_2, z_3, z_4 estén sobre una circunferencia o una recta es que sea real el cociente

$$\frac{z_3 - z_1}{z_3 - z_2} \bigg/ \frac{z_4 - z_1}{z_4 - z_2}$$

3. Fórmula de De Moivre y raíces de la unidad.—Entendemos por raíz n-ésima de un número a aquel número b tal que $b^n = a$. En particular, el número 1 tiene dos raíces cuadradas, 1 y -1, pues $1^2 = (-1)^2 = 1$. El número 1 tiene una sola raíz cúbica real mientras que tiene cuatro raíces cuartas: los números reales 1 y -1 y los imaginarios i y $-i$. Estos hechos sugieren que debe haber otras dos raíces cúbicas de 1 en el campo complejo, haciendo un total de tres. Que efectivamente es así puede verse sin dificultad mediante la fórmula de De Moivre.

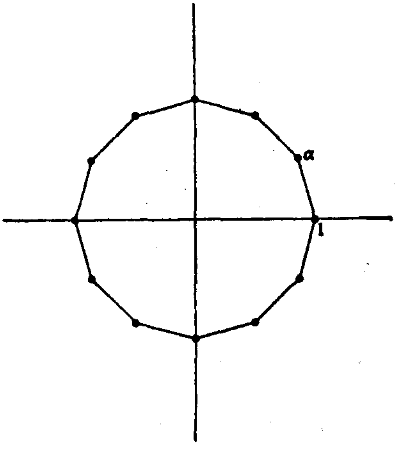


FIG. 25.—Representación geométrica de las raíces dozavas de la unidad.

Vamos a demostrar que *en el cuerpo de los números complejos hay exactamente* n *raíces* n*-ésimas diferentes de 1, las cuales están representadas por los vértices de un* n*-ágono regular inscrito en la circunferencia unidad, siendo uno de sus vértices el punto* z = 1. Esto resulta casi evidente de la figura 25 (dibujada para el caso $n = 12$). El primer vértice del polígono es 1, y el siguiente es

$$\alpha = \cos\frac{360^\circ}{n} + i \operatorname{sen}\frac{360^\circ}{n}, \qquad [12]$$

ya que su argumento debe ser la n-ésima parte del ángulo total de 360°. El vértice inmediato es $\alpha \cdot \alpha = \alpha^2$, pues se obtiene girando el vector α un ángulo de $\dfrac{360^\circ}{n}$. El vértice siguiente será α^3, etc., y, finalmente, después de reiterar n veces, volvemos nuevamente al vértice 1; esto es, se tiene

$$\alpha^n = 1,$$

lo que también resulta evidente de la fórmula [11], ya que

$$\left[\cos\frac{360^\circ}{n} + i \operatorname{sen}\frac{360^\circ}{n}\right]^n = \cos 360^\circ + i \operatorname{sen} 360^\circ = 1 + 0i.$$

Resulta que $\alpha^1 = \alpha$ es una raíz de la ecuación $x^n = 1$, y lo mismo

ocurre con el vértice inmediato $\alpha^2 = \cos\left(\frac{720^\circ}{n}\right) + i \operatorname{sen}\left(\frac{720^\circ}{n}\right)$
Esto se obtiene sin más que escribir

$$(\alpha^2)^n = \alpha^{2n} = (\alpha^n)^2 = (1)^2 = 1,$$

o, por la fórmula de De Moivre:

$$(\alpha^2)^n = \cos\left(n\frac{720^\circ}{n}\right) + i \operatorname{sen}\left(n\frac{720^\circ}{n}\right) = \cos 720^\circ + i \operatorname{sen} 720^\circ = 1 + 0i = 1.$$

De la misma manera veríamos que todos los n números

$$1,\ \alpha,\ \alpha^2,\ \alpha^3, \cdots, \alpha^{n-1}$$

son raíces n-ésimas de 1. Si seguimos adelante en la sucesión de exponentes o utilizamos exponentes negativos, no se obtienen nuevas raíces; en efecto, $\alpha^{-1} = 1/\alpha = \alpha^n/\alpha = \alpha^{n-1}$, y $\alpha^n = 1$, $\alpha^{n+1} = (\alpha)^n\,\alpha = 1 \cdot \alpha = \alpha$, etc., de forma que se repiten los valores anteriores. Se deja como ejercicio al lector el demostrar que no hay otras raíces n-ésimas.

Si n es par, uno de los vértices del n-ágono coincide con el punto -1, de acuerdo con el hecho algebraico de que en este caso -1 es una raíz n-ésima de 1.

La ecuación a la que satisfacen las raíces n-ésimas de la unidad

$$x^n - 1 = 0 \qquad [13]$$

es de grado n, pero puede reducirse fácilmente a una ecuación de grado $n - 1$, para lo cual basta hacer uso de la identidad algebraica

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + x^{n-3} + \cdots + 1). \qquad [14]$$

Dado que el producto de dos números es 0 si, *y sólo si*, uno al menos de los factores es 0, el primer miembro de [14] se anula sólo si uno de los dos factores del segundo miembro es cero, esto es, sólo si $x=1$, o bien

$$x^{n-1} + x^{n-2} + x^{n-3} + \cdots + x + 1 = 0. \qquad [15]$$

Por tanto, ésta es la ecuación a la que deben satisfacer las raíces α, $\alpha^2, \ldots, \alpha^{n-1}$, y recibe el nombre de *ecuación ciclotómica* (divisora de la circunferencia); p. ej., las raíces cúbicas imaginarias de 1,

$$\alpha = \cos 120^\circ + i \operatorname{sen} 120^\circ = {}^1/_2(-1 + i\sqrt{3}),$$
$$\alpha^2 = \cos 240^\circ + i \operatorname{sen} 240^\circ = {}^1/_2(-1 - i\sqrt{3}),$$

