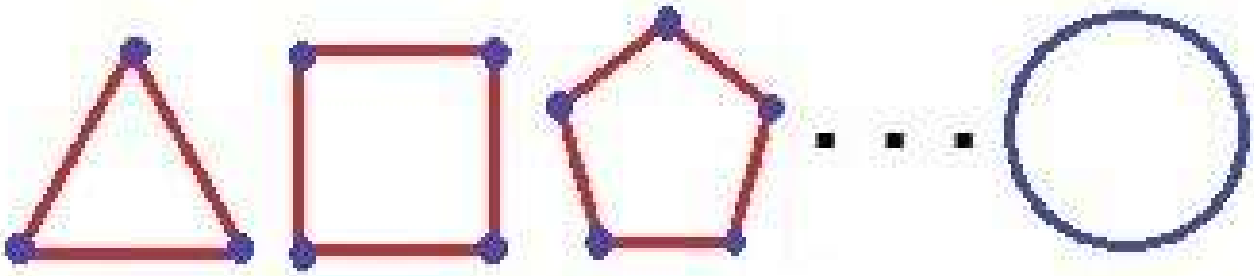
CMC Editions

ELEMENTOS DE LA TEORIA DE LOS CARDINALES INFINITOS

COMENTADOS DESDE UNA PERSPECTIVA ESTADÍSTICA

C. M. Cuadras

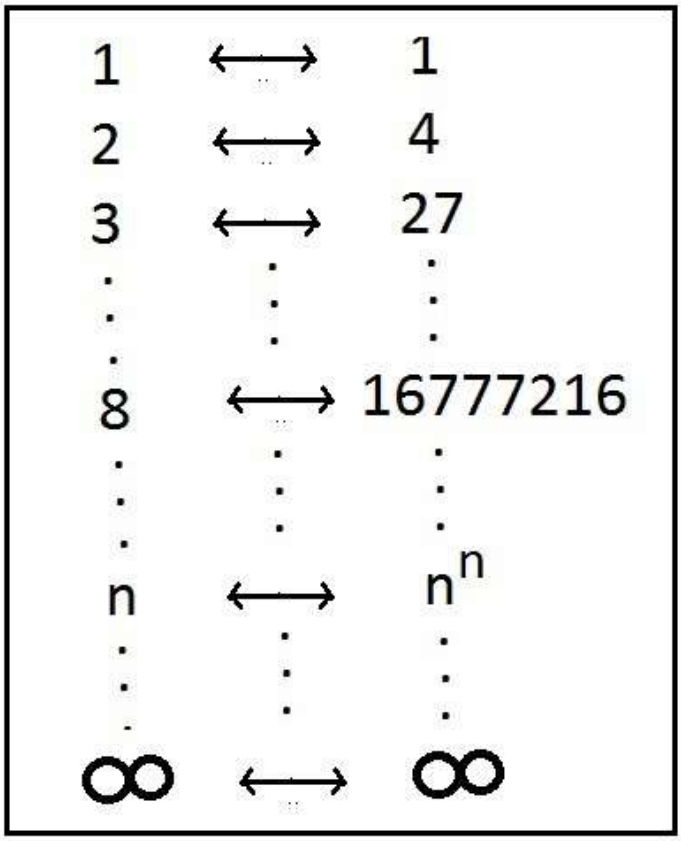


$$\aleph_0 < \aleph_1 \leq 2^{\aleph_0}$$

Barcelona 2020

INTRODUCCIÓN A LA TEORÍA DE LOS CARDINALES INFINITOS Y A ALGUNAS ESTRUCTURAS MATEMÁTICAS

COMENTARIOS DESDE UNA PERSPECTIVA ESTADÍSTICA



ELEMENTOS DE LA TEORIA DE LOS CARDINALES INFINITOS COMENTADOS DESDE UNA PERSPECTIVA ESTADÍSTICA

Carles .M. Cuadras

Diciembre 2020

Índice

Prólogo

El concepto del infinito ha interesado a los mateméticos desde los tiempos de la Grecia antigua. A mediados del siglo XIX se pudo desarrollar una teoría coherente sobre los infintos, que sería plenamente aceptada en el siglo XX. Debido a la imposibilidad de encontrar un equivalente físisco en el Universo real, el estudio de las magnitudes infinitas forma parte de la filosofía matemática, admitiendo solamente ilustraciones geométricas idealizadas.

Un cardinal finito es un número ordinario. Un cardinal infinito, o transfinito, es una magnitud que mide el tamaño de un conjunto infinito. Motivado por dos trabajos publicados en 2015 y 2019, y en un seminario impartido en un centro cultural, en esta monografía se explican y comentan los aspectos fundamentales de los cardinales transfinitos, con un estudio detallado de la hipótesis del continuo, haciendo referencias al principio de elección y al teorema de incompletitud de Gödel, teorema que afirma que ciertos enunciados maatemáticos son indemostrables. Se intenta, en algunos casos, relacionar tales conceptos con la probabilidad y la estadística.

La tercera parte se dedica a la construcción axiomática y formal de los números ordinarios (naturales, enteros, racionales y reales). La cuarta y última parte describe dos estructuras matemáticas, también basadas en axiomas, y que son importantes en estadística. En la exposición de las definiciones y propiedades, se alterna el rigor matemático con la intuición geométrica y la inducción numérica.

Capítulo 1

Números cardinales y aritmética transfinita

1.1 Introducción

En esta monografia se comentan y demuestran algunas propiedades de los números transfinitos también llamados cardinales infinitos, entendiendo que estos conceptos forman parte del fundamento de las matemáticas. Ciertas demostraciones son informales y no rigurosas, pero suficientes para entender cómo se ordenan los infinitos de diferentes magnitudes. Otras demostraciones poseen el debido rigor matemático, propio de una monografía especializada. Empecemos relacionando los infinitos con los infinitésimos.

Dos infinitésimos pueden ser comparados aunque ambos tiendan a cero. Por ejemplo, si $x > 0$ y $dx \to 0$, el límite del cociente

$$\frac{d(e^{x^2})}{dx^2} \to e^{x^2},$$

nos revela que $d(e^{x^2}) = 2xe^{x^2}dx$ es "mucho mayor" que $dx^2 = 2xdx$. Es decir, un "cero" es mucho mayor que otro "cero". Hay cantidades nulas que no son iguales.

De manera análoga, podemos decir que dos infinitos pueden ser comparados y probar que uno puede ser mucho mayor que el otro.

Supondremos conocidas las nociones básicas de la **teoría de conjuntos**. Recordaremos que un **conjunto** consta de **elementos** en cierto modo homogéneos entre sí, pues verifican alguna propiedad que les caracteriza

1. Por $a \in \mathbb{A}$ indicamos que el elemento a pertenece al conjunto $\mathbb{A}$.

2. El **conjunto vacío** carece de elementos y se indica por $\varnothing$.

3. $\mathbb{A}$ está incluido en $\mathbb{B}$, es decir, $\mathbb{A}$ es **subconjunto** de $\mathbb{B}$ y lo indicaremos por $\mathbb{A} \subset \mathbb{B}$, si todo elemento de $\mathbb{A}$ es también elemento de $\mathbb{B}$.

4. Todo conjunto está incluido en un conjunto general $\mathbf{\Omega}$.

5. La **unión** de de $\mathbb{A}$ con $\mathbb{B}$ es otro conjunto $\mathbb{A} \cup \mathbb{B}$.

6. La **intersección** de $\mathbb{A}$ con $\mathbb{B}$ es otro conjunto $\mathbb{A} \cap \mathbb{B}$.

7. El **complementario** de $\mathbb{A}$ lo indicamos por $\overline{\mathbb{A}}$ y está formado por los elementos de $\mathbf{\Omega}$ que no son de $\mathbb{A}$.

8. La unión de $\mathbb{A}$ y su complementario $\overline{\mathbb{A}}$ es $\mathbf{\Omega}$. Es decir, $\mathbb{A} \cup \overline{\mathbb{A}} = \mathbf{\Omega}$.

9. Dos conjuntos $\mathbb{A}$ y $\mathbb{B}$ son **disjuntos** si no tienen elementos comunes. Es decir, $\mathbb{A} \cap \mathbb{B} = \varnothing$.

10. Indicamos por $P(\mathbb{A})$ el conjunto de las **partes** o subconjuntos de $\mathbb{A}$, incluyendo también $\varnothing$ y $\mathbb{A}$, considerando $\mathbb{A}$ como subconjunto de sí mismo.

11. El conjunto **producto** $\mathbb{A} \times \mathbb{B}$ está formado por los pares ordenados (a, b), donde $a \in \mathbb{A}$ y $b \in \mathbb{B}$.

12. Una **función** $f : \mathbb{A} \to \mathbb{B}$ es una regla que a cada elemento a de $\mathbb{A}$ le hace corresponder un elemento b de $\mathbb{B}$.

Son de especial importancia las funciones que definen **correspondencias biyectivas** o correspondencias **uno-a-uno** entre dos conjuntos, pues permiten definir los números cardinales.

Recordemos también que una **relación de equivalencia** aRa' entre dos elementos a, a' de un conjunto $\mathbb{A}$, divide $\mathbb{A}$ en conjuntos disjuntos, llamados **clases de equivalencia**, cuya unión es $\mathbb{A}$. Esta colección de clases de equivalencia se indica por $\mathbb{A}/R$ y se denomina conjunto cociente. Cada elemento de $\mathbb{A}$ pertenece a una (y solo a una) clase de equivalencia.

Empezaremos hablando de los cardinales finitos.

1.2 Cardinales finitos

Diremos que dos conjuntos $\mathbb{A}$ y $\mathbb{B}$ tienen el **mismo cardinal** si existe una correpondencia biyectiva entre ambos.

Es decir,

$$\text{car}(\mathbb{A}) = \text{car}(\mathbb{B})$$

si y sólo si dado $a \in \mathbb{A}$ existe un único $b \in \mathbb{B}$ tal que al elemento a le corresponde el elemento b y recíprocamente.

Ejemplo: Sean $\mathbb{A} = \{a_1, a_2, a_3\}$ y $\mathbb{B} = \{b_1, b_2, b_3\}$. Entonces $a_i \leftrightarrow b_i$, $i = 1, 2, 3$. Vemos que $\text{car}(\mathbb{A}) = \text{car}(\mathbb{B})$. A este número cardinal común le llamamos "tres" y lo simbolizamos con el número natural 3.

En general, todo cardinal finito se simboliza con un número entero positivo, es decir, un número natural. Hablando más estrictamente, si R es la relación de equivalencia $\mathbb{A}R\mathbb{B}$ si $\mathbb{A}$ y $\mathbb{B}$ tienen el mismo cardinal, el conjunto cociente se identifica con los números naturales. Consideraremos también el 0 como un número natural. Indicaremos el conjunto de los números naturales por

$$\mathbb{N} = \{0, 1, 2, \ldots, n, \ldots\}.$$

El cardinal del conjunto $\mathbb{A}$ es **finito** si no es posible encontrar una correspondencia biyectiva entre $\mathbb{A}$ y un subconjunto propio de $\mathbb{A}$.

$$\mathbb{A} \text{ es finito si } \mathbb{B} \subset \mathbb{A} \text{ implica } \text{car}(\mathbb{B}) < \text{car}(\mathbb{A}).$$

Ejemplo: $\mathbb{A} = \{a_1, a_2, a_3\}$ es un conjunto de cardinal finito porque es imposible establecer una biyección entre $\mathbb{A}$ y $\{a_1, a_2\}$, o entre $\mathbb{A}$ y cualquier otro subconjunto de $\mathbb{A}$.

Indicaremos por $P(\mathbb{A})$ el conjunto de las partes de $\mathbb{A}$. Como una ilustración sencillla, si $\mathbb{A} = \{a_1, a_2, a_3\}$ entonces

$$P(\mathbb{A}) = \{\varnothing, \{a_1\}, \{a_2\}, \{a_3\}, \{a_1, a_2\}, \{a_1, a_3\}, \{a_2, a_3\}, \mathbb{A}\}.$$

Observamos que $P(\mathbb{A})$ contiene $2^3 = 8$ subconjuntos.

Propiedad 1 *Si el cardinal de $\mathbb{A}$ es n (número finito) entonces el cardinal de $P(\mathbb{A})$ es 2^n*

$$car(\mathbb{A}) = n \;\Rightarrow car(P(\mathbb{A})) = 2^n.$$

Prueba: Considerando combinaciones de k elememntos tomados de los n elementos de $\mathbb{A}$, vemos que

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = (1+1)^n = 2^n.$$

El siguiente corolario es evidente en el caso finito.

Corolario 1 *El cardinal de un conjunto no vacío es menor que el cardinal de las partes (subconjuntos) de este conjunto*

$$car(\mathbb{A}) < car(P(\mathbb{A})).$$

1.3 Cardinales infinitos

El estudio riguroso de los cardinales infinitos empezó con George Cantor. Anteriormente, el infinito se consideraba un concepto útil pero no operativo. El "horror al infinito" es manifiesto en las vías de Santo Tomás de Aquino. Galileo Galilei rechazaba el infinito con el argumento de que la correspondencia $n \leftrightarrow 2n$ convertía en equivalentes el conjunto $\mathbb{N}$ de los naturales y el conjunto $\mathbb{P}$ de los números pares, siendo $\mathbb{P} \subset \mathbb{N}$. Galileo no concebía que un conjunto tuviera el mismo tamaño que su mitad. Sin embarfo, Cantor consideró que esta era precisamente una propiedad natural de los conjuntos infinitos.

Diremos que el conjunto $\mathbb{A}$ es **infinito** si puede establecerse una correspondencia biyectiva entre $\mathbb{A}$ y un subconjunto propio $\mathbb{B}$ de $\mathbb{A}$

$$\text{car}(\mathbb{A}) = \text{car}(\mathbb{B}) \quad \text{para algún } \mathbb{B} \subset \mathbb{A}.$$

Hemos visto que $\text{car}(\mathbb{N}) = \text{car}(\mathbb{P})$. Luego $\mathbb{N} = \{0, 1, 2, \ldots, n, \ldots\}$ es un conjunto infinito. Obsérvese que utilizamos puntos suspensivos horizontales (las llamadas lagunas infinitas), para describir $\mathbb{N}$, puesto que una descripción exhaustiva es imposible.

Conforme a la llamada notación de los "alephs" utilizada más adelante (capítulo 2), indicaremos el cardinal de $\mathbb{N}$ por A_0.

$$A_0 = \text{car}(\mathbb{N}).$$

A_0 es el infinito más pequeño, es decir, el primer cardinal no finito. Un conjunto con cardinal A_0 diremos que es **numerable**.

Otro conjunto infinito es el de los números racionales $\mathbb{Q}$, es decir, los números m/n donde m y n son enteros (positivos o negativos).

Propiedad 2 *$\mathbb{N}$ y $\mathbb{Q}$ tienen el mismo cardinal. Es decir, $\mathbb{Q}$ es numerable:*

$$car(\mathbb{Q}) = A_0.$$

Prueba. Admitamos que todo subconjunto de $\mathbb{N}$ es numerable, por ser de fácil demostración. Consideremos los racionales m/n irreductibles (no se puede simplificar la fracción), con n positivo. La correspondencia

$$-m/n \to 2^m 3^n \text{ si } -m < 0, \qquad m/n \to 5^m 7^n \text{ si } m > 0,$$

muestra que cada número racional se corresponde con un único número natural.

El conjunto $\mathbb{R}$ de los números reales es otro conjunto interesante. A diferencia de $\mathbb{Q}$, el conjunto $\mathbb{R}$ **no es numerable**. Esta notable propiedad, demostrada por Cantor, revela por primera vez en la historia de las matemáticas, que hay conjuntos de magnitud mayor que la de $\mathbb{N}$.

Indicaremos por c el cardinal de $\mathbb{R}$. Admitiremos (como un postulado geométrico) que la recta real está en correspondencia biyectiva con $\mathbb{R}$. Consideremos también $\mathbb{R}_+$ conjunto de los números reales positivos y el segmento o intervalo $[0,1]$.

Propiedad 3 $\mathbb{R}$, $\mathbb{R}_+$ *y el segmento* $[0,1]$ *tienen el mismo cardinal*

$$c = car(\mathbb{R}) = car(\mathbb{R}_+) = car([0,1]).$$

Prueba: Establecemos la correspondencia $x \to 2^x$ tal que a todo x (positivo o negativo) le corresponde 2^x que siempre es positivo. Así $\mathbb{R}$ está en correspondencia biyectiva con $\mathbb{R}_+$. Luego $c = \text{car}(\mathbb{R}) = \text{car}(\mathbb{R}_+)$.

Consideremos ahora el 0 junto con los reales positivos y establezcamos la correspondencia

$$x \to x/(x+1),$$

que prueba que $\text{car}(\mathbb{R}_+) = \text{car}([0,1])$, pues si x está entre 0 e ∞ entonces $x/(x+1)$ está comprendido entre 0 y 1.

El cardinal c se denomina **potencia del continuo**.

Propiedad 4 $\mathbb{R}$ *no es numerable. Por lo tanto*

$$A_0 < c.$$

Prueba. Por reducción al absurdo. Supongamos que el segmento $[0,1]$ es numerable. Expresemos sus números en base 2 de forma ordenada

$$\begin{aligned} &0, a_{11}a_{12}\cdots a_{1n}\cdots \\ &0, a_{21}a_{22}\cdots a_{2n}\cdots \\ &0, a_{31}a_{32}\cdots a_{3n}\cdots \\ &\cdots \end{aligned} \tag{1.1}$$

Construyamos el número $0, b_1b_2b_3\cdots$ de modo que $b_i = 1 - a_{ii}$ para todo $i = 1, \ldots, n, \ldots$. Este número no puede pertenecer a la secuencia numerable (1.1), pues difiere del primero en la primera cifra después de la coma (si $a_{11} = 0$, $b_1 = 1$ y si $a_{11} = 1$, $b_1 = 0$), difiere del segundo en la segunda cifra, del tercero en la tercera cifra, y así sucesivamente. Luego $[0,1]$ no puede ser numerable.

x	y	z		Conjunto
0	0	0	$\cdots$	Vacío
1	0	0	$\cdots$	$\{x, \ldots\}$
0	1	0	$\cdots$	$\{y, \ldots\}$
0	0	1	$\cdots$	$\{z, \ldots\}$
1	1	0	$\cdots$	$\{x, y, \ldots\}$
1	0	1	$\cdots$	$\{x, z, \ldots\}$
$\vdots$		$\vdots$		$\vdots$
1	1	1	$\cdots$	$\mathbb{A}$

Tabla 1.1: Codificación binaria de las partes de un conjunto.

Propiedad 5 *El cardinal del conjunto de las partes de* $\mathbb{N}$ *es* 2^{A_0}

$$car(P(\mathbb{N})) = 2^{A_0}.$$

Prueba. Veamos primero una "prueba" no rigurosa. El conjunto de las partes de un subconjunto finito de $\mathbb{N}$ con n elementos, tiene cardinal 2^n. Si hacemos tender n a ∞, es decir, a A_0, obtenemos el resultado.

Podemos probarlo de un modo más general y riguroso. Escribamos los subconjuntos de un conjunto $\mathbb{A}$ mediante sucesiones de $0'$s y $1'$s (bits) según contengan o no los elementos $x, y, z, \ldots$ de $\mathbb{A}$.

Por ejemplo, la sucesión $000\cdots0\cdots$ (todo ceros) está relacionada con el conjunto vacío. La sucesión $100\cdots$ (uno seguido de ceros) está relacionada con el subconjunto $\{x, \ldots\}$ que al menos contiene a x. La sucesión $111\cdots1\cdots$ (todo unos) contiene a todos los elementos de $\mathbb{A}$ (todos los números naturales si $\mathbb{A}$ es $\mathbb{N}$). Como podemos construir $2 \times 2 \times 2 \times \cdots$ sucesiones distintas, multiplicando tantas como elementos tiene $\mathbb{A}$, vemos que $\text{car}(P(\mathbb{A})) = 2^{\text{car}(\mathbb{A})}$. En particular $\text{car}(P(\mathbb{N})) = 2^{A_0}$.

Conviene notar que no hay una cantidad numerable, en general, de tiras de bits en la tabla 1.1. De hecho, hemos probado la siguiente

Propiedad 6 *El cardinal del conjunto de las partes de* $\mathbb{A}$ *es*

$$car(P(\mathbb{A})) = 2^{car(\mathbb{A})}.$$

Debemos interpretar 2^{A_0} como una operación **convencional** y como una magnitud relativa. Por ejemplo, 2^{A_0} es un infinito "mucho mayor" que A_0.

Las magnitudes de los conjuntos $\mathbb{R}$ y $\mathbb{N}$ se relacionan tomando la colección de subconjuntos (las partes) de $\mathbb{N}$.

Propiedad 7 .

$$c = 2^{A_0}.$$

Prueba. Escribamos cualquier número del segmento $[0, 1]$ en base binaria, por ejemplo $0, 11010001$. Como esta base tiene dos cifras, el 0 y el 1, podemos encontrar tantos números como $2 \times 2 \times 2 \times \cdots$, es decir, el 2 multiplicado tantas veces como $\text{car}(\mathbb{N}) = A_0$.

Combinando las dos proposiciones anteriores, tenemos que

$$\text{car}(P(\mathbb{N})) = c = 2^{A_0}.$$

Para ser más precisos en la definición de cardinales, establezcamos la relación de equivalencia $\mathbb{A}R\mathbb{B}$ si $\mathbb{A}$ y $\mathbb{B}$ poseen el mismo cardinal, y tomemos el conjunto cociente. Obtenemos los números cardinales (finitos o infinitos), pues cada clase de equivalencia agrupa los conjuntos con el mismo número de elementos, y dos clases de equivalencia distintas definen números distintos. Una definición todavia más precisa de cardinal (debida a Von Neumann), se enuncia en la sección 2.2.

De lo visto hasta aquí, los números cardinales son $0, 1, 2, \ldots, n, \ldots, A_0, c$. Pero hay muchos más.

1.4 Aritmética transfinita

Los cardinales no tienen las mismas propiedades que los números ordinarios. Al escribir la suma de dos cardinales queremos decir el cardinal del conjunto reunión.