son las raíces de la ecuación

$$x^2 + x + 1 = 0,$$

como puede comprobar el lector por sustitución directa. Análogamente, las raíces quintas de 1, aparte la unidad, satisfacen a la ecuación

$$x^4 + x^3 + x^2 + x + 1 = 0. \qquad [16]$$

Para construir un pentágono regular debemos resolver esta ecuación de cuarto grado, la cual, por un simple artificio algebraico, se reduce a una ecuación cuadrática en $w = x + \frac{1}{x}$. Si dividimos [16] por x^2 y reagrupamos los términos:

$$x^2 + \frac{1}{x^2} + x + \frac{1}{x} + 1 = 0.$$

o bien, ya que $\left(x + \frac{1}{x}\right)^2 = x^2 + \frac{1}{x^2} + 2$, obtenemos la ecuación

$$w^2 + w - 1 = 0.$$

Mediante la fórmula [7] anterior, esta ecuación tiene las raíces

$$w_1 = \frac{-1 + \sqrt{5}}{2}, \qquad w_2 = \frac{-1 - \sqrt{5}}{2}$$

Por consiguiente, las raíces quintas de 1 son las correspondientes a dos ecuaciones cuadráticas

$$x + \frac{1}{x} = w_1, \quad \text{o} \quad x^2 + {}^1/_2(\sqrt{5} - 1)x + 1 = 0,$$

y

$$x + \frac{1}{x} = w_2, \quad \text{o} \quad x^2 - {}^1/_2(\sqrt{5} + 1)x + 1 = 0,$$

que el lector puede resolver por medio de la fórmula ya utilizada.

Ejercicios:

1. Hállense las raíces sextas de 1.
2. Calcúlese $(1 + i)^{11}$.
3. Hállense los diferentes valores de $\sqrt{1 + i}$, $\sqrt[3]{7 - 4i}$, $\sqrt[3]{i}$, $\sqrt[5]{-i}$.
4. Calcúlese $\frac{1}{2i}(i^7 - i^{-7})$.

***4. El teorema fundamental del álgebra.**—No sólo toda ecuación de la forma $ax^2 + bx + c = 0$ ó de la forma $x^n - 1 = 0$ es resoluble en el cuerpo de los números complejos, sino que se verifica en general que *toda ecuación algebraica de grado* n, *de coeficientes reales o complejos,*

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 = 0, \qquad [17]$$

tiene soluciones en el cuerpo de los números complejos. Este resultado fué establecido para las ecuaciones de tercero y cuarto grados en el siglo XVI por Tartaglia, Cardano y otros, que resolvieron dichas ecuaciones mediante fórmulas esencialmente análogas a la de la ecuación de segundo grado, si bien mucho más complicadas. Durante casi doscientos años se estudiaron con gran insistencia las ecuaciones de quinto grado y grados superiores; pero todos los esfuerzos para resolverlas por métodos similares fracasaron. Fué una gran hazaña del joven Gauss el dar la primera demostración completa en su tesis doctoral (1799) de la *existencia* de soluciones, aunque la cuestión de generalizar las fórmulas clásicas que expresan las soluciones de las ecuaciones de grado inferior al quinto mediante operaciones racionales y extracción de raíces quedó sin respuesta en su tiempo (véase pág. 128).

El teorema de Gauss dice que *para toda ecuación algebraica de la forma* [17], *donde* n *es un entero positivo y los coeficientes números reales cualesquiera o incluso números complejos, existe al menos un número complejo* $\alpha = c + di$ *tal que*

$$f(\alpha) = 0.$$

El número α se llama una *raíz* de la ecuación [17]. Daremos una demostración de este teorema en el Apéndice del capítulo V. Si de momento lo consideramos demostrado, podemos probar el llamado *teorema fundamental del álgebra* (con mayor propiedad debería llamarse teorema fundamental del sistema de los números complejos); esto es, *todo polinomio de grado* n

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0, \qquad [18]$$

puede descomponerse en el producto de exactamente n *factores*

$$f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n), \qquad [19]$$

siendo $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ *números complejos, raíces de la ecuación* $f(x) = 0$. Como ejemplo para aclarar este teorema, el polinomio

$$f(x) = x^4 - 1$$

puede escribirse en la forma

$$f(x) = (x - 1)(x - i)(x + i)(x + 1).$$

De la descomposición [19] resulta evidente que las α son raíces de la ecuación $f(x) = 0$, ya que para $x = \alpha_1$, un factor de $f(x)$, y en consecuencia $f(x)$ mismo, es igual a cero.

En algunos casos los factores $(x - \alpha_1)$, $(x - \alpha_2)$, ... de un polinomio $f(x)$ de grado n no son todos distintos, como se ve en el ejemplo

$$f(x) = x^2 - 2x + 1 = (x - 1)(x - 1),$$

que tiene sólo la raíz $x = 1$, «contada dos veces» o «con multiplicidad 2». En todo caso, un polinomio de grado n no puede tener más de n factores distintos $(x - \alpha)$, y la correspondiente ecuación, n raíces.

Para demostrar el teorema de la descomposición en factores, haremos uso de la identidad algebraica

$$x^k - \alpha^k = (x - \alpha)(x^{k-1} + \alpha x^{k-2} + \alpha^2 x^{k-3} + \cdots + \alpha^{k-2}x + \alpha^{k-1}), \quad [20]$$

que para $\alpha = 1$ se reduce a la fórmula de sumación de una progresión geométrica. Como hemos supuesto que se verifica el teorema de Gauss, podemos admitir que $\alpha = \alpha_1$ es una raíz de la ecuación [17], de modo que

$$f(\alpha_1) = \alpha_1^n + a_{n-1}\alpha_1^{n-1} + a_{n-2}\alpha_1^{n-2} + \cdots + a_1\alpha_1 + a_0 = 0.$$

Restando ésta de $f(x)$ y reagrupando los términos, obtenemos la identidad

$$f(x) = f(x) - f(\alpha_1) = (x^n - \alpha_1^n) + a_{n-1}(x^{n-1} - \alpha_1^{n-1}) + \cdots + a_1(x - \alpha_1). \quad [21]$$

Ahora bien: según [20], podemos sacar el factor $(x - \alpha_1)$ de cada término de [21], con lo cual el grado del otro factor de cada término se reduce en una unidad. Si de nuevo reagrupamos los términos, se obtiene

$$f(x) = (x - \alpha_1)g(x),$$

donde $g(x)$ es un polinomio de grado $n - 1$:

$$g(x) = x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1x + b_0 .$$

(Para nuestro objeto resulta innecesario calcular los coeficientes b_k.)

Ahora podemos aplicar el mismo procedimiento a $g(x)$; por el teorema de Gauss, existe una raíz α_2 de la ecuación $g(x) = 0$, de modo que

$$g(x) = (x - \alpha_2)h(x),$$

siendo $h(x)$ un polinomio de grado $n - 2$. Reiterando el mismo proceso un total de $(n - 1)$ veces (por supuesto que esta frase no es sino un equivalente del proceso de inducción matemática) obtenemos finalmente la descomposición completa en factores

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)\ldots(x - \alpha_n). \qquad [22]$$

De [22] resulta no sólo que los números complejos $\alpha_1, \alpha_2, \ldots, \alpha_n$ son raíces de la ecuación [17], sino también que son sus *únicas* raíces; pues si fuera y una raíz de la ecuación [17], por [22] se tendría

$$f(y) = (y - \alpha_1)(y - \alpha_2)\cdots(y - \alpha_n) = 0.$$

Hemos visto en la página 103 que un producto de números complejos se anula si, *y sólo si*, uno de los factores es igual a 0; en consecuencia, una de las diferencias $(y - \alpha_r)$ debe ser nula, e y igual a α_r, como queríamos demostrar.

*VI. NÚMEROS ALGEBRAICOS Y TRASCENDENTES

1. Definición y existencia.—Un *número algebraico* es cualquier número x, real o complejo, que satisface a una ecuación algebraica de la forma

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \qquad (n \geqslant 1,\ a_n \neq 0) \qquad [1]$$

donde los coeficientes a_k son *enteros*; p. ej., $\sqrt{2}$ es un número algebraico, pues satisface a la ecuación

$$x^2 - 2 = 0.$$

En forma análoga, toda raíz de una ecuación de coeficientes enteros de grados 3.º, 4.º, 5.º, o superior es un número algebraico, sean o no expresables dichas raíces mediante radicales. El concepto de número algebraico es una generalización natural del de número racional, que constituye el caso especial para $n = 1$.

Que no todo número real es algebraico puede probarse por un procedimiento debido a Cantor, consistente en demostrar que el conjunto de los números algebraicos es *numerable*. Como el conjunto de todos los números reales no es numerable, de ello resulta la existencia de números reales no algebraicos.

Un método para enumerar el conjunto de los números algebraicos es el siguiente: a cada ecuación de la forma [1] se le adjunta el entero positivo

$$h = |a_n| + |a_{n-1}| + \cdots + |a_1| + |a_0| + n$$

que llamaremos su *altura*. Para un valor *fijo* de h existe sólo un número *finito* de ecuaciones [1] de altura h, y cada una de éstas tiene a lo sumo n raíces diferentes; por tanto, existe sólo un número finito de números algebraicos cuyas ecuaciones son de altura h, y podemos ordenar todos los números algebraicos en una sucesión, partiendo de los de altura 1, a continuación los de altura 2, y así sucesivamente.

Esta demostración de que el conjunto de los números algebraicos es numerable asegura la existencia de números no algebraicos; tales números se llaman *trascendentes*, pues, como dijo Euler, «trascienden al poder de los métodos algebraicos».

La demostración de Cantor de la existencia de números trascendentes a duras penas puede llamarse constructiva. Teóricamente, se puede construir un número trascendente aplicando el proceso diagonal de Cantor a un cuadro numerable de las expresiones decimales de las raíces de las ecuaciones algebraicas; pero este procedimiento es por completo impracticable y no conduciría a ningún número del que se pudiera escribir realmente su expresión en el sistema decimal o en otro cualquiera. Por otra parte, los problemas más interesantes relativos a los números trascendentes se reducen a demostrar que ciertos y determinados números, tales como π y e (estos números serán definidos en el capítulo IV) son, en efecto, trascendentes.

****2. El teorema de Liouville y la construcción de números trascendentes.**—Una demostración de la existencia de números trascendentes anterior a la de Cantor fué dada por J. Liouville (1809-1882), y permite efectivamente *construir* ejemplos de tales números. Es algo más difícil que la demostración de Cantor, como ocurre casi siempre con las demostraciones constructivas comparadas con las que se limitan a probar la existencia. Incluímos la demostración para conocimiento del lector más preparado, aunque tampoco requiere gran bagaje matemático.

Liouville demostró que los números algebraicos irracionales son aquellos que no pueden ser aproximados mediante números racionales con un alto grado de exactitud, salvo que los denominadores de las fracciones que constituyen dichas aproximaciones sean muy grandes.