Supongamos $\mathbb{A}$ y $\mathbb{B}$ conjuntos disjuntos (no tienen elementos comunes). Definimos la **suma** de dos cardinales

$$\text{car}(\mathbb{A}) + \text{car}(\mathbb{B}) = \text{car}(\mathbb{A} \cup \mathbb{B}).$$

Consideremos ahora el conjunto producto $\mathbb{A} \times \mathbb{B}$, cuyos elementos son pares ordenados (a, b), donde $\mathbb{A}$ y $\mathbb{B}$ no son necesariamente disjuntos. Definimos la **multiplicación** de dos cardinales

$$\text{car}(\mathbb{A}) \cdot \text{car}(\mathbb{B}) = \text{car}(\mathbb{A} \times \mathbb{B}).$$

Las operaciones entre números transfinitos y finitos dan lugar a números transfinitos. Por ejemplo, para todo número finito real k se cumple:

$$A_0 + k = A_0, \quad c + k = c.$$

Las sumas y productos utilizando cardinales infinitos necesitan más explicación.

Propiedad 8 *Los cardinales A_0 y c verifican:*

1. $A_0 + A_0 = A_0$
2. $A_0 \times A_0 = A_0$
3. $A_0 + c = c$
4. $A_0 \times c = c$
5. $c + c = c$
6. $c \times c = c$

Prueba. Si $\mathbb{A} = \{a_1, a_2, \ldots\}$ y $\mathbb{B} = \{b_1, b_2, \ldots\}$ son numerables entonces $\mathbb{A} \cup \mathbb{B}$ es también numerable, pues podemos escribir sus elementos como $\{a_1, b_1, a_2, b_2, , \ldots\}$. Luego 1) es cierto. Además, considerando el intervalo $(0, 1)$ y el conjunto $\mathbb{N}$, y tomando $\mathbb{N} \cup (0, 1)$, probamos 3). Si escribimos en binario los pares ordenados de $\mathbb{N} \times (0, 1)$, podemos probar 4).

Probemos 2) viendo que si $\mathbb{A}$ y $\mathbb{B}$ son numerables, $\mathbb{A} \times \mathbb{B}$ también lo es. A cada par (a, b) le corresponderá el par de números naturales (m, n). La aplicación $(a, b) \leftrightarrow (m, n) \to 2^m 3^n$, muestra que $\mathbb{A} \times \mathbb{B}$ está en correspondencia con un subconjunto de números naturales, luego es numerable.

La 5) y 6) son consecuencia de 1), puesto que

$$c + c = 2^{A_0} + 2^{A_0} = 2^{A_0+1} = 2^{A_0}$$
$$c \times c = 2^{A_0} \times 2^{A_0} = 2^{A_0+A_0} = 2^{A_0} = c$$

Corolario 2 *La recta real $\mathbb{R}$, el plano $\mathbb{R}^2$ y el espacio $\mathbb{R}^3$ tienen la misma potencia.*

Así pues, resulta que el espacio $\mathbb{R}^3$ tiene también la potencia del continuo. Sorprende que el pequeño segmento $[0, 1]$ posea el mismo número de puntos que todo el espacio tridimensional, que imaginamos de enorme magnitud. Conviene advertir que solamente son dos conjuntos matemáticos infinitos equiparables. En el mundo físico, esta comparación es inimaginable.

Con más generalidad y teniendo en cuenta que $c \times \cdots \times c = c$ con independencia del número de veces que multiplicamos, vemos que dos espacios euclídeos de diferente dimensión tienen el mismo cardinal:

$$\text{car}(\mathbb{R}^m) = \text{car}(\mathbb{R}^n) = c.$$

1.5 La hipótesis del continuo

Cantor estaba muy satisfecho de probar que $A_0 < c$. El infinito numerable era superado por la potencia del continuo. Sin embargo pronto le plantearon una objeción a su teoría. La cuestión era saber si entre A_0 y c había otro cardinal infinito, que indicamos por g, verificando:

$$A_0 < g < c.$$

Cantor afirmó que no había ningún g e intentó probarlo. La afirmación de que g no existe y por lo tanto el siguiente infinito después de A_0 es c y no otro, se conoce como **hipótesis del continuo**. Los esfuerzos de Cantor (y el de otros matemáticos notables) en probar la hipótesis del continuo (HC), fueron infructuosos. Desconocían que se trataba de una proposición **indecidible**, es decir, que no se puede demostrar ni su veracidad ni tampoco su falsedad.

Observemos que manipular números transfinitos es sumamente delicado. Sabemos que el siguiente al número natural n es el número $n+1$. Pero dentro del conjunto $\mathbb{Q}$ de los números racionales, no es posible hablar de un siguiente. No podemos precisar cual es el siguiente de $2/3$, ni el siguiente racional que viene después de $41/75$, siendo este siguiente mayor que $41/75$. Es imposible, salvo que establezcamos una ordenación aprovechando que $\mathbb{Q}$ es numerable. Pero esta ordenación no respetaría la magnitud. Es decir, si el racional a_{n+1} es el siguiente de a_n, no necesariamente $a_n < a_{n+1}$. Con los números reales las cosas empeoran, pues $\mathbb{R}$ no es numerable. Pasando ahora a los números transfinitos y considerando el número A_0, puede ocurrir que no tenga sentido hablar del siguiente número transfinito, aunque hayamos probado que $A_0 < c$. Sin embargo, aceptando el axioma de elección, todo cardinal es biyectable con un ordinal (véase la sección 2.2). Luego dos cardinales cualesquiera distintos son comparables. Pero, aunque por comodidad, en esta monografía hemos utilizado el término "siguiente", seguimos sin poder hablar con claridad del cardinal "siguiente inmediato" a un cardinal dado.

El famoso Teorema de Gödel afirma que en un sistema formal hay propiedades que son indemostrables. La hipótesis del continuo es una de estas propiedades. El mismo Gödel demostró que no puede refutarse (afirmar que es falsa). Más tarde Cohen demostró que tampoco puede probarse (afirmar que es cierta). Luego la hipótesis del continuo es un axioma independiente de los otros axiomas de la teoría de conjuntos. La Matemática sin este axioma es coherente y con este axioma también lo es.

Una proposición sobre los números naturales define un subconjunto $\mathbb{A}$ incluido en $\mathbb{N}$. Por ejemplo, "n es primo" define el conjunto $\{3, 5, 7, 11, 13, \ldots\}$. Veamos ahora un caso muy particular del Teorema de Gödel.

Propiedad 9 *Algunas proposiciones sobre los números naturales son indemostrables.*

Prueba. Una proposición viene descrita por un elemento de $P(\mathbb{N})$, conjunto de las partes de $\mathbb{N}$. Mediante nuestro lenguaje y símbolos matemáticos,

podemos describir a lo sumo una cantidad numerable de proposiciones, es decir A_0. Sin embargo el cardinal de $P(\mathbb{N})$ es $c = 2^{A_0}$. Como $A_0 < c$, hay (infinitas) proposiciones verdaderas pero imposibles de enunciar y por lo tanto indemostrables.

Esta "demostración" tiene relación con la llamada paradoja semántica de Richard, a saber, que el conjunto de descripciones semámticas de números no puede ser numerable. Sin embargo, en la "demostración" de la propiedad anterior hemos supuesto una limitación física, en el sentido de que determinadas proposiciones son tan largas y complejas que no las podemos enunciar. Veamos a continuación una demostración formal de la paradoja de Richard.

Propiedad 10 *Las funciones $f(n)$ cuyo dominio es $\mathbb{N}$ constituyen un conjunto no numerable.*

Prueba. Son ejemplos de funciones $f(n) = n^2$, $f(n) = n^2 - n^3/9$. Supongamos que tales funciones se pueden numerar: $f_1(n)$, $f_2(n)$, $f_3(n)$, etc. Definimos la nueva función $g(n) = f_n(n) + 1$. La función g no puede estar en la lista numerable anterior, pues difiere de f_1 en $n = 1$, difiere de f_2 en $n = 2$, difiere de f_3 en $n = 3$, etc. Contradicción. Luego el conjunto de funciones $f(n)$ no se puede enumerar.

1.6 Notas históricas

Hay que remontarse a los tiempos aristotélicos para referirse al infinito. Una mención temprana a los números infinitos se halla en las paradojas de Zenón. En geometría se decía que dos rectas paralelas se cortan en el infinito, o se encuentran en un punto inalcanzable, para dar a entender que no se encuentran nunca. Con los precedentes del aristotelismo, la oposición a la noción de infinito influye en Santo Tomás de Aquino, en cuyas Vias se enuncian argumentos sobre la causa eficiente primera por considerar que no puede haber infinitas causas. La paradoja de Kepler-Olbers dice que si hubieran infintas estrellas la noche estaría iluminada. Galileo rechazó el infinito como cantidad, argumentando que en caso de aceptarlo, los números naturales y los números pares serían equiparables. Gauss (1831) sólo aceptaba el infinito como algo potencial, "una manera de hablar", no como un objeto absoluto o actual. El infinito no era un número, sino un concepto, una metáfora.

A pesar del rechazo de grandes sabios. la primera memoria sobre los infinitos lleva el título "Élémens de la géométrie de l'infini" (1727) de Fontenelle, que además del infinito potencial (el que aparece como un límite), aceptaba el infinito actual, que incluso puede ser manipulado algebraicamente. Una muestra de la polémica

suscitada es el título de la memoria "Absurdos geométricos que engendran ciertas interpretaciones del infinito matemático", del académico José Doménech y Estapá, publicada en Barcelona en 1894.

El estudio sistemático del tema lo cultiva el matemático alemán Georg Cantor (1845-1918). Estudiando el dominio de unicidad de los desarrollos en serie de Fourier, empezó a interesarse por la recta real como conjunto y por los "tamaños" o "magnitudes" de los conjuntos. En 1874, considerando que la paradoja de Galileo en realidad era una propiedad natural de los conjuntos infinitos, enunció que los números reales constituyen un conjunto de magnitud mayor que la de los números naturales. Poco después comunicó a Dedekind que la recta real estaba en correspondencia con el plano, es decir, ambos conjuntos eran equiparables. Este sorprendente resultado se publicó en 1878, con evidente retraso debido a la intervención de Kronecker. En 1878 Cantor establece la hipótesis del continuo, que afirma que no existen conjuntos de mayor magnitud que la numerable pero inferior a la de los números reales. Cantor intentó probar esta hipótesis sin éxito. Pero sus teorías no eran bien aceptadas. Su mentor Kronecker le calificó de charlatán científico, renegado y corruptor de jóvenes matemáticos. Poincaré (1905) comentó que la aritmética transfinita, a la que llaamaba teoría cantoriana de conjuntos, era un atentado a la matemática. No obstante, Hilbert en su lista de 23 problemas para resolver, propuesta en 1900, incluyó la hipótesis del continuo como primer problema. La cuestión se resuelve "en tablas" probando Gödel (1940) que no puede refutarse. Cohen (1963) probó que sí puede aceptarse. Aceptar o rechazar la hipótesis del continuo, no contradice la aritmética. Dicha hipótesis es independiente e indecidible.

No parece que la imposibilidad de probar la hipótesis del continuo, tema que minó la salud de Cantor, fuera conocida con prontitud. Bacmann (1955) en el libro "Transfinite Zahlen", Munroe (1952, 1959) en su libro "Introduction to measure and integration", Hahn (1956), en su artículo "Infinity". publicado en "The World of Mathematics" (traducido "El infinito" en 1968), Sierpinski (1956) en "La hipothèse du continu", y Orts (1957) en la memoria académica "El principio de elección", enuncian todos ellos la hipótesis del continuo como un problema no resuelto. Cabe decir que el artículo de Hahn está basado en una conferencia dictada en Viena en los años 1930, pero ni en su publicación en 1956 ni en la versión española de 1968, aparecen comentarios sobre la imposibilidad de resolver el problema del continuo. La misma omisión se advierte en "Los principios de la matemática", de Bertrand Russell, traducción de 1967, aunque la obra original es de 1902. Por cierto, B. Russell consideró "probable" la hipótesis del continuo y al hablar del infinito absoluto (defendido por Spinoza y Cantor), B. Russell comenta: "si existe". En 1965, Lipschutz en "General topology" menciona la hipótesis del continuo y su independencia de los axiomas de la teoría de conjuntos, mentando los resultados de

1963, pero sin citar a Cohen.

Nagel (1957), en "La demostración de Gödel" (traducido en 1968), menciona la aritmética transfinita de Cantor, pero sin dar detalles, y advierte sobre la posibilidad de que ciertas "antinomias" de la teoría de conjuntos puedan afectar a otras ramas de las matemáticas. Dou (1970) en su libro "Fundamentos de la matemática", aporta una demostración del teorema de Gödel, y menciona el problema del continuo, pero no dice nada de su indecidibilidad. Incluso más tarde, Obregón (1975), en "Teoría de la probabilidad", lo considera de interes teórico aún sin resolver. Y eso que pocos años antes, Mosterín (1971) en "Teoría axiomática de conjuntos", y Navarro (1973) en "La nueva matemática", comentan la irresolubilidad de la hipótesis del continuo, citando los trabajos de Gödel y Cohen. También demuestra estar al corriente del tema citando estos trabajos, Cuesta (1981) en "La sinfonía del infinito", considerando además la hipótesis del continuo como una ontología platónica. Digamos finalmente que Dou (1970) no descarta que tales proposiciones indecidibles puedan ser probadas mediante "metamatemática", y Chaitin (1991) incluso llega a afirmar que si los humanos no podemos responder a ciertas cuestiones matemáticas, Dios sí que puede. De hecho, Cantor consideró que la sucesión interminable de infinitos (véase el capítulo siguiente) estaba limitada por un infinito absoluto, que identificaba con Dios. Quizás Cantor, profundamente religioso y que había estudiado filosofía, respetó la Definición 6 de la "Ética" de Spinoza, que define a Dios como el ser absolutamente infinito.

Mencionemos tres anécdotas. Hilbert ilustró el infinito mediante el hotel de infinitas habitaciones, todas numeradas y ocupadas. Llega un autocar con infinitos clientes. El conserje, mostrando gran ingenio, decide enviar al huésped de la habitación n a la habitación 2n, consiguiendo liberar todas las habitaciones impares, lo que permite alojar a los nuevos clientes. Y el comentario irónico del académico Rodríguez-Salinas: el *Homo Sapiens*, después de Cantor, debería denominarse *Homo Trans-sapiens*. Por último, destaquemos la visión literaria del teorema de Gödel, bien narrada por Volpi en la novela "En busca de Klingsor" (2002).

Capítulo 2

Teoría de los alephs

Un aleph $\aleph$ (primera letra del alfabeto hebreo) es un símbolo para indicar un cardinal infinito. Su definición permite ordenar los infinitos. De momento solo conocemos $\aleph_0$ (que indicamos por A_0) y c.

2.1 La sucesión de los alephs

Una vez descubierto que había un cardinal infinito mayor que el numerable (hasta entonces el único infinito conocido), se abrió la veda para construir otros cardinales todavía mayores. Avancemos que el siguiente cardinal después de c está formado por el conjunto de funciones reales (continuas o no) con dominio un intervalo, como el $[0, 1]$.

2.1.1 Sucesión de Cantor

Empezando por A_0, tratemos de construir una sucesión indefinida y ordenada de cardinales, a saber:

$$A_0 < A_1 < \cdots < A_n < \cdots$$

La sucesión propuesta por Cantor (1895) consiste en tomar $A_0 = \text{car}(\mathbb{N})$, $A_1 = \text{car}(P(\mathbb{N})) = c$, $A_2 = \text{car}(P(P(\mathbb{N})))$ y así sucesivamente. De este modo, el cardinal siguiente a uno dado se construye tomando el conjunto de las partes o subconjuntos del anterior. En otras palabras, si tenemos el cardinal A_n entonces $A_{n+1} = 2^{A_n}$.
Nota: En atención al lector, utlizaremos la notación $A_0, A_1, \ldots$ en vez de $\aleph_0$, $\aleph_1, \ldots$, utilizada por Cantor.

La principal propiedad, demostrada por Cantor (1891), nos asegura que cada cardinal es de mayor magnitud que el anterior.

Propiedad 11 $A_n < A_{n+1} = 2^{A_n}$.

Prueba. Supongamos que $A_n = \text{car}(\mathbb{A})$ donde $\mathbb{A}$ es un conjunto. Entonces $A_{n+1} = 2^{A_n} = \text{car}(P(\mathbb{A}))$. Es obvio que $A_n \leq 2^{A_n}$. Tratemos de probar que es estrictamente menor.

Supongamos que $\mathbb{A}$ y $P(\mathbb{A})$ están en correspondencia biyectiva. Es decir, $A_n = 2^{A_n}$. Disponiendo los elementos de $\mathbb{A}$ como en la tabla 1.1, podemos suponer que a un subconjunto de $\mathbb{A}$ le corresponde un único elemento de $\mathbb{A}$. Entonces

$$\begin{aligned} 1000\cdots &\leftrightarrow a_{11}a_{12}a_{13}\cdots \\ 0100\cdots &\leftrightarrow a_{21}a_{22}a_{23}\cdots \\ 0010\cdots &\leftrightarrow a_{31}a_{32}a_{33}\cdots \end{aligned}$$

donde a_{ij} es 0 o 1.Por ejemplo, $01001101011\cdots$. Definamos la secuencia $b_1b_2b_3\cdots$ siendo $b_i = 1 - a_{ii}$. Esta secuencia representa un subconjunto de $\mathbb{A}$, ver tabla 1.1. Sin embargo no puede pertenecer a la lista anterior pues difiere en la cifra (0 o 1) situada en la diagonal. Luego 2^{A_n} supera en magnitud a A_n y por lo tanto debemos admitir que $A_n < 2^{A_n}$. Adviértese que la notación empleada es convencional, pues las secuencias anteriores no son numerables para $n > 0$, es decir, considerando un cardinal mayor que $A_{0.}$.

Otra demostarción puramente lógica y más directa, debida a Cantor, es como sigue. Supongamos que φ es una aplicación biyectiva tal que a cada elemento de $\mathbb{A}$ le corresponde un subconjunto de $\mathbb{A}$. Es decir, si $\mathbb{B} \subset \mathbb{A}$ entonces $\varphi(b) = \mathbb{B}$ para un único $b \in \mathbb{A}$.

Definamos $\mathbb{B} = \{x \in \mathbb{A} \text{ tal que } x \notin \varphi(x)\}$. Supongamos $\varphi(b) = \mathbb{B}$. Entonces, si $b \in \mathbb{B}$, por la definición de $\mathbb{B}$ vemos que $b \notin \varphi(b) = \mathbb{B}$. Pero si $b \notin \mathbb{B}$ entonces $b \in \varphi(b) = \mathbb{B}$. Esto es absurdo, luego φ no puede ser una aplicación exhaustiva, pues hay elementos de $\mathbb{A}$ que no tienen imagen en $P(\mathbb{A})$.

Nota. Al parecer, la demostración de Cantor inspiró la paradoja de Bertrand Russell (1902). Se define la clase de conjuntos

$$\mathbb{M} = \{\mathbb{A} \text{ tal que } \mathbb{A} \notin \mathbb{A}\}.$$

Entonces $\mathbb{M} \in \mathbb{M}$ si y sólo si $\mathbb{M} \notin \mathbb{M}$.

La sucesción de alephs propuesta por Cantor es precisa y está bien definida. Sin embargo:

a) Es imposible imaginar qué conjunto es $P(P(P...P(\mathbb{N}))...)$ (k veces) cuando k es grande.

b) Seguimos sin saber si entre A_n y A_{n+1} hay otro cardinal infinito g tal que $A_n < g < A_{n+1}$.

c) Los cardinales infinitos son, a lo sumo, entes geométricos que no pueden relacionarse con ningún objeto del mundo físico.

d) Es imposible imaginar físicamente las partes de un conjunto, pues muchos de estos subconjuntos poseen elementos comunes.

e) Si $\mathbb{A}$ es un ente físico, $P(\mathbb{A})$ no puede existir físicamente. Cuando hemos fabricado una partición se ha "roto" $\mathbb{A}$ y ya no podemos llevar a cabo otra partición.

Cantor afirmaba que no había ningún cardinal g tal que $A_n < g < A_{n+1} = 2^{A_n}$. Esta aserción, aceptada implícitamente en análisis matemático, se llama **hipótesis generalizada del continuo** (HGC), Sin embargo, la HGC es indecidible. No se puede probar ni su falsedad ni su veracidad. Sierpinski probó en 1947 que aceptando la HGC, se puede demostrar el axioma de elección (capítulo 4). Hoy en día, se acepta que ampliando los axiomas de la teoría de conjuntos (axiomas de Zermelo-Fraenkel), sería posible demostrar la hipótesis del continuo (Delahaye, 2020).

2.1.2 Sucesión que toma el siguiente

Otra construcción menos problemática es como sigue. Dado el cardinal A_n el cardinal A_{n+1}es el siguiente inmediato, en el sentido de que si $g > A_n$ y adenás $g \leq A_{n+1}$ entonces $g = A_{n+1}$. No obstante, no debemos olvidar que estamos tratando con infinitos y el concepto de "siguiente inmediato" puede ser impreciso o imposible de construir. Recordemos que no podemos hablar de número racional (o real) que sea el siguiente a un número racional (o real) dado.

Sea A_1 el número cardinal que sigue a A_0. No se sabe cual es, pero podemos encontrar su acotación.

Propiedad 12 *$A_1 \leq 2^{A_0}$ donde A_1 es el cardinal que sigue a A_0.*

Prueba. Sabemos que $A_0 < 2^{A_0}$. Luego el siguiente cardinal A_1 no puede ser mayor que 2^{A_0}.

Relacionando el cardinal de $\mathbb{N}$ con la hipótesis del continuo, y asumiendo

el axioma de elección (enunciado en la sección 4.1), podemos afirmar que

$$A_0 < A_1 \leq c = 2^{A_0}.$$

Aceptando la hipótesis generalizada del continuo, tenemos que

$$A_1 = 2^{A_0} = c < A_2 = 2^{A_1} = f,$$

donde el cardinal f se explica en la sección 2.3.