Supongamos que el número z satisface a la ecuación algebraica de coeficientes enteros

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = 0 \qquad (a_n \neq 0), \tag{2}$$

pero no a una ecuación de grado inferior. Se dice entonces que z es un número algebraico *de grado n*; p. ej., $z = \sqrt{2}$ es un número algebraico de grado 2 por satisfacer a la ecuación $x^2 - 2 = 0$ y no ser raíz de ninguna ecuación de primer grado; $z = \sqrt[3]{2}$ es de tercer grado, ya que satisface a la ecuación $x^3 - 2 = 0$ y, según hemos visto en el capítulo III, a ninguna ecuación de grado inferior. Un número algebraico de grado $n > 1$ no puede ser racional, pues un número racional $z=p/q$ satisface a la ecuación de grado 1, $qx - p = 0$. Ahora bien: todo número irracional z puede aproximarse hasta el grado de exactitud deseado por un número racional, lo que significa que podemos determinar una sucesión

$$\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots$$

de números racionales con denominadores crecientes tales que

$$\frac{p_r}{q_r} \to z.$$

El teorema de Liouville afirma que para todo número algebraico z de grado $n > 1$ tal aproximación debe adolecer de un error mayor que $1/q^{n+1}$; esto es, que la desigualdad

$$\left| z - \frac{p}{q} \right| > \frac{1}{q^{n+1}} \tag{3}$$

subsiste para denominadores q suficientemente grandes.

Nos proponemos demostrar el teorema; pero en primer lugar vamos a ver cómo permite la construcción efectiva de números trascendentes. Sea el número (véase pág. 25 para la definición del símbolo $n!$)

$$z = a_1 \cdot 10^{-1!} + a_2 \cdot 10^{-2!} + a_3 \cdot 10^{-3!} + \cdots + a_m \cdot 10^{-m!} +$$
$$+ a_{m+1} \cdot 10^{-(m+1)!} + \cdots = 0{,}a_1a_2000a_300000000000000000a_40000000\ldots,$$

donde los a_i son números dígitos arbitrarios de 1 a 9 (podemos, p. ej., elegir todos los a_i iguales a 1). Tal número se caracteriza por el rápido crecimiento de las series de ceros, interrumpidas por dígitos aislados no ceros. Designemos por z_m la fracción decimal finita obtenida tomando sólo los términos de z hasta incluir el $a_m \cdot 10^{-m!}$. Entonces

$$|z - z_m| < 10 \cdot 10^{-(m+1)!}. \qquad [4]$$

Supongamos que z fuera algebraico de grado n, y pongamos en [3] $p/q = z_m = p/10^{m!}$, con lo que obtenemos

$$|z - z_m| > \frac{1}{10^{(n+1)m!}}$$

para m suficientemente grande. Combinando esta desigualdad con la [4] tendríamos

$$\frac{1}{10^{(n+1)m!}} < \frac{10}{10^{(m+1)!}} = \frac{1}{10^{(m+1)!-1}},$$

de modo que $(n+1)m! > (m+1)! - 1$ para todo m suficientemente grande, y esto es evidentemente falso para todo valor de m mayor que n (el lector puede hacer una demostración detallada de esta afirmación), lo que conduce a una contradicción; en consecuencia, z es trascendente.

Queda ahora por demostrar el teorema de Liouville. Supongamos que z es un número algebraico de grado $n > 1$ que satisface a [1], de forma que

$$f(z) = 0. \qquad [5]$$

Sea $z_m = p_m/q_m$ una sucesión de números racionales tales que $z_m \to z$. Entonces

$$f(z_m) = f(z_m) - f(z) = a_1(z_m - z) + a_2(z_m^2 - z^2) + \cdots + a^n(z_m^n - z^n).$$

Dividiendo ambos miembros de la ecuación por $z_m - z$, y utilizando la identidad algebraica

$$\frac{u^n - v^n}{u - v} = u^{n-1} + u^{n-2}v + u^{n-3}v^2 + \cdots + uv^{n-2} + v^{n-1}$$

obtenemos

$$\frac{f(z_m)}{z_m - z} = a_1 + a_2(z_m + z) + a_3(z_m^2 + z_m z + z^2) + \cdots + \qquad [6]$$
$$+ a_n(z_m^{n-1} + \cdots + z^{n-1}).$$

Como z_m tiene por límite z, para valores grandes de m diferirá de z en menos de 1, por lo que podemos escribir, para valores suficientemente grandes de m,

$$\left|\frac{f(z_m)}{z_m - z}\right| < |a_1| + 2|a_2|(|z| + 1) + 3|a_3|(|z| + 1)^2 + \cdots + \qquad [7]$$
$$+ n|a_n|(|z| + 1)^{n-1} = M,$$

que es un número fijo, ya que suponemos fijo z en nuestro razonamiento. Si ahora elegimos m suficientemente grande para que el denominador q_m de $z_m = p_m/q_m$ sea mayor que M, se tendrá

$$|z - z_m| > \frac{|f(z_m)|}{M} > \frac{|f(z_m)|}{q_m} \qquad [8]$$

Por brevedad escribamos p y q en lugar de p_m y q_m: Entonces

$$|f(z_m)| = \left|\frac{a_0q^n + a_1q^{n-1}p + \cdots + a_np^n}{q^n}\right| \qquad [9]$$

Ahora bien: el número racional $z_m = p/q$ no puede ser raíz de $f(x)=0$, pues si así fuese se podría suprimir el factor $(x - z_m)$ de $f(x)$, y z satisfaría a una ecuación de grado inferior a n; por consiguiente, $f(z_m) \neq 0$. Pero el numerador del segundo miembro de [9] es entero; por lo menos, pues, igual a 1. Finalmente, de [8] y [9] tenemos

$$|z - z_m| > \frac{1}{q}\frac{1}{q^n} = \frac{1}{q^{n+1}}, \qquad [10]$$

lo que demuestra el teorema

Durante las últimas décadas ha avanzado mucho la investigación acerca de la posibilidad de aproximar los números algebraicos mediante los racionales; p. ej., el matemático noruego A. Thue (1863-1922) demostró que en la desigualdad [3] de Liouville el exponente $n + 1$ puede ser sustituído por $(n/2) + 1$. C. L. Siegel probó posteriormente el enunciado aún más preciso (más preciso para valores grandes de n) de que subsiste para el exponente $2\sqrt{n}$.