2.2 Ordinales

Los números naturales se pueden ordenar de menor a mayor. El conjunto $\mathbb{N}$, entendido como un ordinal, se indica por ω. En teoría moderna de conjuntos, se conviene que $0 = \varnothing$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, etc. Entonces $2 < 3$ es equivalente a $2 \in 3$, en el sentifdo de que $3 = \{0, 1, 2\}$ contiene al 2 como elemento. Además $\omega = \{0, 1, 2, \ldots\}$, $\omega + 1 = \{0, 1, 2, \ldots, \omega\}$, $\omega + 2 = \{0, 1, 2, \ldots, \omega, \omega + 1\}$, etc. Vemos que $\omega < \omega + 1$ es equivalente a $\omega \in \omega + 1$. De este modo la sucesión ordinal

$$0 < 1 < 2 < \cdots < \omega < \omega + 1 < \omega + 2 < \cdots$$

sugiere la sucesión de los alephs

$$A_0 < A_1 < A_2 < \cdots < A_\omega < A_{\omega+1} < A_{\omega+2} < \cdots$$

siendo A_ω el cardinal siguiente a la sucesión "natural" de cardinales. Asumiendo el axioma de elección, la sucesión existe en el sentido de que A_0 es el primer cardinal, A_1 es el siguiente de A_0, el siguiente de A_1 es A_2, etc. Sin embargo, siendo conocidas las propiedades teóricas de A_ω, se desconoce su esencia. Formalmente se puede definir de dos maneras

$$A_\omega = \sup_{n<\omega} A_n \qquad A_\omega = \sum_{n<\omega} A_n$$

Obsérveae que A_ω es un cardinal que no es siguiente de ningún otro cardinal.

En la figura 5.1 se representa una sucesión de polígonos de 0, 1, 2, 3,... vértices, tendiendo a la circunferencia. Sin embargo, el polígono límite, representación de ω, es numerable y por lo tanto no se puede identificar con la circunferencia completa, que no es numerable.

Propiedad 13 *Consideremos los polígonos regulares de n vértices inscritos en la circunferencia. El límite de estos polígonos cuando n tiende a infinito, es un conjunto numerable.*

Prueba. Podemos identificar la circunferencia con el intérvalo $[0, 1]$, que es un conjunto continuo no numerable. Multplicando por 360, obtenemos el intervalo $[0, 360]$. Como 360 es equivalente a 0, podemos prescindir del 360, es decir, del valor equivalente 1. Consideremos los conjuntos

$$\mathbb{V}_1 = \{0\}, \mathbb{V}_2 = \{0, 1/2\}, \mathbb{V}_3 = \{0, 1/3, 2/3\},\ \mathbb{V}_4 = \{0, 1/4, 2/4, 3/4\}.$$

Multplicando por 360, obtenemos las posiciones (ángulos) de los vértices de los correspondientes polígonos. Por ejemplo, $\mathbb{V}_4$ representa´ el cuadrado inscrito en la circunferencia, véase la figura 3.1, donde $1/4$ es un vértice del cuadrado. En general, definimos

$$\mathbb{V}_n = \{0, 1/n, 2/n, \ldots, (n-1)/n\},$$

querepresentaría un polígono de n vértices inscrito en la circunferencia. Estamos interesados en el límite geométrico de $\mathbb{V}_n$, al que llamaremos $\mathbb{V}_\infty$. Este conjunto no es vacío pues contiene, por ejemplo, $\mathbb{V}_4$, ya que $(n/4)/n$ tiende a $1/4$, $(n/2)/n$ tiende a $1/2$, y $(3n/4)/n$ tiende a $3/4$. Más en general, contiene a $\mathbb{V}_k$ pues si k'/k pertenece a $\mathbb{V}_k$ entonces $(k'n/k)/n$ tiende a k'/k.

Tomemos ahora el conjunto reunión $\mathbb{W} = \bigcup_{n\geq 1} \mathbb{V}_n$. Fusionando las repeticiones, los elementos de $\mathbb{W}$ son

$$\mathbb{W} = \{0, 1/2, 1/3, 2/3, 1/4, 3/4, 1/5, 2/5, 3/5, 4/5, 1/6, 5/6, \ldots\},$$

es decir, constituyen un subconjunto del conjunto $\mathbb{Q}$ de los números racionales. Luego $\mathbb{W}$ es numerable. Como $\mathbb{V}_\infty \subset \mathbb{W}$ tenemos que $\mathbb{V}_\infty$ es también numerable. Así pues, el límite del conjunto de vértices de los polígonos regulares se confunde con la circunferencia, pero no es la circunferencia propiamente dicha, ya que $\mathbb{V}_\infty$ tiene cardinal A_0 y la circunferencia tiene cardinal c.

Por otra parte, admitiendo el axioma de elección, se puede probar el **teorema de numerabilidad**: A todo conjunto $\mathbb{A}$ se le puede asociar algún ordinal α, de modo que $\mathbb{A}$ y α están en correspondencia biyectiva. Este importante teorema da lugar a la definición moderna de cardinal, que elige un representante de la clase de equivalencia de los conjuntos equipotentes: **Definición**. El cardinal de un conjunto $\mathbb{A}$ es el menor ordinal en correspondencia biyectiva con $\mathbb{A}$.

Todo número natural n es a la vez ordinal y cardinal. También ω es ordinal y cardinal, pero $\omega + 1$ no es cardinal, pues ambos tienen la misma potencia que $\mathbb{N}$, pero $\omega + 1$ no es el menor ordinal.

Sabemos qué son los dos primeros cardinales A_0 (numerable) y c (no numerable). Estudiemos ahora el tercer cardinal.

2.3 El cardinal que sigue al continuo

El cardinal A_2 es el siguiente a c. Con la hipótesis generalizada del continuo (HGC) debemos admitir que $A_2 = 2^{A_1}$. Sin la HGC entonces $A_2 \leq 2^{A_1}$. Pero, ¿qué es 2^{A_1}?

Existen varios conjuntos cuyo cardinal es 2^{A_1}. Por supuesto, el conjunto $P(\mathbb{R})$, es decir, el formado por todos los subconjuntos de la recta real, tiene este cardinal. Como hemos avanzado antes, el conjunto de las funciones reales con dominio un intervalo tiene cardinal A_2 (aceptando HGC) o cardinal 2^c en caso contrario. Llamemos $\mathbb{F}$ a este conjunto.

Propiedad 14 *El cardinal de $\mathbb{F}$ es de magnitud superior a la potencia del continuo*

$$car(\mathbb{F}) > c.$$

Prueba. Supongamos que $\text{car}(\mathbb{F}) = c$. Entonces a cada función le podemos asociar un número real x entre 0 y 1, pues la potencia del intervalo $[0, 1]$ es c. Sea h_x la función asociada a $x \in [0, 1]$. Definimos la función real $\overline{h}$ tal que $\overline{h}(x) = h_x(x) + 1$. Esta función difiere de $h_0(t)$ en el punto 0 pues $\overline{h}(0) = h_0(0) + 1$. Difiere de $h_{1/2}(1/2)$ en el punto $1/2$ pues $\overline{h}(1/2) = h_{1/2}(1/2) + \dot{1}$. En general $\overline{h}$ difiere de h_x en $t = x$. La suposición $\text{car}(\mathbb{F}) = c$ no se sostiene porque hemos construido una función $\overline{h}$ que no pertence al conjunto $\mathbb{F}$. Luego $\mathbb{F}$ no tiene la potencia del continuo.

Propiedad 15 *El cardinal de $\mathbb{F}$ es el mismo que el del conjunto de las partes de $\mathbb{R}$*

$$car(\mathbb{F}) = car(P(\mathbb{R})) = 2^c.$$

Prueba. $\text{car}(P(\mathbb{R})) = 2^c$ es un caso particular de la demostración anterior de que $\text{car}(P(\mathbb{A})) = 2^{\text{car}(A)}$ (véase la Propiedad 6), tomando como $\mathbb{A}$ el conjunto $\mathbb{R}$, cuyo cardinal es c. Véase la tabla 1.1.

Consideremos ahora el plano $\mathbb{R}^2$. Como $\mathbb{R}$ y $[0, 1]$ tienen el mismo cardinal c, nos restringiremos a las funciones con dominio el intervalo $[0, 1]$. Imaginemos cada función real como una curva que parte del eje vertical OY (ver figura 2.1).

Consideremos otra recta vertical a la derecha del eje OY. Llamaremos V a esta recta. La cantidad de curvas posibles pasando por V tiene potencia c. Por lo tanto podemos conseguir que pasen por $c \times c = c^2$ pares de puntos, el primero en OY, el segundo en V. Este proceso lo podemos repetir tantas veces como rectas verticales, es decir, c veces. Luego la potencia de las

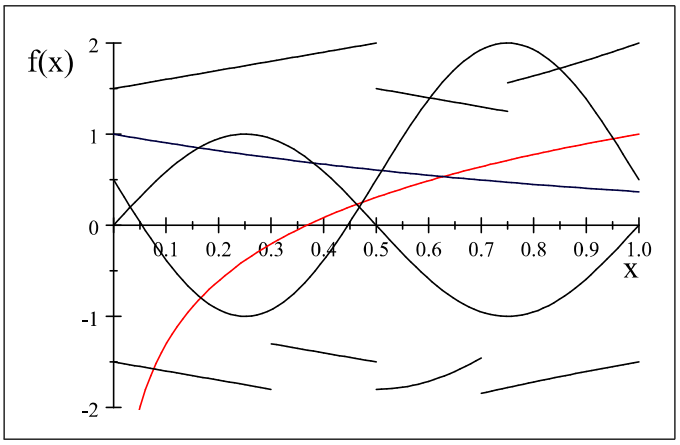


Figura 2.1: Algunas funciones (continuas o no continuas) con dominio el intervalo [0,1].

funciones posibles es $c \times c \times \cdots$ multiplicando c consigo mismo c veces. Es decir c^c. Tenemos pues

$$\text{car}(\mathbb{F}) = c^c = (2^{A_0})^c = 2^{c \times A_0} = 2^c.$$

Sabemos que $c < 2^c$. Como hemos dicho antes, $c^c = 2^c$ es una potencia convencional, pero coherente con la aritmética ordinaria.

Sorprendentemente, cuando nos restringimos a las funciones continuas, la cardinalidad disminuye drásticamente.

Propiedad 16 *El conjunto $\mathbb{F}_c \subset \mathbb{F}$ de todas las funciones continuas,tiene cardinal c.*

Prueba. Una función continua queda caracterizada por los valores que toma en los números racionales. Siguiendo el mismo razonamiento anterior, vamos a desplazar la recta V no continuamente, sino recorriendo el conjunto de los números racionales comprendidos entre 0 y 1. Este conjunto es numerable, luego

$$\text{car}(\mathbb{F}_c) = c^{A_0} = (2^{A_0})^{A_0} = 2^{A_0 \times A_0} = 2^{A_0} = c.$$

Llamemos $f = \text{car}(\mathbb{F})$. Admitiendo la HGC tendremos que $f = A_2$, es decir, f es el siguiente de c. Si ignoramos la HGC entonces $f \leq A_2$.

Hay otros conjuntos con cardinal f.

1) $f = \text{car}(P(\mathbb{R}^k))$, siendo $\mathbb{R}^k$ el espacio Euclídeo de dimensión k.

2) $f = \text{car}(L([0,1]))$, donde $L([0,1])$ es el conjunto de todas las funciones de probabilidad con soporte en $[0,1]$.

2.4 Números transfinitos todavía mayores

Podemos encontrar cardinales de mayor magnitud que $f = \text{car}(\mathbb{F})$, sin recurrir a la construcción del conjunto $P(\mathbb{F})$ de las partes de $\mathbb{F}$. Veamos una proposición general, cuya prueba es de tipo diagonal, similar a las pruebas anteriormente dadas.

Sea $\mathbb{K}$ un conjunto no vacío. Consideremos la clase $\mathbb{K}_{\mathbb{K}}$ de aplicaciones (o funciones) con dominio $\mathbb{K}$ y recorrido también $\mathbb{K}$.

Propiedad 17 *Si $\mathbb{K}$ es un conjunto no vacío, el cardinal de $\mathbb{K}$ es menor que el de $\mathbb{K}_{\mathbb{K}}$.*

Prueba: Supongamos que ambos cardinales son iguales. Entonces podemos indicar una función de $\mathbb{K}_{\mathbb{K}}$ como f_x, donde $x \in \mathbb{K}$. Definamos una nueva función $f(x)$ como sigue: $f(x) = \overline{[f_x(x)]}$ donde $\overline{[\cdots]}$ significa conjunto complementario. Entonces, si $f \in \mathbb{K}_{\mathbb{K}}$ le podemos asignar un índice s, es decir, $f = f_s$ y por lo tanto $f(s) = f_s(s)$, siendo $f_s(s)$ un elemento de $\mathbb{K}$ al que llamaremos $\mathbb{S}$. Pero por la definición de $f(x)$ tenemos que $f(s) = \overline{[f_s(s)]} = \overline{\mathbb{S}}$. De ser cierta la suposición inicial, llegaríamos a la igualdad $\mathbb{S} = \overline{\mathbb{S}}$, lo que solo puede ocurrir si $\mathbb{K}$ es el conjunto vacío. Concluimos que $f(x)$ no puede formar parte de la clase de funciones con índice un elemento de $\mathbb{K}$.

Si $A_n = 2^{A_{n-1}}$ es el cardinal de $\mathbb{K}$, siguiendo un razonamiento parecido al utilizado en la Propiedad 15, el cardinal de todas las funciones $f : \mathbb{K} \to \mathbb{K}$ es $A_n^{A_n}$. Luego

$$\text{car}(\mathbb{K}_{\mathbb{K}}) = A_n^{A_n} = \left(2^{A_{n-1}}\right)^{An} = 2^{A_n \times A_{n-1}} = 2^{A_n}.$$

Finalmente, indiquemos por $\mathbb{A}_{\mathbb{B}}$ elconjunto de todas las aplicaciones (o funciones) de $\mathbb{A}$ sobre $\mathbb{B}$. Se verifica la siguiente propiedad cuya demostración es análoga a las anteriores.

Propiedad 18 *Si $\mathbb{A}$ y $\mathbb{B}$ son dos conjuntos no vacíos*

$$car(\mathbb{A}_{\mathbb{B}}) = \ car(\mathbb{B})^{car(\mathbb{A})} > car(\mathbb{A}).$$

En particular si $\mathbb{B} = \{0, 1\}$ es un conjunto con sólo 2 elementos y $\mathbb{A}$ es un conjumto no vacío, entonces

$$\text{car}(\mathbb{A}_{\{0,1\}}) = 2^{\text{car}(\mathbb{A})} = \text{car}(P(\mathbb{A})) > \text{car}(\mathbb{A}).$$

Las siguientes propiedades de dos conjuntos $\mathbb{A}$ y $\mathbb{B}$ no vacíos son evidentes.

Propiedad 19 *Si car*$(\mathbb{A}) =$ *car*$(\mathbb{B})$ *entonces car*$(P(\mathbb{A})) =$ *car*$(P(\mathbb{B}))$.

Propiedad 20 *Si car*$(\mathbb{A}) <$ *car*$(\mathbb{B})$ *entonces car*$(P(\mathbb{A})) <$ *car*$(P(\mathbb{B}))$.

Distinción entre límite y cardinal. Los cardinales infinitos pueden provocar confusiones. El conjunto de los números naturales $\mathbb{N}$ y el conjunto $\mathbb{L} = \{0,\ 1,\ 4,\ 27, \ldots,\ n^n, \ldots\}$ tienen la misma potencia A_0, pues la correspondencia $n \leftrightarrow n^n$ es biyectiva. No obstante, el límite de n es el infinito ordinario, que identificamos con A_0, nos induce a pensar que el límite de n^n se puede identificar con $A_0^{A_0}$. Sin embargo ambos conjuntos $\mathbb{N}$ y $\mathbb{L}$ son numerables, $\text{car}(\mathbb{N}) = \text{car}(\mathbb{L}) = A_0$, mientras que

$$A_0^{A_0} = \text{car}(\mathbb{N}_{\mathbb{N}}) > A_0$$

por las propiedades 17 y 18.

Cardinales equivalentes. El cardinal de los números reales entre 0 y 1 es c, la potencia del continuo. Si estos números los expresamos en base 2, como podemos escribir las cifras 0 y 1 tantas veces como A_0, vemos que el cardinal es 2^{A_o}. Si estos mismos números los expresamos en base 3 (ver capítulo 3), o en base 10, obtenemos 3^{A_0} y 10^{A0}. Incluso, si suponemos que todos los números naturales están indicados con un símbolo distinto para cada uno de ellos, es decir, empleando A_0 cifras distintas, vemos que se pueden formar $A_0^{A_0}$ números reales. Todos estos cardinales infinitos son equivalentes:

$$2^{A_o} = 3^{A_0} = 10^{A0} = A_0^{A_0} = c.$$

Capítulo 3

Una perspectiva estadística

3.1 Probabilidad nula y conjunto de Cantor

Hemos visto algunas operaciones con números transfinitos mediante sumas y multiplicaciones, pero hemos evitado las divisiones. Sabemos de cursos elementales que $\infty + \infty = \infty$, $\infty \times \infty = \infty$, pero se nos advertía de que $0 \times \infty$ y ∞/∞ son operaciones cuyo resultado es indeterminado.

Sin embargo, en el caso finito sabemos que $n/n = 1$. Estamos pues tentados a escribir

$$\frac{A_0}{A_0} = 1, \qquad \frac{A_0}{c} = 0, \qquad \frac{c}{c} = 1.$$

No obstante, $A_0/c = 0$ es cierto, como consecuencia de tomar el límite al cociente $n/2^n$.

Vamos a ver dos ejemplo en los que $A_0/A_0 = 2$ y $c/c = 0$.

Sea $\mathbb{P}$ el conjunto de los números pares y $\mathbb{N}$ el de los naturales. Consideremos los primeros $2n$ números naturales y los primeros n números pares. Entonces, como consecuencia de que

$$\frac{2n}{n} = 2 \quad \text{y} \quad \frac{2^{2n}}{2^n} = \frac{1}{2^n} \to 0,$$

sentimos la tentación de escribir

$$\frac{\text{car}(\mathbb{N})}{\text{car}(\mathbb{P})} = 2 \quad \text{y} \quad \frac{\text{car}(P(\mathbb{N}))}{\text{car}(P(\mathbb{P}))} = \frac{c}{c} = 0.$$

Probabilidad nula. Consideremos ahora el conjunto $\mathbb{Q}$ de los números racionales. Vamos a restringirnos al cnjunto $\mathbb{Q}_I$ de los racionales dentro del intervalo $[0, 1]$. Elijamos un número real al azar entre 0 y 1, siendo todos los posibles números equiprobables.

Propiedad 21 *La probabilidad de elegir un número racional es cero*

$$\Pr(\mathbb{Q}_I) = 0.$$

Prueba. El conjunto $\mathbb{Q}_I$ es numerabale. A cada racional le podemos hacer corresponder un número natural n. Sea pues $\mathbb{Q}_I = \{q_1, q_2, \ldots, q_n, \ldots\}$.

Tomemos un número ϵ real positivo arbitrariamente pequeño. Podemos cubrir el racional q_1 por un intervalo I_1 de longitud $\epsilon/2$, y en general, el racional q_n por un intervalo I_n de longitud $\epsilon/2^n$. Estos intervalos pueden solaparse. Entonces

$$\Pr\left(\bigcup_{n=1}^{\infty} I_n\right) < \sum_{n=1}^{\infty} \Pr(I_n) = \sum_{n=1}^{\infty} \frac{\varepsilon}{2^n} = \varepsilon,$$

pues cada intervalo I_n tiene probabilidad $\varepsilon/2^n$. Como ε es tan pequeño como queramos, esta probabilidad es cero.

Podemos imaginar la figura 3.1 como la esfera de un reloj. Si el reloj se para al azar, la probabilidad de que el momento exacto de detención de la aguja sea un número racional, es igual a 0. Sin embargo, solo somos capaces de registrar este instante mediante un número racional con escasas cifras decimales. Además, puede ocurrir que sea imposible medir el tiempo transcurrido en recorrer la aguja ciertos conjuntos no medibles.

Conjunto de Cantor. Es un conjunto que se construye quitando intervalos al intervalo $[0, 1]$. Empecemos dividiendo este intervalo en 3 partes, eliminando el intervalo central $(1/3, 2/3)$. De los dos intervalos que quedan les quitamos el intervalo central a cada uno. Y así sucesivamente hasta quedar un conjunto "lleno de agujeros" al que llamaremos $\mathbb{C}$.

Expresemos ahora los números entre 0 y 1 en base 3. Un número cualquiera sería de la forma

$$0,1011201022011\cdots$$

es decir, contendría solo las cifras 0, 1 y 2.

Un número pertence al conjunto $\mathbb{C}$ si y solo si, en base 3, no contiene la cifra 1. Por ejemplo, el número

$$0,02202202022$$

Propiedad 22 *El conjunto de Cantor tiene la potencia del continuo*

$$car(\mathbb{C}) = c.$$

Figura 3.1: La probabilidad de que la aguja de un reloj se detenga al azar sobre un número racional vale cero. Es decir, el tiempo que tarda la aguja en pasar por los números racionales es nulo. Por otra parte, si aceptamos el axioma de elección, (sección 4.1) puede ocurrir que sea imposible medir el tiempo transcurrido en recorrer la aguja ciertos conjuntos no medibles (Imagen tomada de Dauben, 1995).

Prueba. Podemos establecer la correspondencia siguiente entre los números x e y

$$x = 0, a_1 a_2 a_3 \cdots \text{ (en base 2)} \leftrightarrow y = 0, b_1 b_2 b_3 \cdots \text{(en base 3)}$$

siendo $b_i = 0$ si $a_i = 0$ y $b_i = 2$ si $\mathrm{a}_i = 1$. Vemos que x es un número cualquiera entre 0 y 1 mientras que y pertence a $\mathbb{C}$, pues tiene las mismas cifras, pero cambiando unos por doses, y está expresado en base 3, no conteniendo ninguna cifra 1. Como la potencia del intervalo $(0, 1)$ es c, el conjunto $\mathbb{C}$ tiene la misma potencia.