El tema de los números trascendentes ha fascinado siempre a los matemáticos, pero hasta época muy reciente se conocían muy pocos ejemplos de números de interés intrínseco de los que se supiera eran trascendentes (en el capítulo III discutiremos el carácter trascendente de π, del cual resulta la imposibilidad de efectuar la cuadratura del círculo con la regla y el compás). En una famosa comunicación al Congreso internacional de matemáticas celebrado en París en 1900, David Hilbert propuso treinta problemas matemáticos fáciles de formular, algunos incluso en lenguaje elemental y hasta popular, pero ninguno de ellos resuelto y ni siquiera inmediatamente accesible a la técnica matemática entonces existente. Estos «problemas de Hilbert» fueron un reto al subsiguiente período del desarrollo matemático, y casi todos han sido ya resueltos, constituyendo a menudo su solución un claro progreso de la potencia del instrumento matemático y de sus métodos generales. Uno de los problemas que parecían más inaccesibles consistía en demostrar la trascendencia del número

$$2^{\sqrt{2}}$$

o al menos probar que se trataba de un número irracional; durante más de treinta años no surgió ni la más remota esperanza de hallar un método prometedor de atacar el problema. Por fin Siegel e, independientemente, el joven matemático ruso A. Gelfond, descubrieron nuevos métodos para demostrar el carácter trascendente de muchos números importantes de la matemática, incluído el número de Hilbert $2^{\sqrt{2}}$, y más en general, cualquier número de la forma a^b siendo a un número algebraico $\neq 0$ ó 1, y b un número algebraico irracional.

SUPLEMENTO AL CAPÍTULO II

EL ÁLGEBRA DE LOS CONJUNTOS

1. **Teoría general.**—El concepto de *clase* o *conjunto* de objetos es uno de los más fundamentales de la matemática. Se define un conjunto mediante una propiedad o atributo $\mathfrak{A}$ que cada objeto considerado debe poseer o no; aquellos objetos que poseen la propiedad forman un conjunto correspondiente A. Así, si consideramos los enteros, y la propiedad $\mathfrak{A}$ es la de ser primo, el conjunto correspondiente A es el constituído por todos los números primos 2, 3, 5, 7, ...

El estudio matemático de los conjuntos se basa en el hecho de que éstos pueden ser combinados mediante ciertas operaciones para formar otros conjuntos, al igual que los números se combinan por adición y multiplicación para dar lugar a otros números. El estudio de las operaciones con los conjuntos constituye el «álgebra de conjuntos», que tiene muchas semejanzas formales (aunque también presenta diferencias) con el álgebra de los números. El hecho de que los métodos algebraicos puedan aplicarse al estudio de objetos no numéricos, como los conjuntos, pone de manifiesto la gran generalidad de conceptos de la matemática moderna. En los últimos años se ha visto que el álgebra de los conjuntos ilumina muchas ramas de la matemática, tales como la teoría de la medida y la teoría de las probabilidades; resulta también valiosa en la reducción sistemática de los conceptos matemáticos a sus fundamentos lógicos.

En lo que sigue I representará un conjunto fijo de objetos de naturaleza cualquiera que llamaremos conjunto universal o universo, y A, B, C, ... representarán subconjuntos arbitrarios de I. Si I es el conjunto de todos los enteros, A puede representar el conjunto de los enteros pares, B el de los impares, C el de los números primos, etc. O bien I puede ser el conjunto de todos los puntos de un plano dado, A el de todos los puntos interiores a una circunferencia determinada, B el conjunto de todos los puntos de otro círculo del plano, etc. Por conveniencia incluímos como «subconjuntos» de I al propio conjunto I y al «conjunto vacío» O, que no contiene elementos. El propósito de esta generalización artificial es el de conservar la regla de que a toda propiedad $\mathfrak{A}$ corresponda el subconjunto A de todos los elementos de I que poseen dicha propiedad. En el caso de que $\mathfrak{A}$ sea alguna propiedad válida universalmente, tal como la expresada por la ecuación trivial $x = x$, el correspondiente subconjunto de I será el mismo I, puesto que todo objeto satisface a esta ecuación, en tanto que si $\mathfrak{A}$ es alguna propiedad contradictoria en sí misma, como $x \neq x$, el correspondiente subconjunto no contendrá ningún objeto y lo representaremos por el símbolo O.

El conjunto A se dice que es un *subconjunto* del B si no hay ningún objeto en A que no esté también en B. En este caso escribimos

$$A \subset B \quad \text{o} \quad B \supset A.$$

P. ej., el conjunto A de todos los enteros múltiplos de 10 es un subconjunto del conjunto B de los enteros múltiplos de 5, ya que todo múltiplo de 10 lo es también de 5. La afirmación de $A \subset B$ no excluye la posibilidad de que sea $B \subset A$. Si ambas relaciones tienen lugar, decimos que los conjuntos A y B son iguales y escribimos

$$A = B.$$

Para que esto se verifique, cada elemento de A debe pertenecer a B, y recíprocamente; de modo que los conjuntos A y B contienen exactamente los mismos elementos.

La relación $A \subset B$ tiene muchas analogías con la relación de orden $a \leqslant b$ entre los números reales. En particular se verifica que

1) $A \subset A$.
2) Si $A \subset B$ y $B \subset A$, $A = B$.
3) Si $A \subset B$ y $B \subset C$, $A \subset C$.

Por esta razón la relación $A \subset B$ se denomina una «relación de orden». Su principal diferencia con la relación $a \leqslant b$ para los números consiste en que, mientras para *cada* par de números a y b subsiste siempre una de las relaciones $a \leqslant b$ ó $b \leqslant a$, esto no se verifica para los conjuntos; p. ej., si A designa el conjunto formado por los enteros 1, 2, 3,

$$A = \{1, 2, 3\},$$

y B el formado por los números 2, 3, 4,

$$B = \{2, 3, 4\},$$

entonces ni $A \subset B$ ni $B \subset A$. Por esta razón, la relación $A \subset B$ se dice que determina una ordenación parcial de los conjuntos, mientras la relación $a \leqslant b$ determina una ordenación completa entre los números.

De pasada observemos que en virtud de la definición de la relación $A \subset B$ resulta que

4) $O \subset A$ para cualquier conjunto A, y
5) $A \subset I$,

siendo A cualquier subconjunto del universo I. La relación 4) puede resultar un tanto paradójica, pero se halla de acuerdo con la interpretación estricta del signo $\subset$. Pues la afirmación $O \subset A$ sería falsa sólo si el conjunto vacío O contuviese un objeto no contenido en A, y como el conjunto vacío no contiene objeto alguno, resulta esto imposible, cualquiera que sea el conjunto A.

Vamos a definir ahora dos operaciones con conjuntos que tienen muchas de las propiedades algebraicas de la adición y multiplicación ordinarias de números, aunque conceptualmente son muy distintas. Sean A y B dos conjuntos cualesquiera; entenderemos por «unión» o «suma lógica» de A y B el conjunto formado por todos los objetos que pertenecen, bien a A o a B (incluídos los que puedan pertenecer a ambos), y este conjunto lo representaremos por el símbolo $A + B$. Definimos la «intersección» o «producto lógico» de A y B como el conjunto formado únicamente por aquellos elementos que pertenecen a *ambos* conjuntos A y B, y lo representaremos por el símbolo $A \cdot B$, o simplemente AB. Para aclarar estas operaciones, sean de nuevo A y B los conjuntos

$$A = \{1, 2, 3\}, \qquad B = \{2, 3, 4\},$$

Entonces $$A + B = \{1, 2, 3, 4\}, \qquad AB = \{2, 3\}.$$

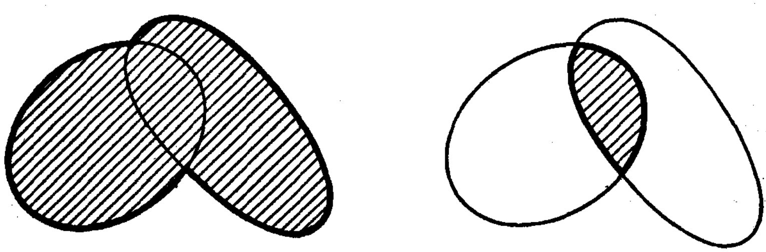
Entre las propiedades algebraicas importantes de las operaciones $A + B$ y AB se encuentran las siguientes, que pueden ser comprobadas por el lector basándose en la definición de las mismas:

6) $A + B = B + A$ 7) $AB = BA$
8) $A + (B + C) = (A + B) + C$ 9) $A(BC) = (AB)C$
10) $A + A = A$ 11) $AA = A$
12) $A(B + C) = (AB + AC)$ 13) $A + (BC) = (A + B)(A + C)$
14) $A + O = A$ 15) $AI = A$
16) $A + I = I$ 17) $AO = O$
18) la relación $A \subset B$ es equivalente a una de las dos relaciones $A + B = B$, $AB = A$.

La verificación de estas leyes es un problema de lógica elemental; p. ej., 10) dice que el conjunto formado por aquellos objetos que pertenecen, bien a A o a A es precisamente el conjunto A, mientras 12) afirma que el conjunto formado por aquellos objetos que son de A

y también de B o de C es el mismo que el formado por aquellos objetos que pertenecen, bien a ambos A y B, o a ambos A y C. El razonamiento lógico implicado en este y otros razonamientos puede aclararse mediante la representación de los conjuntos A, B, C por recintos planos, teniendo cuidado de considerar todas las posibilidades en cuanto a que los conjuntos en cuestión tengan elementos distintos y comunes entre sí.

Habrá observado el lector que las leyes 6), 7), 8), 9) y 12) coinciden con las familiares leyes conmutativa, asociativa y distributiva del álgebra, de donde resulta que todas las reglas del álgebra ordinaria de números que sean consecuencia de dichas leyes son también váli-



$A + B$ AB

FIG. 26.—Adición e intersección de dos conjuntos.

das en el álgebra de los conjuntos. Las leyes 10), 11) y 13), por otra parte, no tienen análogas en el caso de los números, lo que da al álgebra de conjuntos una estructura más sencilla que la del álgebra de los números; p. ej., el teorema del binomio del álgebra ordinaria, en el álgebra de los conjuntos viene reemplazado por la igualdad

$$(A + B)^n = (A + B) \cdot (A + B) \cdot \quad \cdots \quad \cdot (A + B) = A + B,$$

que es consecuencia de 11). Las leyes 14), 15) y 17) nos dicen que las propiedades de O e I respecto a la unión e intersección de conjuntos son muy similares a las propiedades de los números 0 y 1 respecto a la adición y multiplicación ordinarias. La ley 16) no tiene análoga en el álgebra de números.