Propiedad 23 *El conjunto de Cantor tiene probabilidad cero*

$$\Pr(\mathbb{C}) = 0.$$

Prueba. Consideremos un dado de 3 caras con las cifras 0, 1, 2. Lanzando n veces el dado, la probabilidad de que no salga el 1 es

$$(2/3)^n \to 0.$$

Es decir, si lanzamos el dado muchas veces, la probabilidad de que obtengamos solo las cifras 0 y 2 tiende a 0 cuando aumentamos el número de tiradas.

En consecuencia, es nula la probabilidad de poder construir un número real con solo secuencias de $0's$ y $2's$ y que por tanto pertenezca a $\mathbb{C}$. El resultado sería el mismo si las tres caras del dado tuvieran probabilidades distintas de $1/3$. Vale la pena observar que el suceso "nunca sale 1" es matemáticamente posible pero empíricamente imposible.

Utilicemos ahora un modelo continuo. Supongamos que elegimos un número al azar en $[0, 1]$ con la misma densidad de probabilidad. Si quitamos el intervalo central, la probabilidad de elegir un número real dentro de los dos intervalos extremos es $1 - 1/3$. Si luego quitamos los intervalos centrales de los dos que quedan, la probabilidad desciende a $1-1/3-2(1/9)$. Siguiendo indefinidamente con esta substracción, la probailidad (medida de Lebesque) es

$$1 - 1/3 - 2(1/9) - 4(1/27) - \cdots = 1 - \frac{1}{2}\sum_{k=1}^{\infty}(\frac{2}{3})^k = 1 - 1 = 0.$$

Propiedad 24 *Hay conjuntos que no tienen probabilidad.*

Prueba. Consideremos el intervalo $[0, 1]$ con probabilidad 1, la longitud del intervalo. Diremos que los números reales x, y son equivaletes si $x-y = q$ es un número racional. Dos clases de equivalencia son disjuntas y si tomamos sólo números entre 0 y 1 (sumando o restando un racional si es necesario), la unión de las clases de equivalencia es $[0, 1]$. Aceptando el axioma de elección (véase sección 4.1), elegimos un número real de cada clase de equivalencia para formar el conjunto $\mathbb{A}$. Sea ahora $q_0, q_1, q_2, \ldots$ la sucesión numerable de los números racionales, con $q_0 = 0$. Construyamos los conjuntos $\mathbb{A}_{0,} = q_0+\mathbb{A}$, $\mathbb{A}_1 = q_1 + \mathbb{A}, \ldots, \mathbb{A}_n = q_n + \mathbb{A}, \ldots$. Estos conjuntos son disjuntos y su unión es $[0, 1]$. Si tomamos como probabilidad la medida de Lebesgue (la longitud), entonces todos son equiprobables. Como $\cup_{n=0}^{\infty}\mathbb{A}_n = [0, 1]$, por la propiedad (sigma) aditiva de la probabilidad

$$\Pr(\bigcup_{n=0}^{\infty}\mathbb{A}_n) = \sum_{n=0}^{\infty}\Pr(\mathbb{A}_n) = \Pr([0, 1]) = 1.$$

Si cada probabilidad fuera positiva obtendríamos $\infty = 1$. Si cada probabilidad fuera cero obtendríamos $0 = 1$. Esto es imposible, luego $\mathbb{A}$ es un conjunto que carece de probabilidad.

Un conjunto sin probabilidad, interpretado bajo una perspectiva estadística, significa que no es observable. Luego no podemos repetir una experiencia para registrar la frecuencia de este suceso. Es decir, es un conjunto

que existe pero que no es observable. Véase la figura 3.1. Sin embargo, rechazando el axioma de elección y aceptando el axioma de Solovay, todo subconjunto de $\mathbb{R}$ posee probabilidad (es medible en el sentido de Lebesgue).

3.2 Modelos estadísticos univariantes

En estadística matemática se trabaja con modelos estadísticos. En su versión probabilística, un modelo estadístico es una familia de funciones de densidad dependientes de un parámetro: $f(x, \theta)$ ó $f_\theta(x)$. Por ejemplo

$$f_\theta(x) = \theta \exp(-\theta x), \qquad \text{para } x, \theta > 0, \tag{3.1}$$

es una familia de densidades exponenciales. Este modelo no incluye otras densidades, como la normal.

Nos preguntamos ahora si es posible indexar todas las leyes de probabilidad. Estudiemos el caso de variables aleatorias univariantes. Nos limitaremos a las uni-paramétricas. Excluimos, por ejemplo, la distribución normal que depende de dos parámetros. No obstante, una ligera modificación de la demostración que sigue, permitiría incluir modelos multi-paramétricos.

Propiedad 25 *No existe un modelo estadístico que incluya a todas las leyes de probabilidad univariantes.*

Prueba. Supongamos que las funciones de distribución se pueden indexar. Sea F_θ una función de distribución. Podemos suponer que θ pertenece al soporte de F_θ y que este soporte es $\mathbb{R}$, común a todas las distribuciones.

La función F_θ corresponderá a una variable aleatoria X_θ sobre un cierto espacio de probabilidad, cuyo suceso seguro es Ω. Sabemos que X_θ puede tomar el valor θ. Definamos el suceso

$$\mathbb{A}_\theta = \{\omega \text{ tal que } X_\theta(\omega) = \theta\}.$$

Sea entonces la aplicación $X : \Omega \to \mathbb{R}$ definida como

$$X(\omega) = X_\theta(\omega) + 1 = \theta + 1 \quad \text{ si } \omega \in \mathbb{A}_\theta.$$

Puesto que

$$\bigcup_\theta \mathbb{A}_\theta = \Omega,$$

todo ω tiene imagen $X(\omega)$ en $\mathbb{R}$. Vemos que

$$X(\omega) = \theta + 1 \neq X_\theta(\omega) = \theta \text{ si } \omega \in \mathbb{A}_\theta.$$

Luego X es una variable aleatoria distinta de X_θ para cada θ en al menos el suceso $\mathbb{A}_\theta$.

Por otra parte la función de distribución de X verifica

$$dF(x) = dF_{x-1}(x-1) \neq dF_x(x).$$

Es decir, F difiere de F_x en al menos el punto x de la recta real $\mathbb{R}$. Luego F no pertence a la lista de funciones de distribución indexadas por θ.

Incluso, si consideramos una clase más restringida podría no existir una parametrización. Consideremos por ejemplo las distribuciones de probabilidad con soporte el intervalo $[0,1]$, es decir, $F(0) = 0 \leq F(x) \leq 1 = F(1)$.

Propiedad 26 *No existe un modelo estadístico que incluya todas las distribuciones estrictamente crecientes $F(x)$ con soporte en $[0,1]$.*

Prueba. Vamos a restringirnos a la subclase $\mathbb{G}$ de distribuciones tales que $F(x) > x$. Supongamos que esta subclase se puede parametrizar mediante θ siendo $0 \leq \theta \leq 1$. Sea F_θ una distribución de $\mathbb{G}$. Entonces $F_\theta(x) > x$.

Definimos la nueva distribución $G(x) = \alpha F_x(x) + (1-\alpha)x$, con $0 < \alpha < 1$ tal que $G'(x) > 0$. Entonces $G(0) = 0$, $G(1) = 1$, G es una distribución que verifica $G(x) > \alpha x + (1-\alpha)x = x$, y que podría pertenecer a $\mathbb{G}$. Supongamos $G = F_\theta$ para algún θ. Entonces $G(\theta) = \alpha F_\theta(\theta) + (1-\alpha)\theta = F_\theta(\theta)$ implicaría $G(\theta) = \theta$, lo que contradice la propiedad $G(x) > x$. Luego G no pertenece a $\mathbb{G}$. Es decir, G no pertenece a la lista de funciones de distribución indexadas por θ. Si $\mathbb{G}$ no puede parametrizarse, tampoco admite parametrización la clase más amplia del enunciado.

Nota. Esta propiedad y su demostración tipo "diagonal", guarda una cierta similitud con el teorema de Gödel. Al introducir la familia F_θ estamos enunciando una propiedad que se define mediante un parámetro. Sin embargo, hay distribuciones que existen pero que no tienen esta propiedad, permaneciendo fuera del hipotético modelo estadístico.

Vale también la pena notar que en estadística el parámetro θ es desconocido y que debe estimarse tomando una muestra de la variable aleatoria. Podemos afirmar que $X_\theta(\omega) = \theta$ es matemáticamente posible, pues θ es uno de los valores que toma la variable. Sin embargo $X_\theta(\omega) = \theta$ no es observable. La estadística es una matemática experimental basada en la observación de sucesos, es decir, se debe poder decidir si un suceso se presenta o no tras realizar una experiencia. Para conciliar ambos enfoques matemático y estadístico y dar validez a la demostración anterior, podemos considerar cada suceso $\mathbb{A}_\theta$ para un valor fijado y por lo tanto conocido (por ejemplo, $\theta = 0,27$), del parámetro θ.

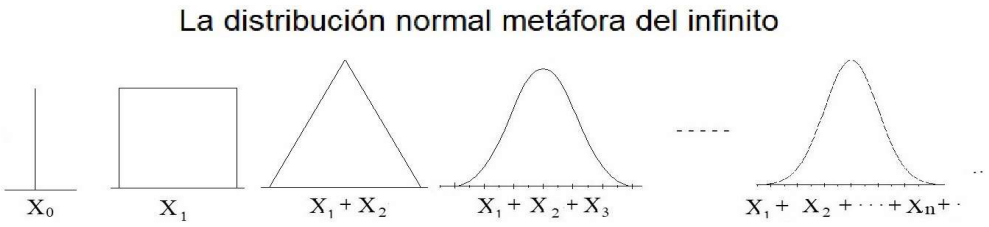


Figura 3.2: El teorema central del límite es un resultado estadístico importante que ilustra la sucesión 0, 1, ..., n, ..., ω. El ordinal ω correspondería a la distribución normal.

3.2.1 El teorema central del límite

En probabilidad y estadística es de gran interés la distribución del límite de una suma de variables aleatorias. Si la suma está estandarizada, bajo ciertas condiciones, su distribución de probabilidad tiende a la ley normal. Esta propiedad nos permite ilustrar la sucesión

$$0 < 1 < 2 < 3 < \cdots < n < \cdots < \omega$$

En efecto, supongamos que X_1 es una variable aleatoria con distribución uniforme. Su densidad viene representada por una recta horizontal. Consideremos otra variable aleatoria X_2, independiente de la primera, y consideremos la suma $X_1 + X_2$. Procediendo de esta manera, tenemos la sucesión

$$X_0,\ X_1,\ X_1 + X_2,\ X_1 + X_2 + X_3, \cdots, X_1 + \cdots + X_n, \cdots, \text{Ley normal},$$

donde por conveniencia X_0 es la constante 0. Se supone que cada variable suma se ha estandarizado restando la media y dividiendo por la desviación típica. La distribución límite es la conocida **distribución normal** o de Gauss, que cumpliría, en este caso, el papel de ω, véase la figura 3.2. Otro ejemplo de sucesión $0, 1, \ldots, \omega$ puede verse en la figura 5.1.

3.3 Modelos estadísticos bivariantes

Desde que Galton y Pearson fundaran la teoría de la regresión y correlación, han aparecifdo numerosos modelos o leyes de probabiliodad capaces de relacionar dos variables aleatorias.

Las llamadas "cópulas" son la base de estos modelos. Una cópula es una función de distribución acumulativa de dos variables con marginales uniformes y se indica por $C(u, v)$.

Se puede probar que, en genral, toda cópula admite la expansión

$$dC(u, v) = dudv + \sum_{n\geq 1} \rho_n a_n(u) b_n(v) dudv, \tag{3.2}$$

donde $\mathbb{S} = \{\rho_1, \rho_2, \ldots, \rho_n, \ldots\}$ se conoce como sucesión de correlaciones canónicas. Hay justificación geométrica para definir el rango (o dimensión) de la cópula C como el cardinal de $\mathbb{S}$. Entonces todos los cardinales están representados en las cópulas. La teoría de los cardinales finitos y transfinitos, tiene significado en un campo tan distinto como el de las distribuciones estadísticas de dos variables.

1. La llamada cópula de independencia $C(u, v) = uv$, tiene rango 0. Es decir, $\text{car}(\mathbb{S}) = 0$, pues $\mathbb{S}$ está vacío.

2. La llamada cópula FGM (de Farlie-Gumbel-Morgenstern)

$$C_\theta(u, v) = uv + \theta u(1 - u)v(1 - v), \quad -1 \leq \theta \leq 1, \tag{3.3}$$

   tiene rango 1. Es decir, $\text{car}(\mathbb{S}) = 1$, pues $\mathbb{S} = \{\theta/3\}$.

3. La cópula

$$C(u, v) = uv + \lambda_1 u(1 - u)v(1 - v) + \lambda_2(2u - 1)u(1 - u)(2v - 1)v(1 - v)$$

   tiene rango 2. Es decir, $\text{car}(\mathbb{S}) = 2$, pues $\mathbb{S}$ contiene dos correlaciiones canónicas.

4. La llamada cópula AMH (de Ali-Mikhail-Haq)

$$C_\theta(u, v) = uv/\left[1 - \theta(1 - u)(1 - v)\right], \quad -1 \leq \theta \leq 1,$$

   tiene rango infinito numerable. Es decir, $\text{car}(\mathbb{S}) = A_0$.

5. La llamada cópula CA (de Cuadras-Augé)

$$C_\theta(u, v) = \min\{u, v\}^\theta (uv)^{1-\theta}, \quad 0 \leq \theta \leq 1,$$

   tiene rango infinito no numerable. Es decir, $\text{car}(\mathbb{S}) = c$.

La cópula CA rompe con lo conocido hasta hace poco tiempo: las cópulas o distribuciones bivariantes tienen rango finito o infinito numerable. Sin embargo, para esta cópula no es aplicable el desarrollo (3.2). Sustituyendo la suma por una integral, para estacópula se aplicaría la expansión

$$C_\theta(u,v) = uv + \int_{Q(u,v)}^{1} f_\theta(\rho)(u/\rho)(v/\rho)d\rho,$$

donde $Q(u,v) = \max\{u,v\}$ y $f_\theta(\rho)$ es una función de correlación canónica. En el caso CA es $f_\theta(\rho) = \theta\rho^{1-\theta}$, con ρ variando entre 0 y 1. Luego $\mathbb{S}$ contiene una infinidad no mumerable de correlaciones canónicas.

En las cópulas el parámetro θ suele medir el grado de dependencia estocástica entre las variables aleatorias relacionadas. No es posible indexar todas las cópulas mediante un único paránetro.

Propiedad 27 *No existe un modelo estadístico que incluya a todas las leyes de probabilidad bivariantes.*

Prueba. Puesto que toda distribución bivariante puede ser generada por una cópula, nos limitaremos a las cópulas y nos restrimgiremos a las llamadas cópulas con Dependencia Cuadrante Positiva estrica (DCP), que son las que cumplen la propiedad

$$C(u,v) > uv \quad \text{para todo } 0 < u,v < 1.$$

Supongamos ahora que las cópulas DCP se pueden indexar con un único parámetro θ. Al ser cópulas DCP este parámetro medirá el grado de dependencia positiva. Una cópula indexada se indicará por C_θ. Supondremos que el parámetro verifica $0 < \theta < 1$, y que el soporte de $C_\theta(u,v)$ es el cuadrado $[0,1]\times[0,1]$. La parametrización se consigue mediante una reparametrización adecuada, si es necesario. Convendremoa que $C_0(u,v) = uv$ y que $C_1(u,v) = \min\{u,v\}$ y a partir de ahora comsideraremos solo el intervalo abierto $0 < \theta < 1$.

Definamos una nueva función C mediante la mixtura

$$C(u,v) = \alpha C_u(u,v) + (1-\alpha)uv,$$

y supongamos que C es una cópula. Esta C obtenida a partir de C_θ es DCP pues

$$\alpha C_u(u,v) + (1-\alpha)uv > \alpha uv + (1-\alpha)uv = uv.$$

En lo sucesivo nos retringiremos a la subclase $\mathbb{F}_\theta$ de cópulas C_θ que son DCP y que $C(u,v)$ es también una cópula para un α fijo apropiado.

Ahora bien, si suponemos $C = C_\theta$ para algún θ, entonces $C(\theta, v) = C_\theta(\theta, v)$, y resultaría que

$$\alpha C_\theta(\theta, v) + (1 - \alpha)\theta v = C_\theta(\theta, v)$$

implicaría $C_\theta(\theta, v) = \theta v$, lo que contradice la propiedad DCP de C. Debemos admitir que $C(\theta, v) \neq C_\theta(\theta, v)$, es decir, C difiere de C_θ en los puntos (θ, v). Luego C no puede formar parte de la familia de cópulas indexadas mediante θ, es decir, C no pertenece a $\mathbb{F}_\theta$. En otras palabras, esta subclase restringida no puede indexarse. Con mayor motivo, otras clases más amplias tampoco pueden indexarse. La demostración sería análoga si suponemos que θ es un parámetro de dimensión dos.

Para una exposición de las distribuciones con rango (dimensión geométrica) infinito no numerable, véase Cuadras (2015), Cuadras *et al.* (2019).

3.4 Analogía transfinita de la distribución normal

Supongamos que X sigue la distribución normal, vista como un límite (figura 3.2). Indiquemos por [normal] la clase de equivalencia de todas las variables con distribución normal obtenidas por transformación lineal de X. Similarmenete podemos definir las clases [Laplace] y [logística]. En general, [todas] es la familia de variables aleatorias con dominio en $\mathbb{R}$. Entonces el cardinal de [normal] es c (indicado por A_1) y el de [todas] es f (indicado por A_2). Sea [normal, normal] el conjunto de vectores (X, Y) con distribución normal bivariante. Similarmente [todas, todas]. Como $X + q$ (con $q \in \mathbb{Q}$) y $X + Y$ son también normales, y si Z no es normal, $X + Z$ tampoco. Similarmente procederíamos con la familia de vatiables Poisson de parámetro entero, que tiene cardinal A_0. Se puede pues establecer una semejanza entre operaciones con variables aleatorias y con cardinales.

Variables aleatorias	Cardinales
[Poisson]+[Poisson]=[Poisson]	$A_0 + A_0 = A_0$
[normal] + [racional] = [normal]	$A_1 + A_0 = A_1$
[normal] + [normal] = [normal]	$A_1 + A_1 = A_1$
[normal] + [todas] = [todas]	$A_1 + A_2 = A_2$
[normal, normal] = [bivariante normal]	$A_1 \times A_1 = A_1$
[todas, todas] = [bivariante todas]	$A_2 \times A_2 = A_2$

Analogías del mismo tipo se cumplen para las llamadas distribuciones estables, como la Cauchy, pues la suma de dos variables independientes Cauchy es también Cauchy. Es decir, [Cauchy] + [Cauchy] = [Cauchy], se relaciona con $A_1 + A_1 = A_1$.

Capítulo 4

El principio de elección

El tema de comparación y ordenación de infinitos se resuelve bastante bien si aceptamos el axioma de elección. Este axioma (postulado o principio), había sido aceptado implícitamente en análisis y teoría de conjuntos.

4.1 Enunciado del axioma

Axioma de elección. Sea $\mathcal{C}$ una colección de conjuntos no vacíos. Existe un conjunto $\mathbb{A}$ que contiene un elemento de cada uno de los conjuntos de la colección $\mathcal{C}$.

Veamos dos ejemplos sencillos (debidos a B. Russell), donde intervien el axioma de elección (AE):

a) Una colección de pares de zapatos.

b) Una colección de pares de calcetines.

En a) podemos construir un conjunto de zapatos eligiendo los del pie izquierdo. En este caso no es necesario el AE. En b) no distinguimos el calcetín del pie izquierdo del calcetín del pie derecho. Para obtener un conjunto con un calcetín de cada par necesitaremos recurrir al AE.

La figura 4.1 ilustra dos ejemplos geométricos del AE. En la figura 4.1 (izquierda) tenemos un haz de elipses concéntricas. Aunque hay infinitas elipses, podemos elegir un punto de cada una sin necesidad del AE. Basta tomar el punto derecho que resulta de cortar las elipses por una recta horizontal y tomar el punto de corte situado a la derecha. Es fácil encontrar estos punos analíticamente. En efecto, los puntos situados a la derecha que cortan a la semirrecta $y = 3$ tienen coordenadas $(x, 3)$, con $x > 3$.

En la figura 4.1 (derecha) vemos curvas cerradas no concéntricas. Si consideramos todas las curvas cerradas del plano, no hay ningún proced-

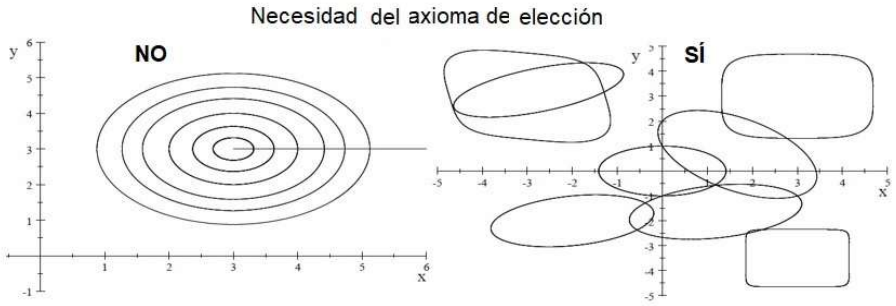


Figura 4.1: Izquierda: Para elegir un punto de cada una de las elipses concéntricas no necesitamos el axioma de elección. Derecha: Para elegir un punto de cada una de las curvas cerradas del plano necesitamos el axioma de elección.

imiento geométrico o analítico que permita seleccionar un punto de cada curva. Quizás podríamos considerar el punto que está arriba. Pero muchas curvas tienen infinitos puntos situados "arriba" de la curva. Los rectángulos, por ejemplo. Entonces, para construir un conjunto conteniendo un punto de cada curva necesitamos utilizar el AE.

El AE facilita el desarrollo de la teoría de conjuntos. Gödel (1940) y Cohen (1963), probaron su independencia de los otros axiomas. Por lo tanto, se pueden elaborar teoremas matemáticos sin el AE o con el AE.

El AE tiene ventajas. Todo conjunto puede ser bien ordenado si lo aceptamos, y todo espacio vectorial tiene una base.. Además, aceptar la hipótesis generalizafa del continuo (HGC) implica el AE.

Empero tiene inconvenientes. Hay colecciones de conjuntos relativamente sencillas en los que no sabemos cómo aplicar el AE. Por ejemplo, todos los subconjuntos de la recta real. ¿Cómo elegir un número de cada subconjunto? Enseguida se nos ocurre tomar el mínimo, pero el intervalo $(0, 1)$ no tiene mínimo perteneciemdo a dicho intervalo. Consideremos ahora el espacio vectorial $\mathbb{R}$ sobre $\mathbb{Q}$. Los elementos de $\mathbb{R}$ son vectores y los de $\mathbb{Q}$ son escalares. Como consecuencia del AE este espacio vectorial posee una base, pero todavía no se ha podido encontrar. Además, si aceptamos el AE, hay subconjuntos de $\mathbb{R}$ que no son medibles, es decir, sin longitud. Hay también sucesos sin probabilidad (véase la figura 3.1). Sin embargo, si se rechaza el AE y se acepta el axioma de Solovay (propuesto en 1970), resulta que todos los subconjuntos de $\mathbb{R}$ son medibles.

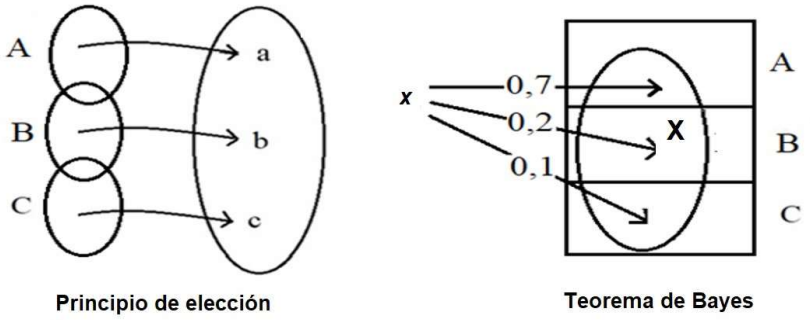


Figura 4.2: El principio de elección postula que podemos formar un nuevo conjunto eligiendo un elemento de cada conjunto de una colección de conjuntos. En determinadas circunstancias este conjunto existe pero no se puede observar experimentalmente. El teorema de Bayes proporciona la probabilidat de que una observación elemental, que verifique ciertas características (indicadas por X), proceda de una causa determinada.

4.2 Relación con el teorema de Bayes

Consideremos ahora un enunciado en cierta manera recíproco del principio de elección. Supongamps que un conjunto seguro **S** es la reunión disjunta de varios sucesos (conjuntos observables), llamados causas (véase la sección 6.1.2). Sea x un suceso elemental obtenido como el resultado de una experiencia E. Supongamos que x pertenece al conjunto X, que es subconjunto observable de **S**. El teorema de Bayes nos proporciona la probabilidad de que x provenga de una causa determinada. Por lo tanto, si el axioma de elección afirma que podem encontrar un conjunto A que contenga un elemento de cada causa, el teorema de Bayes, dado un elemento x que pertenece a X, nos permite calcular el grado de pertenencia a cada una de las causas.Véase la figura 4.2.

4.3 Teorema de Banach-Tarski

Es interesante por lo sorprendente, mencionar la paradoja o teorema de Banach-Tarski que contradice la intuición geométrica. El teorema afirma que admitiendo el AE, una bola sólida se puede dividir en partes (no medibles) y volver a ensamblarlas para formar dos bolas de igual tamaño que la inicial.

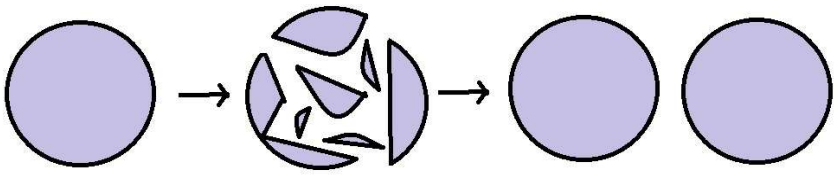


Figura 4.3: Ilustración del teorema de Banach-Tarski. Si se admite el principio de elección, se puede seccionar una bola en diversos trozos y luego ensamblarlos para construir dos bolas iguales a la inicial.

Véase la figura 4.3 y el artículo de Ara (2020). Su enunciado formal es:
Teorema de Banach-Tarski. Sea **B** una bola del espacio. Podemos descomponer **B** en piezas disjuntas

$$\mathbf{B} = A_1 \cup \cdots \cup A_m \cup B_1 \cup \cdots \cup B_n,$$

de modo que

$$\mathbf{B} = A_1^* \cup \cdots \cup A_m^* \text{ y también } \mathbf{B} = B_1^* \cup \cdots \cup B_n^*,$$

donde A_i^* y B_i^* son transformaciones isométricas de A_i y B_i.

Por aplicación reiterada de este teorema, se podría afirmar.que partiendo y luego ensamblando las partes de un guisante, podemos construir una bola del tamaño del Sol.

4.4 Funciones propias de un operador integral*

Para finalizar, comentemos una aplicación avanzada del principio de elección. Sean K y L dos operadores integrales. Integrando se definen los productos internos $(\varphi, K\phi)$ y $(\varphi, L\phi)$

$$(\varphi, K\phi) = \int K(u,v) d\varphi(u) d\phi(v)$$

y similarmente $(\varphi, L\phi)$. Entonces se dice que ψ es función propia de K con respecto a L de valor propio λ si

$$(\psi, K\psi) = \lambda(\psi, L\psi).$$

Se puede probar que existe al menos un valor propio. En general, los valores propios forman un conjunto numerable. Pero puede ocurrir que este

conjunto tenga la potencia del continuo. Entonces los valores propios se obtienen estudiando el cociente $(\psi, K\psi)/(\psi, L\psi)$. Obsérvese que $(\psi, L\psi)$ es una norma.

Propiedad 28 *Sea $\mathbb{S}_\lambda$ el conjunto de valores propios de K con respecto a L. Supongamos $\mathbb{S}_\lambda$ conjunto infinito no numerable. Entonces las funciones propias verifican $(\psi, L\psi) = 0$ salvo (posiblemente) para un conjunto finito. Además,* $\inf \mathbb{S}_\lambda = 0$.

Es decir, salvo un número finito de valores propios (quizás ninguno), todos los valores propios y funciones propias forman un conjunto **no numerable**, donde cada función propia tiene norma 0. Para probar esta propiedad se utiliza el axioma de elección y ciertos resultados avanzados del análisis funcional. Véase el teorema 5 en Cuadras (2015).

4.5 Visión estadística sobre Gödel y Turing

La aserción demostrada ‘por Gödel de que en un sistema axiomático (que incluya la aritmética), no toda proposición es demostrable, se puede enfocar desde la perspectiva del teorema de Turing. Dicho teorema dice que no existe un algoritmo (que pueda programarse) capaz de decidir si todo algoritmo (o programa) finaliza en un tiempo finito o no. Si codificamos un sistema axiomático y sus proposiciones, y lo convertimos en un algoritmo, la incapacidad de saber si finalizará en un tiempo finito, equivaldría a decir que es indecidible. Enunciemos este resultado que admite una demostración “estadística”.

Propiedad 29 *No hay ningún algoritmo general que permita saber si un programa se ejecutará en un tiempo finito.*

Un algoritmo programado es una sucesión de bits (ceros y unos). Hay 2^n sucesiones distintas de n bits. Asignemos a cada algoritmo de longitud n bits la probabilidad $1/2^n$. Supongamos que a_n es el número de programas de n bits que se ejecutan en un tiempo finito (ETF). Si elegimos un programa al azar, la probabilidad de que sea ETF es

$$\Omega = \sum_n a_n/2^n.$$

Si $\Omega = 0$ ningún programa es ETF. Si $\Omega = 1$ todos los programas son ETF. Se puede probar (véase Chaitin , 1991 y las referencia que contiene),

que Ω no es una probabilidad fija, es una probabilidad aleatoria, que se comporta (en base 2) como si sus bits estuvieran elegidos al azar echando una moneda.

Intentando determinar Ω y salir de dudas, podríamos entender Ω como una variable aleatoria, asignarle una distribución de probabilidad y plantear la estimación de Ω desde una perspectiva bayesiana. Pero éste no es el caso. Si escribimos Ω en base binaria, cada bit es independiente de los demás y es irreductible. Para determinar los n primeros bits de Ω hace falta un programa de n bits, de complejidad igual a lo que tratamos de calcular, y a partir de n no es posible seguir adelante.

Al ser Ω algorítmicamente aleatorio, no podemos precisar cuantos programas son ETF. Es decir, de todos los programas, resulta que ninguno, algunos, muchos o todos, se pueden ejecutar en un número finito de etapas. Es una incertidumbre esencial que convierte el problema en indecidible. Por cierto, Chaitin utiliza el símbolo Ω por considerar que es una probabilidad "mística", que contiene toda la verdad matemática constructiva.

4.6 Versión estadística de Banach-Tarski

Si X es una variable aleatoria normal, se puede poner como $X = X_1 + X_2$, donde X_1 y X_2 son también normales independientes. Además:

Propiedad 30 *Si X es una variable aleatoria con media y varianza finitas tal que $X = (X_1 + X_2)/\sqrt{2}$, siendo X_1 y X_2 independientes con la misma distribución que X, entonces X es normal.*

Prueba. Es inmediato ver que la media de X es 0. Sean $X_1, \ldots, X_n$ independientes con la misma distribución que X. Entonces

$$\frac{X_1 + X_2}{\sqrt{2}} \quad \text{y} \quad \left(\frac{X_1 + X_2}{\sqrt{2}} + X_3\right)/\sqrt{2}$$

siguen la misma distribución que X. En general, sigue esta distribución

$$\frac{X_1 + X_2}{\sqrt{2^{n-1}}} + \frac{X_3}{\sqrt{2^{n-2}}} + \cdots + \frac{X_n}{\sqrt{2}}.$$

Por el teorema central del límite la distribución de X es normal.

Con las mismas notaciones de la sección 3.4, podemos afirmar que la clase [normal] se descompone en la suma de dos clases disjuntas e independientes, es decir, [normal] = [normal]$_1$ + [normal]$_2$. Un argumento parecido con la distribución de Poisson, probaría que [Poisson] = [Poisson]$_1$ + [Poisson]$_2$. Vemos que hay una cierta similitud con el teorema de Banach-Tarski.

Capítulo 5

Los números ordinarios

En este capítulo presentamos y estudiamos la construcción lógica de los números enteros y racionales partiendo de los números naturales.

5.1 Los números naturales

El conjunto $\mathbb{N} = \{0,\ 1,\ 2,\ 3, \ldots, n, \ldots\}$ se puede introducir utilizando los axiomas de Peano. Sin embargo supondremos este conjunto bien conocido y nos propondremos una construcción axiomática coherente. Tiene un elemento neutro para la suma llamado cero, y otro elemento neutro para la multiplicación llamado uno. Supondremos como acciones naturales el contar y la frase "tantas veces".

Definición 1 *El conjunto* $\mathbb{N} = \{0,\ 1,\ 2,\ 3, \ldots, n, \ldots\}$ *es el conjunto natural de números que surge para contar objetos, y entonces el primer elemento es el uno, que indicamos por* 1*, o para descontar objetos, y entonces al quedarnos sin objetos lo cuantificamos con el cero, que indicamos por* 0*.*

Axioma 1 *El* 0 *es un número natural.*

Axioma 2 *Todo número natural* n *tiene un siguiente, indicado por* n^+*.*

Axioma 3 *El* 1 *es el número natural siguiente del* 0*.*

Axioma 4 *El* 0 *no es el siguiente de ningún número natural.*

Axioma 5 *Si un conjunto de números naturales contiene al* 0 *y si contiene a* n *también contiene al siguiente de* n*, entonces es el conjunto* $\mathbb{N}$ *de todos los números naturales.*

Escolio. Este axioma se denomina **principio de inducción matemática**. Si se considera que los números naturales comienzan con el 1, entonces el principio se enuncia cambiando el 0 por el 1.

Definición 2 *Si a y b son números naturales, la* ***suma*** $a+b$ *es el número natural que se obtiene tomando el siguiente de a un total de b veces.*

Definición 3 *Si a y b son números naturales, la* ***multiplicación*** *(o producto) $a \times b$ es el número natural que se obtiene sumando el número a un total de b veces. Indicaremos también el producto por ab.*

Definición 4 *Si a y b son números naturales y $b = a + c$, donde c no es 0, entonces a es* ***menor*** *que b, lo que indicaremos por $a < b$.*

Definición 5 *Si a y b son números naturales y $a = b + c$ donde c no es 0, entonces a es* ***mayor*** *que b, lo que indicaremos por $a > b$.*

Definición 6 *Si $a = b$ ó $a > b$ podemos considerar la* ***diferencia*** *a menos b, que indicaremos por $a - b$.*

Proposición 1 *El 0 es el elemento neutro para la suma y el 1 es el elemento neutro para la multiplicación. Es decir, $a + 0 = a$, $a \times 1 = a$.*

Prueba. Resulta evidente por la definición de suma y multiplicación.

Proposición 2 *El siguiente del número natural n que hemos indicado por n^+, se puede interpretar como la suma de n y 1, es decir, $n^+ = n + 1$.*

Prueba. Es evidente por la definición 2.

Proposición 3 *Si a y b son números naturales tales que $a+b = 0$ entonces ambos números son iguales a 0.*

Prueba. Si a no es 0 y b es 0, por la proposición 1, $a + 0 = a = 0$ quedando demostrado. Si ambos no son 0 entonces por la definición 2, $a+b$ se obtiene tomando b veces el siguiente de a. Pero suponer esto contradice el axioma 4.

Veamos a continuación que el conjunto $\mathbb{N}$ admite una buena ordenación.

Proposición 4 *El conjunto* $\mathbb{N} = \{0, 1, 2, 3, \ldots, n, \ldots\}$ *está* ***bien ordenado*** *en el sentido de que, si* $a < b$ *y* $b < c$ *entonces* $a < c$*. Indicaremos esta buena ordenación por*

$$0 < 1 < 2 < \cdots < n < n + 1 < \cdots$$

Prueba. Si $a < b$ por la definición 4, $b = a + b'$. Análogamente si $b < c$ entonces $c = b+c'$. Pero $b = a+b'$. Luego $c = b+c' = (a+b')+c' = a+(b'+c')$ y por lo tanto $a < c$.

Además, por el axioma 3 y la proposición 2, $1 = 0 + 1$ luego $0 < 1$. El número 2 es el siguiente del 1, es decir, $2 = 1 + 1$, luego $1 < 2$. Y así sucesivamente.

Proposición 5 *La suma del cero y de los* n *siguientes números naturales es* $n(n + 1)/2$

$$0 + 1 + \cdots + n = n(n + 1)/2.$$

Prueba. La fórmula es cierta para $n = 0$ y para $n = 1$. Supongamos cierta para un determinado n. Entonces si añadimos $n+1$ a la suma resulta que

$$(0 + 1 + \cdots + n) + (n + 1) = n(n + 1)/2 + (n + 1) = (n + 1)(n + 2)/2.$$

Luego también es válida la fórmula para $n + 1$. Por el axioma 5 la fórmula se cumple para todo número natural.

Definición 7 *Un número natural* a *distinto de cero es* ***compuesto*** *si se puede escribir como* $a = b \times c$ *donde* b *y* c *son distintos de* 1*. Se dice entonces que* b *y* c *son* ***divisores*** *de* a*.*

Definición 8 *Un número natural* p *es* ***primo*** *si no es compuesto. Un número primo no tiene divisores salvo el* 1*.*

Proposición 6 *Hay infinitos números primos.*

Prueba. Supongamos que sólo hay n. Sean $p_1, p_2, \ldots, p_n$ estos n números primos, donde $p_1 = 2$, $p_2 = 3$, etc. Consideremos el número natural

$$p = p_1 \times p_2 \times \cdots \times p_n + 1.$$

Entonces p es también un número primo distinto de los anteriores. Luego debe haber más de n, donde n puede ser arbitrariamente grande.

Proposición 7 *Todo número compuesto es producto de números primos.*

Prueba. Si $a = bc$ y b, c son primos el enuunciado queda probado. Si b no es primo entonces $b = b'c'$. Si b', c' son primos y también lo es c, el enunciado queda probado. Si b' es compuesto lo descomponemos en un producto y así sucesivamente. Como los factores que multiplican son cada vez menores, llegaremos necesariamente a un producto de números primos.

Definición 9 *Un número natural es* ***par*** *si es divisible por* 2 *Un número es* ***impar*** *si no es divisible por* 2*.*

Es evidente que todo número par a es compuesto y al ser divisible por 2 se puede escribir como $a = 2n$.

Definición 10 *Un conjunto* $\mathbb{A}$ *es* ***numerable*** *(o enumerable) si sus elementos se pueden poner en correspondencia uno-a-uno con el conjunto* $\mathbb{N}$ *de los números naturales o con algún subconjunto de* $\mathbb{N}$*. Entonces podemos indicar el conjunto* $\mathbb{A}$ *como*

$$\mathbb{A} = \{a_0, a_1, \ldots, a_n, \ldots\}.$$

Proposición 8 *El conjunto de los números pares es numerable.*

Prueba. Un número par cualquiera se puede expresar como $2n$. La correspomdemcia $n \leftrightarrow 2n$ es uno-a-uno, es decir, biyectiva.

Escolio. Siendo el conjunto de los números pares la "mitad" del conjunto $\mathbb{N}$, vemos sin embargo que ambos tienen el mismo número de elementos. Incluso el conjunto de los números primos, de magnitud inferior, es también numerable, Esta propiedad caracteriza a los conjuntos infinitos y los hace diferentes de los conjuntos finitos.

Conjetura 1 *Todo número par distinto de* 0 *es suma de dos números primos, es decir,*

$$2n = p + q,$$

siendo p *y* q *números primos.*

Aunque el 1 no se considera primo, vamos a tomarlo (sólo aquí) como un número primo. Vemos que

$$2 = 1 + 1,\ 4 = 2 + 2,\ 6 = 3 + 3,\ 8 = 3 + 5,\ 104 = 31 + 73,\ \text{etc.}$$

Esta propiedad fue enunciada por Goldbach (1741). Se ha comprobado ser cierta para números pares muy grandes, pero no se ha podido demostrar (siguiendo un proceso deductivo) para todo número par.

Proposición 9 *Los números primos mayores que* 3 *cumplen la ecuación* $p = 6n - 1$ *ó la ecuación* $p = 6n + 1$, *donde* n *es un número natural mayor que* 0.

Prueba. Los números $6n - 1$ y $6n + 1$ son impares. Cada tres números consecutivos hay uno divisible por 3. Luego el número anterior o posterior a un número primo es divisible por 2 y por 3, es decir, por 6.

Escolio. No todos los números primos se pueden generar mediante estas dos fórmulas, pues hay números $6n - 1$ ó $6n + 1$ que no son primos. Por ejemplo, $23 = 6 \times 4 - 1$ es primo pero $49 = 6 \times 8 + 1$ no es primo.

Dada la importancia de los números primos en la Aritmética, desde muy antiguo los matemáticos han buscado la fórmula que los genere todos. Se sabe que fijado n grande, la cantidad de primos menores que n es del orden de $n/\ln(n)$.

Definición 11 *La terna* (a, b, c) *de números naturales es pitagórica si*

$$a^2 + b^2 = c^2.$$

Proposición 10 *Hay infinitas ternas pitagóricas.*

Prueba. Un ejemplo de terna pitagórica es $(3, 4, 5)$. Supongamos que (a, b, c) es una terna pitagórica. Sea $n > 1$ un número natural cualquiera. Entonces (na, nb, nc) es otra terna pitagórica puesto que

$$n^2a^2 + n^2b^2 = n^2c^2.$$

Escolio. Los números naturales aparecen frecuentemente en contajes de animales, plantas, accidentes ocurridos, número de hijos por pareja, etc. Entonces los diferentes números 0, 1, 2, . . .tienen asignadas probabilidades cuyo estudio es de gran importancia en Estadística. Un modelo probabilístico, llamado distriibución de Poisson, es

$$\Pr(\text{observar } k) = e^{-\lambda}\frac{\lambda^k}{k!}, \qquad k = 0, 1, 2, \ldots,$$

donde λ es un parámetro positivo que indica el promedio ponderado de los posible números k.

Proposición 11 *Consideremos la colección de todos los conjuntos finitos. Existe una subcolección formada por un conjunto con solo un elemento, otro conjunto con solo dos elementos, otro con solo tres, y así sucesivamente.*

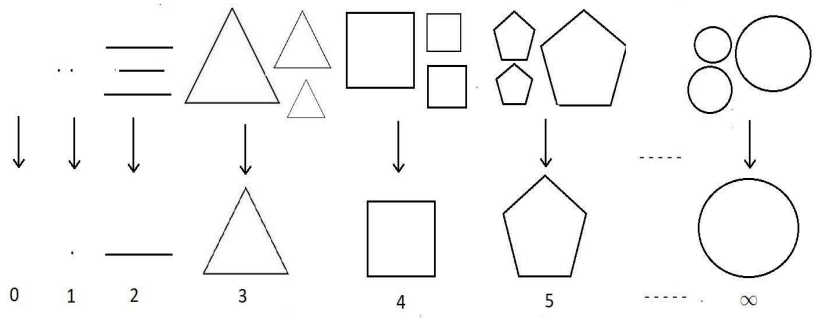


Figura 5.1: Aplicando el principio de elección, podemos seleccionar una clase de conjuntos formada por figuras de un punto, de dos vértices, de tres, de cuatro, de cinco, etc., de modo que tengamos una sola figura para cada colección de polígonos. El límite de estos polígonos se identifica con una circunferemcia (infinitos vértices), aunque no da lugar a la circunferencia completa.