Queda por definir una ulterior operación del álgebra de los conjuntos: sea A un subconjunto cualquiera del conjunto universal I. Por *complemento* de A en I entendemos el conjunto formado por todos los objetos de I que *no* pertenecen a A, y representaremos este conjunto por el símbolo A'. Así, si I es el conjunto de todos los números naturales y A el de los números primos, A' estará formado por 1 y todos los números compuestos. La operación A', que no tiene analogía exacta en el álgebra de los números, goza de las siguientes propiedades:

19) $A + A' = I$ 20) $AA' = O$
21) $O' = I$ 22) $I' = O$
23) $A'' = A$
24) La relación $A \subset B$ es equivalente a la relación $B' \subset A'$.
25) $(A + B)' = A'B'$ 26) $(AB)' = A' + B'$.

Dejamos de nuevo a cargo del lector la verificación de estas leyes.

Las leyes 1) a 26) constituyen la base del álgebra de los conjuntos, y poseen la notable propiedad de «dualidad», entendida en el sentido siguiente: *Si en una cualquiera de las leyes* 1) *a* 26) *los símbolos*

$$\begin{array}{ccc} \subset & \text{y} & \supset \\ O & \text{e} & I \\ + & \text{y} & \cdot \end{array}$$

se intercambian (dondequiera que aparezcan), el resultado es de nuevo una de dichas leyes.

P. ej., la ley 6) se transforma en la 7); la 12) en la 13); la 17) en la 16), etc. De ello resulta que *a todo teorema que pueda demostrarse basándose en las leyes* 1) *a* 26) *corresponde otro teorema «dual», que se obtiene mediante los intercambios indicados*. En efecto, como la demostración de todo teorema consiste en la aplicación sucesiva en cada etapa de alguna de las leyes 1) a 26), la aplicación a cada etapa de la ley dual nos dará la demostración del teorema dual (para una dualidad análoga en geometría, véase Cap. IV).

2. Aplicación a la lógica matemática.—La verificación de las leyes del álgebra de conjuntos se apoya en el análisis del significado lógico de la relación $A \subset B$ y de las operaciones $A + B$, AB y A'. Podemos ahora invertir este proceso y utilizar las leyes 1) a 26) como fundamento de un «álgebra de la lógica». Con más precisión, aquella parte de la lógica concerniente a los conjuntos, o lo que es equivalente, las propiedades o *atributos* de los objetos, puede reducirse a un sistema algebraico formal basado en las leyes 1) a 26). El «universo lógico» define el conjunto I; *cada propiedad o atributo* $\mathfrak{A}$ *de los objetos define el conjunto* A, *constituído por todos los objetos de* I *que poseen este atributo.* Las reglas para traducir la terminología lógica usual al lenguaje de los conjuntos quedan aclaradas con los siguientes ejemplos:

«Bien A o B»	$A + B$
«Ambos A y B»	AB
«No A»	A'

«Ni A ni B»	$(A + B)'$, o de forma equivalente $A'B'$
«No ambos A y B»	$(AB)'$, o de forma equivalente $A' + B'$
«Todo A es B» o «Si A también B» o «A implica B»	$A \subset B$
«Algunos A son B»	$AB \neq O$
«Ningún A es B»	$AB = O$
«Algunos A no son B»	$AB' \neq O$
«No hay ningún A»	$A = O$

En términos del álgebra de conjuntos, el silogismo «Barbara», que dice: «Si todo A es B, y todo B es C, entonces todo A es C», se escribe sencillamente

3) Si $A \subset B$ y $B \subset C$, entonces $A \subset C$.

Análogamente, la «ley de contradicción», que dice: «Un objeto no puede poseer simultáneamente un atributo y no poseerlo», se escribe

20) $AA' = O$,

mientras la «ley del *tertio excluso*» que dice: «un objeto debe poseer un atributo o no poseerlo» se transforma en

19) $A + A' = I$.

Así, pues, la parte de la lógica que puede expresarse con los símbolos $\subset$, $+$, $\cdot$, y $'$ puede tratarse como un sistema algebraico formal sometido a las leyes 1) a 26). Esta fusión del análisis lógico de las matemáticas y del análisis matemático de la lógica ha dado lugar a una nueva disciplina, la *lógica matemática*, que se halla actualmente en vías de vigoroso desarrollo.

Desde el punto de vista de la axiomática es notable el hecho de que las proposiciones 1) a 26), junto con todos los teoremas del álgebra de conjuntos, puedan deducirse de las tres ecuaciones siguientes:

27)
$$\begin{aligned} A + B &= B + A \\ (A + B) + C &= A + (B + C) \\ (A' + B')' + (A' + B)' &= A. \end{aligned}$$

Se deduce de ello que el álgebra de conjuntos puede construirse como una teoría puramente deductiva, al igual que la geometría euclídea, sobre la base de estas tres proposiciones aceptadas como axiomas. Cuando se ha hecho esto, la operación AB y la relación de orden $A \subset B$ se *definen* a partir de $A + B$ y A':

AB representa el conjunto $(A' + B')'$
$A \subset B$ significa que $A + B = B$.

Un ejemplo completamente distinto de un sistema matemático que satisface a todas las leyes formales del álgebra de conjuntos nos lo procuran los ocho números 1, 2, 3, 5, 6, 10, 15, 30, donde $a + b$ se define como el mínimo común múltiplo de a y b; ab, como el máximo común divisor de a y b; $a \subset b$, como la afirmación «a es un factor de b», y a', como el número $30/a$. La existencia de ejemplos tales ha llevado al estudio de los sistemas algebraicos generales que satisfacen a las leyes 27). Dichos sistemas se llaman «álgebras de Boole» en honor de George Boole (1815-1864), matemático y lógico inglés, autor del libro *An Investigation of the Laws of Thought*, publicado en 1854.