Prueba. La existencia de $\{a\}, \{a, b\}, \{a, b, c\}$, etc., es consecuencia del principio de elección.

Escolio. Esta proposición enfrenta la matemática con la metafísica y es una antinomia, un conflicto (para un filósofo, no para un matemático) entre número y realidad. En efecto, si n es un número natural extremadamente grande, no podemos manejar conjuntos físicos con tantos elementos. Nos vemos obligados a usar la imaginación y estamos limitados a considerar sólo conjuntos geométricos de invención matemática. Por ejemplo, tomemos las figuras con un solo punto, los segmentos con dos extremos, los triángulos, los rectángulos, los pentágonos, etc., para poder seleccionar una figura de uno, dos, tres, cuatro o cinco vértices, etc. Obsérvese que el límite de un polígono regular con n vértices, es la circunferencia, que juega el papel de infinito absoluto para este tipo de figuras geométricas. Véase la figura 5.1. Notemos que mientras el límite de los polígonos es numerable, la circunferncia completa es continua y no numerable. Véase la sección 2.2.

Terminemos esta sección observando que si es $a > b$, entonces no existe la diferencia $b - a$ dentro del conjunto $\mathbb{N}$. Es decir, la ecuación lineal

$$a + x = b \quad \text{siendo } b < a,$$

carece de solución en $\mathbb{N}$. Debemos ampliar este conjunto para poder restar sin inconvenientes y conseguir resolver esta ecuación.

5.2 Los números enteros

Nos proponemos construir el conjunto

$$\mathbb{Z} = \{\ldots - n, \ldots, -3, \ -2, \ -1, \ 0, +1, +2, +3, \ldots, +n, \ldots\}$$

.de los números enteros partiendo exclusivamente de los números naturales.

Consideremos el conjunto producto $\mathbb{N} \times \mathbb{N}$. Entre sus elementos (a, b) definimos la relación de equivalencia

$$(a, b)R(a', b') \quad \text{si } a + b' = b + a'.$$

En términos monetarios, podemos interpretar (a, b) como lo que tenemos (igual a a) junto con lo que debemos (igual a b).

Definición 12 *El conjunto $\mathbb{Z}$ de los números enteros es el conjunto cociente*

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/R.$$

Definición 13 *Sobre este conjunto definimos la suma:*

$$(a, b) + (c, d) = (a + c, b + d), \tag{5.1}$$

y la multiplicación

$$(a, b) \times (c, d) = (ac + bd, ad + bc). \tag{5.2}$$

Definición 14 *A los enteros (a, b) tales que $a > b$ les llamaremos **positivos**. Como (a, b) es equivalente a $(a - b, 0) = (a', 0)$, lo indicaremos como $+a'$.*

Definición 15 *A los enteros (a, b) tales que $a < b$ les llamaremos **negativos**. Como (a, b) es equivalente a $(0, b - a) = (0, b')$, lo indicaremos como $-b'$.*

Definición 16 *A la clase de los enteros (a, a) la llamaremos **cero**. Es obvio que (a, a) es equivalente a $(a - a, a - a) = (0, 0)$.*

Definición 17 *A la clase de enteros $(a+1, a)$ la llamaremos **uno**. Es obvio que $(a + 1, a)$ es equivalente a $(a + 1 - a, 0) = (1, 0)$.*

Proposición 12 *El cero es elemento neutro para la suma y el uno lo es para la multiplicación.*

Prueba: Aplicando (5.1)

$$(a,a)+(c,d)=(a+c,a+d) \text{ equivalente a } (c,d).$$

Aplicando (5.2), pero ahora utilizando el uno en su forma más simple $(1,0)$

$$(1,0)\cdot(c,d)=(1\cdot c+0\cdot d, 1\cdot d+0\cdot c)=(c,d).$$

Proposición 13 *La multiplicación de enteros positivos es un entero positivo.*

Prueba. Si (a,b) y (c,d) son positivos podemos sustituir (a,b) por $(a-b,0)=(a',0)$ y (c,d) por $(c-d,0)=(c',0)$. Utlizando (5.2) $(a',0)\cdot(c',0)=(a'c',0)$ que también es positivo.

Proposición 14 *El producto de dos enteros negativos es un entero positivo.*

Prueba. Si (a,b) y (c,d) son negativos podemos sustituir (a,b) por $(0,b-a)=(0,b')$ y (c,d) por $(0,d-c)=(0,d')$. Utlizando (5.2) $(0,b')\cdot(0,d')=(b'd',0)$ que es positivo.

Proposición 15 *El producto de un entero positivo por un entero negativo es un entero negativo.*

La prueba es similar a las dos anteriores. Obsérvese la demostración elegante y formal de las conocidas reglas "más por menos es menos" y "menos por menos es más".

Proposición 16 *El conjunto de los enteros positivos y el cero está en correspondencia biyectiva con los números naturales.*

Prueba. La correspondencia es

$$(0,0)\leftrightarrow 0,\ (1,0)\leftrightarrow 1,\ldots,(a,0)\leftrightarrow a.$$

Por este motivo al entero $+a$ le quitamos el signo $+$.

Proposición 17 *El conjunto $\mathbb{Z}$ de todos los enteros es nunerable.*

Prueba. Al cero $(a,a)=(0,0)$ le hacemos corresponder el 0 natural. Al entero positivo $(a,0)$ le hacemos corresponder el número natural 3^a. Al entero negativo $(0,b)$ le hacemos corresponder 2^b. Luego $\mathbb{Z}$ está en correspondencia con un subconjunto del conjunto $\mathbb{N}$ de los números naturales.

En virtud de las propiedades anteriores, podemos indicar

$$\mathbb{Z} = \{\ldots - n, \ldots, -3, \ -2, \ -1, \ 0, 1, 2, 3, \ldots, n, \ldots\}.$$

El conjunto $\mathbb{Z}$ con las operaciones suma y multiplicación tiene estructura algebraica de **anillo conmutativo**.

Finalizamos esta sección observando que si b no es un divisor de a, no existe el cociente a/b dentro del conjunto $\mathbb{Z}$. En otras palabras, no podemos resolver la ecuación

$$ax = b \quad \text{donde } a \text{ no es divisor de } b.$$

Debemos ampliar este conjunto para conseguir resolver esta ecuación y poder dividir sin inconvenientes.

5.3 Los números racionales

Los números racionales se definen como fracciones de números enteros. Vamos a establecer una defincón formal.

Consideremos el conjunto producto $\mathbb{Z} \times \mathbb{Z}'$, siendo $\mathbb{Z}' = \mathbb{Z} - \{0\}$. Definamos la relación de equivalencia

$$(a, b)R(a', b') \text{ si } a \cdot b' = b \cdot a'.$$

Definición 18 *El conjunto $\mathbb{Q}$ de los números racionales es el conjunto cociente*

$$\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}'/R.$$

*Dado el par (a, b) diremos que a es el **numerador** y b es el **denominador**.*

Definición 19 *Sobre el conjunto $\mathbb{Q}$ definimos la suma*

$$(a, b) + (a', b') = (ab' + a'b, bb'),$$

la multiplicación

$$(a, b) \cdot (a', b') = (aa', bb')$$

y la división

$$(a, b)/(a', b') = (ab', a'b).$$

Proposición 18 *Los elementos neutros para la suma y la multiplicación son el $(0, 1)$ y el $(1, 1)$, respectivamente.*

Prueba. Sumando: $(a,b)+(0,1)=(a,b)$. Multiplicando: $(a,b)\cdot(1,1)=(a,b)$.

Proposición 19 *El opuesto del racional* (a,b) *es el racional* $(-a,b)$ *y el recíproco de* (a,b) *es* (b,a) *si* $a\neq 0$.

Prueba.$(a,b)+(-a,b)=(ab-ab,bb')=(0,bb')$ que es equivalente a $(0,1)$. También $(a,b)\cdot(b,a)=(ab,ab)$ que es equivalente a $(1,1)$.

Proposición 20 *Dos racionales* (a,b) *y* (a',b') *se pueden representar mediante racionales con el mismo denominador.*

Prueba. Tales números son equivalentes a (ab',bb') y $(a'b,bb')$.

Definición 20 *Si* $q=(a,d)$, $q'=(b,d)$ *son dos números racionales con el mismo denominador* $d>0$, *diremos que* $q<q'$ *si* $a<b$.

Proposición 21 *Dados dos números racionales* $(a,b)<(c,d)$ *existe otro número racional comprendido entre ambos.*

Prueba. El número $[(a,b)+(c,d)]/2$ es racional y es mayor que (a,b) y menor que (c,d).

Corolario 3 *El conjunto* $\mathbb{Q}$ *de los números racionales es* ***denso***.

Prueba. Se entiende por denso la propiedad de existir infinitos números racionales entre dos números racionales distintos, aunque estén muy próximos. Por la proposición anterior, podemos constuir tantos numeros intermedios como queramos.

A pesar de ser $\mathbb{Q}$ denso, es un conjunto cuyos elementos se pueden enumerar.

Proposición 22 *El conjunto* $\mathbb{Q}$ *de los números racionales es numerable.*

Prueba. Si a cada racional positivo $(+a,b)$ le hacemos corresponder el número natural 3^a7^b y a cada racional negativo $(-a,b)$ le hacemos corresponder 2^a5^b, tenemos una correspondencia con un subconjunto de $\mathbb{N}$.

Puesto que $(a,b)=(a,1)/(b,1)$, los números racionales se indican por a/b.

El conjunto $\mathbb{Q}$ de los números racionales tiene estructura de **cuerpo conmutativo**. Nótese que las ecuaciones de segundo grado

$$x^2=2,\qquad 2x^2+x=3,$$

no tienen solución dentro del conjunto $\mathbb{Q}$. Debemos ampliar este conjunto con nuevos números, llamados reales (racionales e irracionales).

5.4 Los números reales

A partir de $\mathbb{N}$ hemos construido $\mathbb{Z}$ y a partir de $\mathbb{Z}$ hemos construido $\mathbb{Q}$, siguiendo en ambos casos un procedimiiento algebraico bastante sencillo. Vamos a construir el conjunto $\mathbb{R}$ de todos los números reales con la ayuda del concepto de sucesión de números racionales. Si en las construcciones anteriores han bastado ciertas propiedades básicas de la teoría de conjuntos, ahora necesitamos utilizar el concepto de límite de una sucesión.

El conjunto de los números reales amplía el de los racionales. Ya los griegos descubrieron que la diagonal del cuadrado unidad no era un número racional. Que $\sqrt{2}$ no es racional se prueba fácilmente por reducción al absurdo.

Consideremos ahora la sucesión $(1+1)^1$, $(1+1/2)^2$, $(1+1/3)^3$ y en general $(1+1/n)^n$. Se sabe que esta sucesión converge al número $e = 2,7182\ldots$ lo que indicamos como

$$(1+\tfrac{1}{n})^n \to e.$$

Aunque cada término $a_n = (1+1/n)^n$ es racional, el límite e no lo es.

Definición 21 *Una sucesión (a_n) de números racionales diremos que es* ***convergente*** *si*

$$|a_n - a_{n+m}| \to 0$$

para n tendiendo a infinito. Se dice también que (a_n) es una sucesión de Cauchy.

Escolio. Si el límite de la sucesión (a_n) es L, siendo L racional o no, se cumple

$$|a_n - a_{n+m}| < |a_n - L| + |a_{n+m} - L|\,.$$

Por lo tanto, si $a_n \to L$ debe ser necesariamente $|a_n - a_{n+m}| \to 0$.

Definición 22 *Dos sucesiones (a_n) y (b_n) son equivalentes si su diferencia tiende a cero, es decir*

$$a_n - b_n \to 0.$$

La relación de equivalencia viene a decir que ambas sucesiones tienen el mismo límite.

Definición 23 *Sea $\mathbb{S}$ al conjunto de todas las sucesiones convergentes de números racionales. El conjunto $\mathbb{R}$ de los números reales es el conjunto cociente*

$$\mathbb{S}/R.$$

Proposición 23 *En el conjunto* $\mathbb{R}$ *se pueden definir las operaciones suma, resta, multiplicación y división, siendo la división con numerador cualquiera y denominador distinto de cero.*

Prueba. Si definimos la suma de dos sucesiones (a_n) y (b_n) como la sucesión $(a_n + b_n)$, estamos sumando números racionales. La sucesión suma converge a la suma de dos números reales. Se procede análogamente con las demás operaciones aritméticas.

Proposición 24 *El conjunto* $\mathbb{R}$ *es denso. Dados dos números reales* α *y* β *siempre existe otro número real* γ *tal que* $\alpha < \gamma < \beta$.

Prueba. El número $\gamma = (\alpha + \beta)/2$ está comprendido entre α y β.

Proposición 25 *El conjunto* $\mathbb{R}$ *es no numerable.*

Prueba: Supongamos que el intervalo $[0, 1]$ es numerable, representado por la sucesión $\alpha_1, \ldots, \alpha_n, \ldots$. Podemos expresar α_n en base 2 como

$$\alpha_n = \sum_{k=1}^{\infty} \frac{a_{nk}}{2^k} \quad \text{donde } a_{nk} \in \{0, 1\}.$$

Sea el número real $0 \leq \beta \leq 1$

$$\beta = \sum_{k=1}^{\infty} \frac{(1 - a_{kk})}{2^k}.$$

Entonces $\beta \notin \{\alpha_1, \ldots, \alpha_n, \ldots\}$. Luego el intervalo $[0, 1]$ no es numerable.

A nivel práctico, cuesta distinguir entre $\mathbb{Q}$ y $\mathbb{R}$, pues somos incapaces de manejar un número ilimitado de cifras decimales. La diferencia esencial es la numerablidad y la continuidad. En efecto, al ser $\mathbb{R}$ un conjunto no numerable y continuo, posee un cardinal mucho mayor y es más denso que $\mathbb{Q}$. En $\mathbb{R}$ se pueden realizar operaciones tales como tomar límites, definir elementos inferiores y superiores, definir infinitésimos, funciones continuas, derivadas de funciones, integrales, etc.

Esta construcción de $\mathbb{R}$ es debida a Cantor. Hay otra construcción, basada en "cortaduras", debida a Dedekind.

Digamos finalmente que el conjunto $\mathbb{R}$ de los números reales tiene estructura de **cuerpo conmutativo**. Esta estructura algebraica es consecuencia de que $\mathbb{S}$ es un **anillo de integridad** y las sucesiones convergentes de números racionales tienen estructura de **ideal**. El cociente de un anillo de integridad por un ideal es un cuerpo.

Capítulo 6

Dos estructuras matemáticas

En este capítulo exponemos dos estructuras matemáticas, construidas con definiciones y axiomas y desarrolladas mediante teoremas. Ambas estructuras tienen en común que se basan en conjuntos a los que se asocia una medida cuantitativa.

6.1 Espacio de probabilidades

La estructura básica de la Estadística es el espacio de probabilidades, que consta de un suceso seguro o espacio muestral, de unos sucesos observables y de las probabilidades de estos sucesos.

6.1.1 Sucesos y probabilidades

Sea Ω un conjunto no vacío cuyos elementos ω son los posibles resultados de una experiencia. Por ejemplo, lanzar un dado y observar la cara que sale.

Supongamos que A y B son subconjuntos de Ω, ambos oservables bajo la experiencia, en el sentido de que obtenido un elemento ω podemos decidir si A y B se han presentado o no.

1. Cada ω de Ω es un **suceso elemental**.
2. A y B, subconjuntos de Ω observables, son **sucesos**.
3. El conjunto total Ω es un suceso al que llamaremos s**uceso seguro**.
4. El conjunto vacío $\varnothing$ es un suceso al que llamaremos **suceso imposible**.
5. Dos sucesos A y B son **incompatibles** si son conjuntos disjuntos.

6. El complementario de un suceso A es el **suceso contrario** y se indica por $\overline{A}$.

7. Cuando tenemos la información de que se ha presentado un suceso B, la presencia de otro suceso A queda condicionado por B. Lo indicaremos por A/B.

Definición de probabilidad. Una probabilidad P definida sobre los subconjuntos observables (sucesos) de Ω, asigna a cada suceso A un número real $P(A)$ tal que

$$0 \leq P(A) \leq 1.$$

La probabilidad satisface los siguientes axiomas:
Axioma 1. La probabilidad del suceso seguro es 1

$$P(\Omega) = 1.$$

Axioma 2. Si A y B son sucesos incompatibles, es decir, $A \cap B = \varnothing$, entonces

$$P(A \cup B) = P(A) + P(B).$$

Axioma 3. Si A y B son sucesos de probabilidad no nula entonces

$$P(A \cap B) = P(B)P(A/B). \tag{6.1}$$

Teorema 1. La probabilidad del suceso imposible es $P(\varnothing) = 0$.

Prueba. $\varnothing$ es disjunto de sí mismo y verifica $\varnothing \cup \varnothing = \varnothing$. Por el axioma 2 $P(\varnothing \cup \varnothing) = P(\varnothing) + P(\varnothing)$, lo que implica $P(\varnothing) = 0$.
Teorema 2. La probabilidad del suceso contrario de A es

$$P(\overline{A}) = 1 - P(A).$$

Prueba. A y su contrario $\overline{A}$ son incompatibles y además $A \cup \overline{A} = \Omega$. Por los axiomas 1 y 2 tenemos que

$$P(A \cup \overline{A}) = P(A) + P(\overline{A}) = P(\Omega) = 1.$$

Teorema 3. La probabilidad de la unión de dos sucesos es

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

Prueba. De las propiedades de los conjuntos, sabemos que

$$A = A \cap B + A \cap \overline{B}, \quad A \cup B = B + A \cap \overline{B},$$

donde + indica reunión disjunta. Aplicando el axioma 2 y despejando $P(A \cap \overline{B})$, obtenemos la probabilidad de la unión $A \cup B$.

Teorema 4. Supongamos que Ω es finito con n sucesos elementales equiprobables. Entonces la probabilidad de un suceso A que contiene k sucesos elementales es

$$P(A) = \frac{k}{n}.$$

Prueba. Si los sucesos elementales son $\omega_1, \ldots, \omega_n$ entoncres $\Omega = \{\omega_1\} + \cdots + \{\omega_n\}$. Combinando los axiomas 1 y 2, vemos que cada suceso elemental tiene probabilidad $1/n$. Entonces la probabilidad de A es k/n.

Escolio. La definición y propiedades de la probabilidad se basan en las propiedades de la **frecuencia relativa**, es decir, si tras n repeticiones de una experiencia, un suceso ha sido obervado k veces, la frecuencia relativa es k/n. El teorema 4 es una demostración de la fórmula clásica

$$\text{probabilidad} = \frac{\text{casos favorables}}{\text{casos posibles}}.$$

Este cociente no es válido si Ω es infinito o los casos favorables no son equiprobables.

Definición de independencia. Dos sucesos A y B son estocásticamente **independientes** si

$$P(A \cap B) = P(A)P(B).$$

En caso contrario diremos que son **dependientes**.

Teorema 5. Dos sucesos incompatibles de probabilidad positiva no pueden ser independientes.

Prueba. Si $A \cap B = \varnothing$ entonces $P(A \cap B) = 0$, que es necesariamente distinto del producto $P(A)P(B)$.

Teorema 6. Si A y B son sucesos independientes entonces

$$P(A/B) = P(A).$$

Prueba. Es una consecuencia inmediata de la definición de sucesos independientes y del axioma 3.

Fórmula de la probabilidad condicionada. Sean A y B dos sucesos con $P(B) > 0$. La probabilidad de A condicionada a B es

$$P(A/B) = \frac{P(A \cap B)}{P(B)}.$$

Escolio. Esta fórmula se puede justificar en términos de frecuencias relativas y es una consecuencia inmediata del axioma 3, axioma que es conocido como **principio de las probabilidades compuestas**. Si dos sucesos A y B son dependientes y $P(A/B) > P(A)$, entonces la información de la presencia de B favorece la presencia de A. Por ejemplo, si apostamos por la cara 2 en el lanzamiento de un dado y antes de ver el resultado nos informan de que ha salido par, entonces $P(\{2\}) = 1/6$ aumenta a $P(\{2\}/\text{par}) = 1/3$.

6.1.2 Teorema de Bayes

Supongamos que el suceso seguro es la reunión de k sucesos disjuntos:

$$\Omega = H_1 + \cdots + H_k.$$

Estos sucesos reciben el nombre de "causas". Hay dos fórmulas de fácil demostración en las que intervienen las probabilidades de las causas.
Fórmula de las probabilidades totales. Sea A un suceso. Su probabilidad es

$$P(A) = P(A/H_1)P(H_1) + \cdots + P(A/H_k)P(H_k).$$

Fórmula de Bayes. Supongamos que sabemos que se ha presentaado un suceso B. La probabilidad de una causa H_i es

$$P(H_i/B) = \frac{P(B/H_i)P(H_i)}{P(B/H_1)P(H_1) + \cdots + P(B/H_k)P(H_k)}.$$

Ejemplo. La fórmula de Bayes o teorema de Bayes, es muy importante en Estadística. Supongamos que son conocidas las probabilidades de ciertas enfermedades (posibles causas de una sintomatología). Conocidos unos resultados clínicos B, podemos calcular las probabilidades condicionadas de cada una de las causas $H_1, \ldots, H_k$, es decir, nos permite diagnosticar al paciente asignándole la enfermedad más probable.

6.1.3 Variables aleatorias

Las variables aleatorias son aplicaciones de Ω en el conjunto de los números reales. Se introducen mediante definición y se demuestran sus propiedades enunciando teoremas. Las variables aleatorias permiten formalizar las variables estadísticas (medidas físicas, biométricas, económicas, etc.). Sin embargo Cramer (1967) define las variabes aleatorias y establece, axiomáticamente, sus primeras propiedades. Por otra parte, si se admite el axioma de elección (AE), sólo podemos definir una probabilidad sobre los conjuntos borelianos (los generados por intervalos). Pero si no se acepta el AE, todo subconjunto de la recta real es medible y admite una probabilidad.

6.2 Jerarquía indexada

Cuando se tienen unidades homogéneas en algún sentido, se tiende a clasificarlas de acuerdo con su afinidad. Una biblioteca, por ejemplo, clasifica sus libros por temas (literatura, arte, ciencia, deportes, etc.). Una clasificación importante (iniciada por Linneo), es la que permite clasificar a los animales y vegetales en familias, géneros y especies. Mediante llaves, agrupamos unidades, de manera que una misma unidad no pertenzca a dos grupos distintos. Estas agrupaciones se pueden formalizar objetivamente.

6.2.1 Clasificación jerárquica

Los elementos de un conjunto Ω se pueden dividir en subconjuntos homogéneos. Establecer una clasificación es realizar una partición (división en conjuntos disjuntos). Por ejemplo, los humanos se dividen en cuatro grupos según su grupo sanguíneo.

Si $\Omega = \{w_1, w_2, \ldots, \omega_n\}$ es un conjunto finito, indicaremos sus elementos por $1, 2, \ldots, n$. Una partición de Ω se expresará como

$$\Omega = C_1 + \cdots + C_m.$$

Las particiones pueden estar jerarquizadas. El proceso de construcción de una jerarquía de conjuntos se llama **clasificación jerárquica**.

Llamaremos **jerarquía** a una colección $\mathbf{C}$ de subconjuntos de Ω, llamados **clusters**, que verifica:
Axioma de la intersección. Si $C, C' \in \mathbf{C}$ entonces $C \cap C' \in \{C, C', \emptyset\}$.
Axioma de la reunión. Si $C \in \mathbf{C}$ entonces $C = \cup\{C'$ tal que $C' \in \mathbf{C}$, $C' \subset C\}$.

Una jerarquía es consistente con la acción de considerar un conjunto incluido en Ω.
Teorema 1. Sea C un cluster de una jeraquía $\mathbf{C}$ sobre Ω. Tomando C como conjunto total, podemos definir una nueva jerarquía sobre C.

Prueba. Sea $C = \cup C_i$ la unión de todos los clusters de la jerarquía incluidos en C. Tomemos dos clusters C_i, C_j incluidos en C. Obviamente C_i, C_j cumplen el axioma de la intersección. También se cumple el axioma de la reunión pues si C' es un cluster incluido en C entonces $C' = C' \cap C = \cup(C' \cap C_i)$, donde cada $C' \cap C_i$ es $\emptyset$ ó es un cluster contenido en C. Obtenemos pues una sub-jerarquía construida a partir de un cluster C.

Además, es fácil probar que una jerarquía $\mathbf{C}$ está incluida en otra jerarquía mayor $\widetilde{\mathbf{C}}$, siendo entonces $\mathbf{C}$ una sub-jerarquía de $\widetilde{\mathbf{C}}$.

Definición 1. Una jeraquía **C** se llama **total** si el conjunto Ω y cada elemento aislado $\{i\}$ de Ω pertencen a **C**.
Definición 2. Se llama **índice** de una jerarquia total a una aplicación que a cada cluster C de **C** le asigna un número real $\alpha(C)$ no negativo tal que:

$$\alpha(\{i\}) = 0, \qquad \alpha(C) \leq \alpha(C') \quad \text{si } C \subset C'.$$

Al par $(\mathbf{C}, \alpha)$ le llamaremos **jerarquía indexada**.

Escolio. El concepto de jerarquía formaliza y cuantifica la clasificación de las especies vegetales y animales y puede ser utilizado en muchos otros campos.

1. El primer axioma significa que si tenemos dos clusters, entonces uno está incluido en el otro o ambos son disjuntos, es decir, $C \subset C'$, ó bien $C' \subset C$, ó bien $C \cap C' = \emptyset$. Se pretende evitar que un elemento (por ejemplo, una especie vegetal) de Ω pertenezca simultáneamente a dos clusters excluyentes, ya que entonces estaría mal clasificado.

2. El segundo axioma significa que cada cluster es reunión de los clusters que contiene. Es decir, reuniendo clusters obtenemos clusters más amplios. En particular Ω es reunión de todos los clusters de **C**. Por ejemplo, en el reino animal, un género es reunión de especies, una familia es reunión de géneros, etc.

3. La definición 1 afirma que la jerarquía **C** es total si contiene el conjunto principal Ω y cada uno de los elementos simples de Ω.

4. El índice de la jerarquía proporciona un grado de homogeneidad en cada cluster. Cuanto más pequeño es un cluster más homogéneo es. Por ejemplo, un género es más homogéneo que una familia formada por diversos géneros, pues contiene más especies.

Como ocurre con las probabilidades de sucesos, los valores niméricos asignados a los clusters verifican ciertas propiedades.
Teorema 2. El índice de una jerarquía indexada toma el valor máximo para Ω.

Prueba. Si C es un cluster entonces $C \subset \Omega$. Por la definición 2 tendremos que $\alpha(C) \leq \alpha(\Omega)$.
Teorema 3. Para todo número real $x \geq 0$ la relación binaria $\mathcal{R}_x$ sobre los elementos de Ω

$$i\mathcal{R}_x j \quad \text{si} \quad i, j \in C, \quad \text{siendo} \quad \alpha(C) \leq x, \tag{6.2}$$

es de equivalencia.

Prueba: La relación $\mathcal{R}_x$ es:

Reflexiva: $i\mathcal{R}_x i$ ya que $i \in \{i\}$, siendo $\alpha(\{i\}) = 0 \leq x$.

Simétrica: Evidente.

Transitiva: Sea C_{ij} el mínimo cluster que contiene i, j, y análogamente C_{jk}. Entonces, por el axioma de la intersección:

$$i\mathcal{R}_x j \Rightarrow i, j \in C_{ij}, \quad \alpha(C_{ij}) \leq x, \quad j\mathcal{R}_x k \Rightarrow j, k \in C_{jk}, \quad \alpha(C_{jk}) \leq x,$$

$$\Rightarrow C_{ij} \cap C_{jk} \neq \emptyset \Rightarrow \left\{ \begin{array}{ll} a) & C_{ij} \subset C_{jk} \Rightarrow i, k \in C_{jk}, \\ b) & C_{jk} \subset C_{ij} \Rightarrow i, k \in C_{ij}, \end{array} \right. \Rightarrow i\mathcal{R}_x k. \qquad \square$$

Teorema 4. Para cada número real $x \geq 0$ podemos encontrar una partición de Ω

$$\Omega = C_1 + \cdots + C_m$$

a la que denominaremos clasificación a nivel x.

Prueba. Es una consecuencia del teorema 3, pues toda relación de equivalencia define una partición de Ω.

Si $\alpha(\Omega) = \beta$, dos clasificaciones triviales a nivel $x = \beta$ y a nivel $x = 0$ son, respectivamente,

$$\Omega = \Omega, \qquad \Omega = \{1\} + \cdots + \{n\} \ .$$

El interés de las jerarquías indexadas reside en construir e interpretar clasificaciones (particiones de Ω) a nivel x siendo $0 < x < \beta$.

Enunciemos otra propiedad conjuntista similar al teorema 1. Afirma que si tomamos como elementos una colección de clusters que constituyen una partición, se conserva la estructura de la jerarquía.

Teorema 5. Consideremos una partición $\Omega = C_1 + \cdots + C_m$ y tomemos los clusters de la partición como elementos básicos de Ω, a los que llamaremos átomos. Obtenemos entonces una nueva jerarquía menos fina que la inicial.

Prueba. Si un cluster C verifica $C \subset C_i$ entonces se confunde con C_i. Si $C_i \subset C$ entonces $C = C \cap \Omega$ es unión de átomos. Análogamente otro cluster C'. Luego dos clusters C, C', no contenidos en ningún átomo, son reunión de átomos. Por el axioma de la intersección, o un cluster contiene una parte de los átomos del otro, o ambos no contienen átomos comunes. Además es obvio que cada cluster es la reunión de los clusters que contiene. Se cumplen pues las condiciones de una jerarquía.

6.2.2 Espacio ultramétrico

Una jerarquía indexada $(\mathbf{C}, \alpha)$ tiene además una estructura geométrica interesante, que tiene que ver con la propiedad ultramétrica, que también aparece en otras ramas de las mate,áticas. .

Definición 3. Un espacio ultramétrico (Ω, u) es una estructura formada por un conjunto finito Ω y una función distancia u sobre $\Omega \times \Omega$ verificando, para todo i, j, k de Ω:

a) No negatividad: $u(i, j) \geq u(i, i) = 0$.

b) Simetría: $u(i, j) = u(j, i)$.

c) Propiedad ultramétrica:

$$u(i, j) \leq \sup\{u(i, k), u(j, k)\}.$$

Teorema 6. Todo espacio ultramétrico es métrico, es decir, la distancia u verifica la desigualdad triangular

$$u(i, j) \leq u(i, k) + u(j, k).$$

Prueba. Basta tener en cuenta que $u(i, j) \leq \sup\{u(i, k), u(j, k)\} \leq u(i, k) + u(j, k)$.

Teorema 7. En un espacio ultramétrico todo triángulo es isósceles con la base el lado menor.

Prueba. Sea $\{i, j, k\}$ un triángulo. Si $u(i, j)$ es el lado más pequeño, entonces:

$$\begin{array}{lll} u(i,k) & \leq \sup\{u(i,j), u(j,k)\} & = u(j,k) \\ u(j,k) & \leq \sup\{u(i,j), u(i,k)\} & = u(i,k) \end{array} \Longrightarrow u(i, k) = u(j, k).$$

Teorema 8. Toda jerarquia indexada $(\mathbf{C}, \alpha)$ sobre un conjunto Ω, se puede interpretar como un espacio ultramétrico (Ω, u).

Prueba. Sean i, j, k tres elementos de Ω. A partir de $(\mathcal{C}, \alpha)$ definimos la siguiente distancia

$$u(i, j) = \alpha(C_{ij}),$$

donde C_{ij} es el mínimo cluster (respecto a la inclusión) que contiene i, j. Sea $\{i, j, k\}$ un triángulo y sean también C_{ik}, C_{jk} los mínimos clusters que contienen $\{i, k\}$, $\{j, k\}$ respectivamente. Tenemos que $C_{ik} \cap C_{jk} \neq \emptyset$ y por tanto, considerando el axioma de la intersección, hay dos posibilidades:

a) $C_{ik} \subset C_{jk} \Rightarrow i, j, k \in C_{jk} \Rightarrow C_{ij} \subset C_{jk} \Rightarrow u(i, j) = \alpha(C_{ij}) \leq u(j, k) = \alpha(C_{jk})$,

b) $C_{jk} \subset C_{ik} \Rightarrow i, j, k \in C_{ik} \Rightarrow C_{ij} \subset C_{ik} \Rightarrow u(i, j) = \alpha(C_{ij}) \leq u(i, k) = \alpha(C_{ik})$.

Así pues: $u(i,j) \leq \sup\{u(i,k), u(j,k)\}$.

Escolio. El hecho de que una jerarquía indexada sea también un espacio ultramético, permite la posibilidad de una representación gráfica mediante un **dendograma**. Por ejemplo, consideremos los cinco partidos políticos CU, PP, PSC, IC, ERC que había en Catalunya. Cada partido es un cluster y cada partición de Ω (conjunto total de los partidos) la llamaremos **clustering**. La jerarquía indexada mediante un índice α que va de 0 a 3 es:

	Clustering (clasificación o partición)	α	Denomimación
$\Omega =$	$\{CU\} + \{PP\} + \{PSC\} + \{IC\} + \{ERC\}$	0	(partidos)
$\Omega =$	$\{CU, PP\} + \{PSC, IC\} + \{ERC\}$	1.5	(derecha, izqu., centro)
$\Omega =$	$\{CU, PP\} + \{PSC, IC, ERC\}$	2	(coaliciones)
$\Omega =$	Ω	3	(parlamento)

Esta jerarquía se representa mediante el dendograma de la figura 6.1. Esta figura también contiene (derecha) la agrupación jerárquica de catorce idiomas europeos.

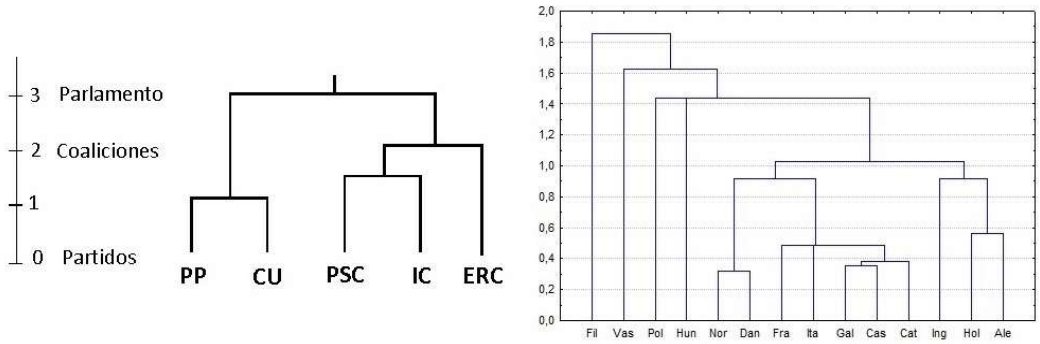


Figura 6.1: Representación de cinco partidos políticos, visualizando mediante un dendograma, la jerarquía indexada. A la derecha dendograma de 14 idiomas europeos según la semejanza entre algunos vocablos comunes.

Apéndices

Apéndice A

RESUMEN DE ARITMÉTICA TRANSFINITA

1. Los conjuntos pueden ser finitos o infinitos en magnitud. Los números naturales 0, 1, 2, 3,..., n,... indican el número de elementos de los conjuntos finitos.

2. En matemáticas se utiliza mucho la frase "n tiende a ∞ " para expresar que n crece indefinidamente y para estudiar el límite de una ecuación. Este ∞ es el que conocemos todos, pero no es el único.

3. El infinito anterior es en realidad la magnitud del conjunto $\mathbb{N} = \{0, 1, 2, 3,\ldots, n,\ldots\}$ de los números naturales. Este infinio se indica por A_0. Diremos que el cardinal de $\mathbb{N}$ es A_0.

4. Un conjunto $\mathbb{A}$ es numerable si se puede establecer una correspondencia entre $\mathbb{A}$ y $\mathbb{N}$. Entonces $\mathbb{A}$ se puede indicar como $\mathbb{A} = \{a_0, a_1, \ldots, a_n, \ldots\}$ y el cardinal de $\mathbb{A}$ es A_0. El conjunto de los números pares $\mathbb{P} = \{0, 2, 4,\ldots, 2n,\ldots\}$ es numerable. También lo es el conjunto $\mathbb{Q}$ de los números racionales.

5. El conjunto $\mathbb{R}$ de los números reales (racionales e irracionales), es no numerable. Sus elementos no se pueden numerar. El cardinal de $\mathbb{R}$ se llama potencia del continuo y se indica por c.

6. Aunque A_0 y c son infinitos, ambos son números cardinales de distinta magnitud, es decir, $A_0 < c$.

7. Se demuestra que la colección de todos los subconjuntos de $\mathbb{N}$ tiene cardinal 2^{A_0}. Además se verifica que $c = 2^{A_0}$.

8. Como $A_0 < c$ y ambos cardinales son infinitos, se plantea la cuestión de si existe o no otro infinito comprendido entre A_0 y c, La hipótesis del continuo afirma que este cardinal intermedio no existe.

9. Durante mucho tiempo se intentó probar la hipótesis del continuo. Sin embargo se ha demostrado que es indecidible. No puede probarse, y hay que aceptarla (o rechazarla) como si fuera un axioma de la teoría de conjuntos.

10. Se demuestra que la colección de todos los subconjuntos de $\mathbb{R}$ tiene cardinal 2^c, . siendo c la potencia del contínuo, que verifica $c = 2^{A_0}$.

11. Indicando $f = 2^c$, este nuevo cardinal infinito verifica $A_0 < c < f$. Se demuestra que f es el cardinal de todas las funciones reales, es decir, de todas las curvas no cerradas (continuas o discontinuas) del plano.

12. La construcción interminable de cardinales infinitos nos lleva a la sucesión de los "alephs" $A_0 < A_1 < \cdots < A_n < \cdots$ donde cada aleph se construye tomando el cardinal de la colección de subconjuntos del anterior. Es decir, partiendo de A_0 tenemos que $A_1 = 2^{A_0}$, $A_2 = 2^{A_1}$, y así sucesivamente.

13. Admitir la hipótesis del contínuo equivale a escribir $A_1 = c$. Si extendemos esta hipótesis al siguiente cardinal, entonces sería además $A_2 = f$.

14. Si no se acepta la hipótesis del continuo, entonces la sucesión $A_0 < A_1 < \cdots < A_n < \cdots$ es más general, en el sentido de que A_1 es el siguiente de A_0, a continuación viene A_2 que es el siguiente inmediato de A_1 y así sucesivamente.

15. Respecto a los infinitos c y f, sólo sabemos que $A_1 \leq c$ y que $A_2 \leq f$. Es decir, $A_0 < A_1 \leq c < A_2 \leq f$ o bien $A_0 < A_1 \leq c \leq A_2 \leq f$, pero descartando el caso particular $A_0 < A_1 < c = A_2 = f$ por razones obvias.

16. Algunos aspectos de los conjuntos se simplifican y enriquecen si se acepta el axioma de elección: podemos elegir un elemento de cada uno de los conjuntos de una colección. Sin embargo, aceptar este axioma conduce a encontrar conjuntos lineales cuya longitud no existe, o a ser posible seccionar una bola sólida y después ensamblarla obteniendo dos bolas iguales a la inicial.

Apéndice B

GLOSARIO

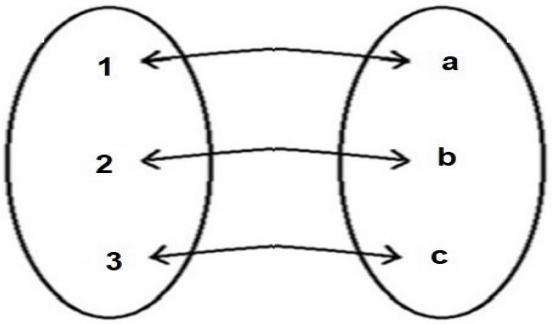
ALEPH. Notación propuesta por Cantor para designar los cardinales infinitos. El primer aleph es $\aleph_0$, cardinal del conjunto de los números naturales. Lo indicamos por A_0.
ARITMÉTICA TRANSFINITA. Operaciones entre números cardinales infinitos que siguen reglas distintas de la aritmética ordinaria. Ejemplos: 1) $A_0 + A_0 = A_0$. 2) $A_0 + c = c$. 3) $c + c = c$. 4) $c \times c = c$.
AXIOMA O PRINCIPIO DE ELECCIÓN. Dada una clase de conjuntos, podemos construir un conjunto que contiene un elemento (y uno solo) de cada uno de los conjuntos de la clase.
BASE BINARIA Un número en base 10 se puede escribir en base 2. El 0, 1, 2, 3, 4 serían 0, 1, 10, 11, 100. ’
CARDINAL. Número de elementos de un conjunto finito. Si el conjunto es infinito, el cardinal se mide mediante una correspondencia biyectiva (es decir, uno-a-uno), con algún conjunto (infinito) conocido. El cardinal del conjunto $\mathbb{A}$ se indica por $\text{car}(\mathbb{A})$.
CONJUNTO FINITO. Un conjunto es finito si no puede ponerse en correspondencia biyectiva con algún subconjunto propio.
CONJUNTO INFINITO. Un conjunto es infinito si es posible establecer una correspondencia biyectiva con algún subconjunto propio.
CONTINUO. La potencia del contínuo es el cardinal del conjunto $\mathbb{R}$ de los numeros reales.
CORRESPONDENCIA BIYECTIVA. También llamada correspondencia “uno a uno” es una relación entre dos conjuntos tal que a cada elemento del primero le corresponde un elemento (y uno solo) del segundo.

ENUMERABLE o NUMERABLE. Es un conjunto que se puede poner en correspondencia biyectiva con un conjunto finito o con $\mathbb{N}$, conjunto de los números naturales.
ESPACIO DE PROBABILIDADES. Estructura formada por un conjunto, una colección de conjuntos observables y una función de probabilidad que debe cumplir ciertos axiomas.
HIPÓTESIS DEL CONTINUO. Formulada por Cantor, afirma que entre los dos cardinales infinitos de $\mathbb{N}$ y de $\mathbb{R}$ no hay ningún otro cardinal. No existe g tal que $A_o < g < c$. Es una propiedad indecidible, que no se puede demostrar.
JERARQUÍA INDEXADA. Estructura conjuntista formada por un conjunto y una colección de sibconjuntos, a los que se les asigna un índice numérico. Deben verificar ciertos axiomas que permitan construir particiones del conjunto principal, que se interpretan como clasificaciones.
NO MEDIBLE. Aceptando el principio de elección, existen conjuntos sin medida o "sucesos" sin probabilidad.
NÚMEROS ENTEROS. Conjunto $\mathbb{Z}$ formado por números con parte entera positiva o negativa, es decir, $\mathbb{Z} = \{\ldots - n, \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots, n, \ldots\}$. El conjunto $\mathbb{Z}$ es enumerable.
NÚMEROS NATURALES. Conjunto $\mathbb{N}$ formado por los números $0, 1, 2, 3, \ldots, n, \ldots$. El conjunto $\mathbb{N}$ es numerable. Su cardinal se indica por A_0.
NÚMEROS RACIONALES. Conjunto $\mathbb{Q}$ formado por las fracciones m/n entre dos números enteros. El conjunto $\mathbb{Q}$ es numerable, es decir, de cardinal A_0.
NÚMEROS REALES. Conjunto $\mathbb{R}$ formado por todos los números enteros, racionales e irracionales. Los números π y $\sqrt{2}$ son irracionales. El conjunto $\mathbb{R}$ es no numerable. Su cardinal se indica por c.
PARTES DE UN CONJUNTO. Dado un conjunto no vacío $\mathbb{S}$, el conjunto $P(\mathbb{S})$ está formado por todos los subconjuntos de $\mathbb{S}$. Si $A = \text{car}(\mathbb{S})$,se verifica $\text{car}(P(\mathbb{S})) = 2^{A.}$
PARTICIÓN. Clase de subconjuntos disjuntos de un conjunto Ω cuya reunión da lugar a Ω.
SUCESIÓN DE LOS ALEPHS. Sucesión de cardinales infinitos $\aleph_0 < \aleph_1 < \cdots < \aleph_n < \cdots < \aleph_\omega < \cdots$. Cantor propuso construir $\aleph_{n+1}$ a partir de $\aleph_n = \text{car}(\mathbb{S})$, siendo $\mathbb{S}$ un conjunto, definiendo $\aleph_{n+1} = \text{car}(P(\mathbb{S}))$ donde $P(\mathbb{S})$ es el conjunto de las partes de $\mathbb{S}$. Aquí indicaremos la sucesión por $A_0 < A_1 < \cdots < A_n < \cdots$. Aunque se sabe que $A_n < A_{n+1}$, se desconoce si $A_{n+1} = \text{car}(P(\mathbb{S}))$ es realmente el cardinal que sigue a A_n. Otra sucesión de alephs consiste en tomar $A_0 < A_1 < \cdots < A_n < \cdots$ donde A_1 es el siguiente de A_0, A_2 es el siguiente de A_1, etc., entendiendo por siguiente el menor cardinal de entre los cardinales superiores a uno dado. La hipótesis del continuo se formularía como $A_0 < A_1 \leq 2^{A_0}$.