3. Una aplicación a la teoría de las probabilidades.—El álgebra de conjuntos aclara notablemente la teoría de las probabilidades. Para considerar sólo el caso más sencillo, imaginemos un experimento con un número finito de resultados posibles, todos los cuales se supondrán «igualmente probables». El experimento puede consistir, p. ej., en sacar una carta al azar de una baraja de 52 cartas perfectamente barajadas. Si el conjunto de los resultados posibles del experimento se representa por I, y si A designa cualquier subconjunto de I, entonces la probabilidad de que el resultado del experimento pertenezca al subconjunto A se define por el cociente

$$p(A) = \frac{\text{número de elementos de } A}{\text{número de elementos de } I}$$

Si designamos el número de elementos de un conjunto A por el símbolo $n(A)$, esta definición puede escribirse en la forma

$$p(A) = \frac{n(A)}{n(I)} \qquad [1]$$

En nuestro ejemplo, si A representa el subconjunto de «corazones», entonces $n(A) = 13$, $n(I) = 52$ y $p(A) = 13/52 = 1/4$.

Los conceptos del álgebra de conjuntos intervienen en el cálculo de probabilidades cuando se conocen las probabilidades de ciertos conjuntos y se desean calcular las correspondientes a otros; p. ej., si conocemos $p(A)$, $p(B)$ y $p(AB)$, podemos calcular la probabilidad $p(A + B)$:

$$p(A + B) = p(A) + p(B) - p(AB). \qquad [2]$$

La demostración es inmediata; en efecto,

$$n(A + B) = n(A) + n(B) - n(AB),$$

ya que los elementos comunes a A y a B, esto es, los elementos de AB, están contados dos veces en la suma $n(A) + n(B)$, y, en consecuencia, debemos restar de esta suma $n(AB)$ para obtener el resultado correcto que corresponde a $n(A+B)$. Dividiendo cada término de esta igualdad por $n(I)$ obtenemos la ecuación [2].

Se obtiene una fórmula más interesante al considerar tres subconjuntos, A, B, C, de I. De [2] resulta

$$p(A + B + C) = p[(A + B) + C] = p(A + B) + p(C) - p[(A + B)C].$$

Por la ley 12) de la página 120 sabemos que $(A + B)C = AC + BC$. En consecuencia,

$$p[(A + B)C] = p(AC + BC) = p(AC) + p(BC) - p(ABC).$$

Sustituyendo en la ecuación previa este valor de $p[(A + B)C]$ y el valor de $p(A + B)$ dado por [2], obtenemos el resultado deseado:

$$p(A + B + C) = p(A) + p(B) + \\ + p(C) - p(AB) - p(AC) - p(BC) + p(ABC). \qquad [3]$$

Como ejemplo, consideremos el siguiente experimento: se escriben al azar los tres dígitos 1, 2, 3 y se pide la probabilidad de que uno al menos ocupe su correspondiente lugar. Sea A el conjunto de todas las permutaciones en las que el 1 está en primer lugar; B el de aquellas donde el 2 está en segundo lugar, y C el conjunto de todas las permutaciones en las que el 3 está en tercer lugar. Deseamos, por tanto, calcular $p(A + B + C)$. Es obvio que

$$p(A) = p(B) = p(C) = \frac{2}{6} = \frac{1}{3};$$

pues cuando un dígito ocupa su propio lugar hay dos ordenaciones posibles para los restantes dentro del total de $3 \cdot 2 \cdot 1 = 6$ permutaciones posibles de los tres dígitos. Además,

$$p(AB) = p(AC) = p(BC) = \frac{1}{6}$$

y

$$p(ABC) = \frac{1}{6},$$

ya que hay sólo una forma de presentarse para cada uno de estos casos. De [3] resulta que

$$p(A + B + C) = 3 \cdot \frac{1}{3} - 3\left(\frac{1}{6}\right) + \frac{1}{6} =$$

$$= 1 - \frac{1}{2} + \frac{1}{6} = \frac{2}{3} = 0{,}6666 \cdots$$

Ejercicio: Hállese la fórmula correspondiente a $p(A + B + C + D)$ y aplíquese al caso de cuatro dígitos. La probabilidad correspondiente es $5/8 = 0{,}6250$.

La fórmula general para la suma de n subconjuntos es

$$p(A_1 + A_2 + \cdots + A_n) = \sum_1 p(A_i) - \sum_2 p(A_iA_j) + \sum_3 p(A_iA_jA_k) - \\ - \cdots \pm p(A_1A_2 \cdots A_n), \qquad [4]$$

donde los símbolos $\sum_1, \sum_2, \sum_3, \cdots, \sum_{n-1}$ representan las sumas de todas las combinaciones posibles de los conjuntos $A_1, A_2, \cdots, A_n$ tomados uno a uno, dos a dos, $\cdots$, $(n - 1)$ a $(n - 1)$. Esta fórmula puede establecerse por inducción matemática de igual modo que dedujimos [3] a partir de [2]. De [4] es fácil probar que si los n dígitos 1, 2, 3, $\cdots$, n se escriben al azar, la probabilidad de que al menos un dígito ocupe su propio lugar es

$$p_n = 1 - \frac{1}{2!} + \frac{1}{3!} - \frac{1}{4!} + \cdots \pm \frac{1}{n!}, \qquad [5]$$

en la cual el último término se toma con signo más o menos, según sea n par o impar. En particular, para $n = 5$, la probabilidad es

$$p_5 = 1 - \frac{1}{2!} + \frac{1}{3!} - \frac{1}{4!} + \frac{1}{5!} = \frac{19}{30} = 0{,}63333\cdots.$$

Veremos en el capítulo VIII que al tender n a infinito, la expresión

$$S_n = \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \cdots \pm \frac{1}{n!}$$

tiende al límite $1/e$, cuyo valor con cinco decimales es 0,36788. Dado que, por [5], $p_n = 1 - S_n$, queda demostrado que al tender n a infinito,

$$p_n \to 1 - 1/e = 0{,}63212.$$