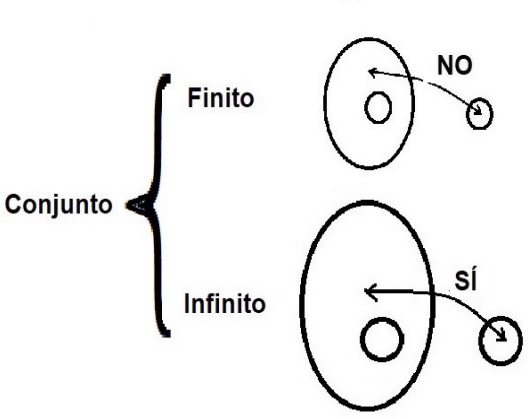
Apéndice C

CARDINALES EN IMÁGENES

Figuras

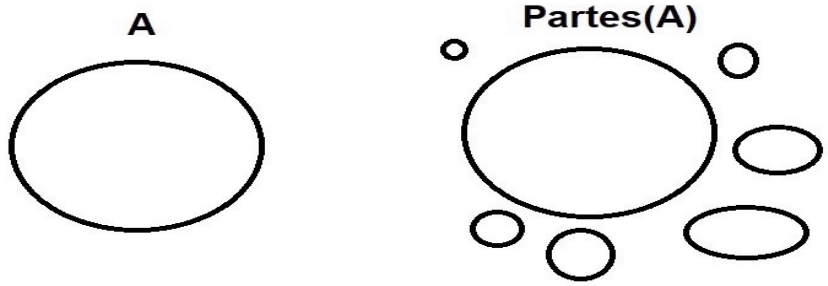


Correspondencia biyectiva también llamada uno-a-uno que identifica el tamaño de dos conjuntos distintos.



En un conjunto infinito se puede establecer una correspondencia biyectiva con un subconjunto propio.

Teorema de Cantor



$$\text{cardinal (A)} < \text{cardinal (Partes(A))} = 2^{\text{cardinal(A)}}$$

El tamaño de un conjunto A es menor que el tamaños de la colección de subconjuntos (o partes) de A.

Hipótesis del continuo

{0,1,2,3,4}	Finito	F
{0,1,2,3,4,5,...,n,...}	Numerable	N
———————	Continuo	C

$F < N < C$

Existe G tal que $N < G < C$?

La hipótesis de que no existe un infinito intermedio entre el numerable y el continuo es indecidible (no se puede demostrar).

Sucesión de ordinales

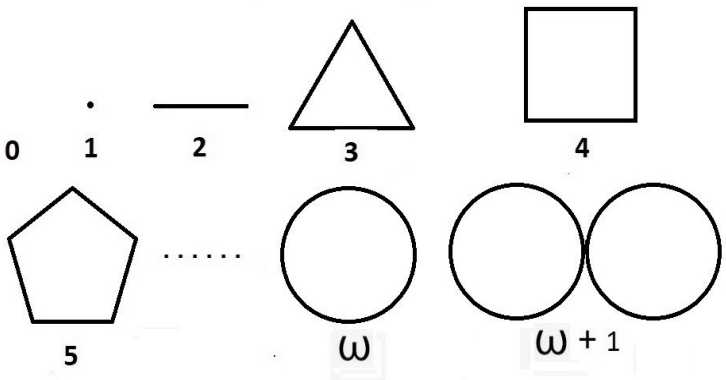
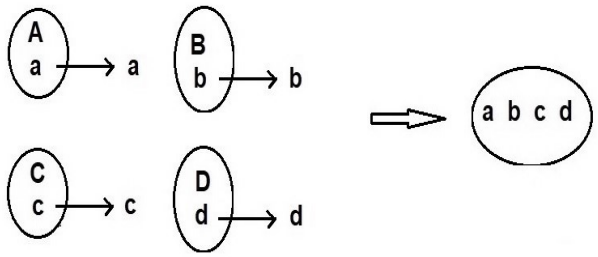
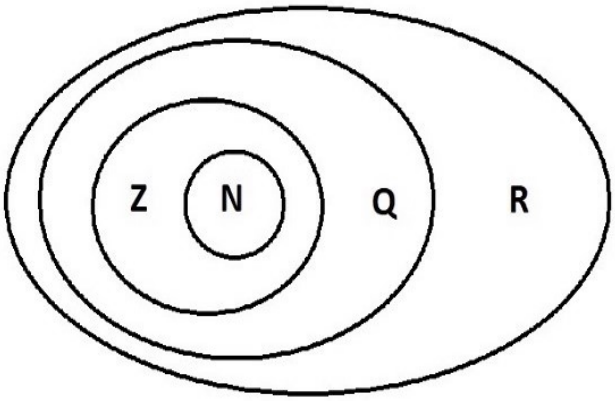


Ilustración poligonal de la sucesión de ordinales finitos a los que siguen el ordinal numerable ω y su siguiente inmediato ω + 1.

Principio de elección



El principio de elección postula que dada una colección de conjuntos podemos elegir un elemento de cada uno de los conjuntos.



Los números reales R incluyen a los racionales Q que incluyen a los enteros Z y estos a los naturales N.

Cambio de base

Base								
Decimal	0	1	2	3	4	5	6	7
Binaria	0	1	10	11	100	101	110	111

Algunos números en base 10 expresados en base 2. También se pueden expresar en otra base, como la base 3.

Referencias

[1] Ara, P. (2020) La paradoxa de Banach-Tarski i el semigrup tipus. *Butlletí de la Societat Catalana de Matemàtiques*, 35(1), 5-22.

[2] Bacmann, H. (1955) Transfinite Zahlen. Springer, Berlin.

[3] Chaitin, G. G. (1991) El azar de los números. *Mundo Científico*, 115 (11), 772-777.

[4] Cramer, H. (1967) Métodos matemáticos de la estadística. Aguilar, Madrid.

[5] Cuadras, C. M. (2015) Contributions to the diagonal expansion of a bivariate copula with continuous extensions. *Journal of Mulltivariate Analysis*, 139, 28-44.

[6] Cuadras, C. M. (2019) Nuevos métodos de análisis multivariante. CMC Editions. Barcelona.

[7] Cuadras, C. M., Diaz, W., Salvo-Garrido, S. (2019) Two generalized bivariate FGM distributions and rank reduction. *Communications in Statistics-Theory and Methods,* DOI 10.1080/03610926.2019.1620280

[8] Cuesta, N. (1981) La sinfonía del infinito. Ed. Univ. de Salamanca.

[9] Dauben, J. W. (1995) Georg Cantor. *Investigación y Ciencia*, Temas: Grandes Matemáticos.

[10] Delahaye, J-P. (2020) Demostrar la hipótesis del continuo. *Investigación y Ciencia*, 524, 72-79, mayo 2020.

[11] Dou, A. (1970) Fundamentos de la matemática. Ed. Labor, Barcelona.

[12] Fresán, J. (2010) El sueño de la razón. RBA, Barcelona.

[13] Hahn, H. (1968) El infinito. Sigma. El Mundo de las Matemáticas. Ed. Grijalbo, Barcelona.

[14] Lipschuz, S. (1965) General topology. Schaum Pub. Co., New York.

[15] Mosterín, J. (1971) Teoría axiomática de conjuntos. Ariel, Barcelona.

[16] Munroe, M. E. (1952, 1959) Introduction to measure and integration. Addison Wesley Pub. Co., Reading.

[17] Nagel, E., Newman, J. R. (1968) La demostración de Gödel. Sigma. El Mundo de las Matemáticas. Ed. Grijalbo, Barcelona.

[18] Navarro, J. (1973) La nueva matemática. Salvat Editores, Barcelona.
[19] Navarro, J. (2011) Ideas fugaces teoremas eternos. RBA, Barcelona.
[20] Obregón, I. (1975) Teoría de la probabilidad. Ed. Limusa, México.
[21] Orts, J. M. (1957) El principio de elección. *Memorias de la Real Academ. de Ciencias y Artes de Barcelona*, Vol 32, núm. 9.
[22] Pla, J. (1993) Axiomes alternatius de la teoria de conjunts i llur influència en matemàtiques. *Arxius de la Secció de Ciències*, CVII. Institut d'Estudis Catalans, Barcelona.
[23] Russell, B. (1967) Los principios de la matemática. Espasa Calpe, Madrid.
[24] Schimmerling, E. (2011) A course on set theory. Cambridge Univ. Press, Cambridge.
[25] Sierpinski, W. (1956) Hypothèse du continu. Clelsea Pub., N. York.

VERDADES NO DEMOSTRABLES: TEOREMAS DE GÖDEL Y SUS GENERALIZACIONES

BALTASAR RODRÍGUEZ-SALINAS
Real Academia de Ciencias

Si se nos preguntase cuáles son las contribuciones más importantes a las matemáticas en el siglo XX, contestaríamos que son la creación o descubrimiento de la teoría de conjuntos por G. Cantor y los teoremas de incompletitud de K. Gödel.

La teoría de conjuntos con sus paradojas dio un gran impulso a los fundamentos de las matemáticas y a la noción de verdad.

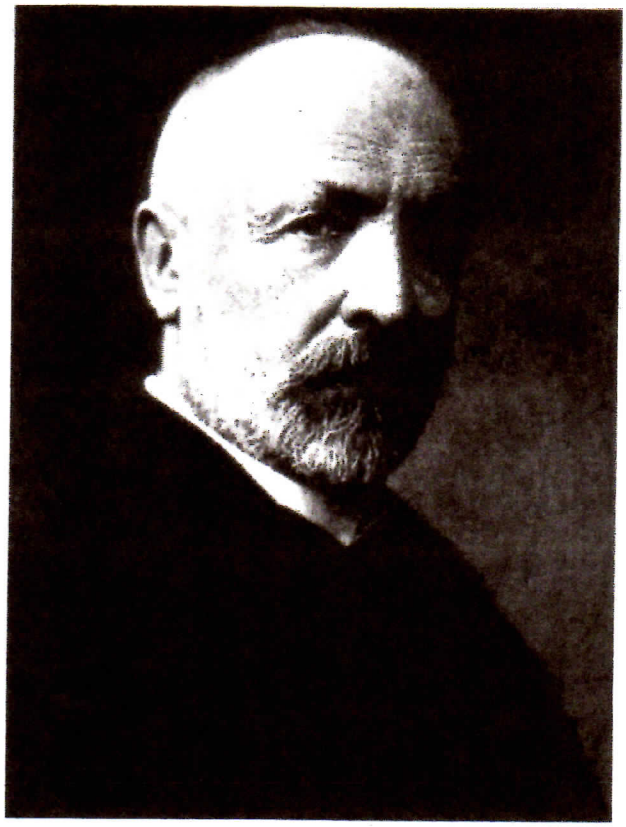
Las matemáticas se fundamentan en la verdad, pero no en una verdad cualquiera de carácter relativo, sino en una de carácter absoluto. Sin embargo, últimamente han surgido dudas de si existe esa verdad.

Si no existe la verdad, la frase «no existe la verdad» sería verdadera en contra de la suposición de que no existe la verdad. Esta contradicción sería para muchos una demostración de que existe la verdad. Pero si reflexionamos podemos llegar más lejos, puesto que se debería admitir que si no existe la verdad tampoco existiría la mentira y estaríamos en un mundo caótico en contra de todo lo que percibimos y en donde la mentira sería la verdad.

Si nos piden un ejemplo de verdad absoluta, daríamos como tal las proposiciones de la aritmética. Sus verdades las conocemos por la intuición razonable, de modo que mediante la lógica podemos deducir los teoremas a partir de los axiomas. Antes de Gödel, incluido Hilbert, se creía que todas las verdades de la aritmética eran demostrables. Pero Gödel demostró en 1931 que existen verdades aritméticas no demostrables, entre ellas la consistencia o no contradicción de la aritmética.

La existencia de verdades no demostrables tiene una aplicación importantísima en la teología, puesto que Dios es una verdad no demostrable, como lo prueba la experiencia y el fracaso de demostraciones contundentes, admitidas por todos, de la existencia de Dios. Para demostrar la existencia de Dios tenemos que basarnos en una verdad lógicamente equivalente que no puede ser más que la misma Verdad porque Dios es la Verdad.

Se han hecho intentos de demostrar la no existencia de Dios, pero si se identifica Dios con la verdad, ello es radicalmente imposible. Porque si no existiese la verdad, la lógica caería en defecto por basarse en la verdad que se considera que no existe. Es más, el empleo de la lógica viene a ser un reconocimiento implícito de la existencia de la verdad.



Georg Cantor.

Nuestra mente capta las verdades mediante la intuición razonable y la lógica. La intuición razonable es un don que está muy dentro de nuestro ser y procede de fuera y que captamos mediante la reflexión. Y la lógica es un don que conocemos por la palabra y el lenguaje.

Usualmente, las matemáticas se basan en los axiomas. De los axiomas se deducen los teoremas mediante las reglas deductivas o de inferencia. Es claro que el conjunto de reglas deductivas debe ser no vacío y finito para que pue-

K. Gödel (izquierda) junto a A. Einstein.

da ser manejable por el hombre. Dado un conjunto A de axiomas y prefijadas las reglas deductivas, denotaremos por $T(A)$ el conjunto de los teoremas de A. Este conjunto, si A es finito, es numerable. Entonces $T(A)$ es el sistema lógico o teoría generado por A.

Dos conjuntos finitos se dice que tienen el mismo número cardinal si se puede establecer una correspondencia biyectiva (o uno a uno) entre ambos. De la misma manera, como se puede establecer una correspondencia biyectiva entre el conjunto $\mathbb{N}$ de los números naturales y el conjunto $2\mathbb{N}$ formado por los números pares asignando a cada número natural n el número par $2n$, diremos que $\mathbb{N}$ y $2\mathbb{N}$ tienen el mismo cardinal. De manera general, un conjunto se dice numerable si tiene el mismo número cardinal que el conjunto $\mathbb{N}$ y contable si es finito o numerable. Se puede probar que todo subconjunto de $\mathbb{N}$ es contable. Los conjuntos infinitos están caracterizados por la propiedad de no ser coordinables con ninguna de sus partes propias, por lo que en el sentido de la cardinalidad todo conjunto finito es mayor que cualquiera de sus partes propias. Esto no pasa con $\mathbb{N}$, que tiene el mismo cardinal que $2\mathbb{N}$, y en general con todos los subconjuntos infinitos.

Como se sabe, la diferencia de dos números naturales es un número entero y el cociente de dos números enteros es un número racional cuando el divisor es distinto de cero. Los números reales surgen como una sucesión de números racionales, pero intuitivamente son números decimales con infinitas cifras detrás de la coma. Esto si se utiliza la numeración usual con base 10, pero también se puede utilizar cualquier otra base, como por ejemplo 2, como ocurre en la informática. Surge ahora la pregunta, si el cardinal del conjunto $\mathbb{R}$ de los números reales es igual que el del conjunto de los números naturales. Cantor probó, utilizando la teoría de conjuntos, que ambos son distintos, mientras que el conjunto de los números naturales es numerable. Pero la pregunta vuelve a surgir si sólo se admiten demostraciones dentro de la aritmética. La contestación es que dentro de la aritmética no se puede demostrar que el conjunto de los números reales no es contable.

Un sistema de axiomas se dice que es consistente cuando en el sistema lógico $T(A)$ de los teoremas de A no hay contradicción, esto es, si $T(A)$ no contiene a la vez un teorema P y su negación $\neg P$ = no P.

El sistema lógico de la aritmética S_0 admite un sistema de axiomas finito A_0 tal que, según el primer teorema de incompletitud de Gödel existe una proposición indecidible P; es decir, que no se puede demostrar P ni su negación. Es claro que, si existe la verdad en las matemáticas, por el principio del tercio excluso, P o su negación es verdadera. Más adelante vamos a dar una idea de la demostración de este teorema de Gödel.

La existencia de la verdad en las matemáticas es una cuestión muy delicada que requiere una reflexión que vamos a desarrollar a continuación.

En el análisis matemático se prueba utilizando la teoría de conjuntos que existe una medida, llamada de Lebesgue, con propiedades muy atrayentes y fecundas sobre una clase muy amplia de subconjuntos de la recta real $\mathbb{R}$, llamados medibles Lebesgue. Esta medida para un intervalo coincide con su longitud y es tal que la clase de los conjuntos medibles Lebesgue es cerrada por la unión e inter-

Henri-León Lebesgue.

sección contable de conjuntos y también por la diferencia. Pues bien, del axioma de elección se deduce que existe un conjunto A no medible Lebesgue de la recta real $\mathbb{R}$ y, por otra parte, según el axioma de Solovay todo subconjunto A de $\mathbb{R}$ es medible Lebesgue. Esto debe asombrar a cualquiera. Pero además ocurre que el axioma de elección es consistente con la axiomática de Zermelo-Fraenkel y, por otra parte, el axioma de Solovay es también consistente con esta axiomática de la teoría de conjuntos más la existencia de un cardinal inaccesible. Entonces la unión, o mejor la conjunción, del axioma de elección, del axioma de Solovay y de la axiomática de Zermelo-Fraenkel es inconsistente por contener una contradicción. Esto no es posible si existe la verdad matemática y fueran verdaderos el axioma de elección y el axioma de Solovay. Luego, si existe la verdad en las matemáticas, existen sistemas consistentes de axiomas, que contienen axiomas no verdaderos.

Aunque no es necesario conocer en qué consiste el axioma de elección para comprender la parte esencial de lo que hemos dicho, vamos a exponerlo. Dada una familia de conjuntos disjuntos y no vacíos, el axioma de elección expresa que existe un conjunto formado por un elemento y sólo uno de cada uno de dichos conjuntos.

La existencia de conjuntos no medibles Lebesgue del espacio $\mathbb{R}^3$ queda patente de manera muy sugestiva por la paradoja de Banach-Tarski, consecuencia del axioma de elección, que consiste en poder descomponer una bola como un guisante en un número finito de partes para recomponer una bola como el Sol. Aunque en el caso del plano $\mathbb{R}^2$ existen igualmente conjuntos no medibles Lebesgue, esta descomposición no es posible por existir una medida finitamente aditiva sobre todos los conjuntos de $\mathbb{R}^2$, que es una extensión de la medida de Lebesgue, como se prueba mediante el teorema de Hahn-Banach.

Como hemos visto, existen sistemas de axiomas que son consistentes pero que contienen proposiciones no verdaderas. En concreto, una de dos, o el axioma de Solovay es falso o el axioma de elección es falso. Por tanto, la consistencia de un sistema de axiomas es necesaria para que dichos axiomas sean todos verdaderos, pero no es suficiente. Esto justifica que como L. E. J. Brouver, aunque desde otro punto de vista, digamos que «La certeza es más importante que la consistencia». Probablemente, el sistema de axiomas ZF+noCH es consistente pero no verdadero.

Ahora vamos a dar una idea de la anunciada demostración del primer teorema de incompletitud de Gödel, si bien para mayor sencillez en primer lugar desarrollaremos otra.

Sea A un sistema de axiomas finito o contable consistente y supongamos que la frase «el conjunto de los números reales no es contable» es una proposición verdadera. Entonces, si esta proposición P es un teorema de A, siendo $T(A)$ contable, se sigue que existe un número real que es una proposición verdadera que no es un teorema de A (conviene tener en cuenta que todo número real α se identifica con la proposición $\alpha = \alpha$). Por otra parte, si P no es un teorema de A, resultaría que la misma P sería una proposición verdadera que no es un teorema de A.

A. Tarski (izquierda) junto a K. Gödel.

Conviene recordar que el primer teorema de incompletitud de Gödel afirma que si A es un sistema lógico consistente con ciertas propiedades (en concreto, si es finitamente axiomatizable) y, por tanto, contable, que contiene los axiomas de la aritmética, entonces existe una proposición verdadera que no es un teorema de A.

De otro modo, sea A un sistema de axiomas consistente y contable. Entonces, si la frase «la clase de las proposiciones verdaderas no es un conjunto contable» es una proposición verdadera P, se sigue de igual forma que anteriormente que existe una proposición verdadera que no es un teorema de A, porque en el peor de los casos dicha proposición P sería una proposición verdadera que no es un teorema de A. Esta proposición está casi dentro del sistema lógico $T(A)$, generado por A, porque sólo se utiliza en ella la intuición de que la clase de las proposiciones verdaderas no es contable. Es claro que si esto fuese cierto o no se aceptase, sólo existiría un solo número cardinal infinito verdadero: el χ_0, y se renegaría de la obra de Cantor.

Como se sabe, la proposición de que el conjunto de los números reales no es contable es una consecuencia de la compleción del conjunto de los números racionales y de un razonamiento análogo al que establece el teorema de Baire. Por otra parte, si se admite que el conjunto de los números reales es contable, resulta que la medida de Lebesgue sobre $\mathbb{R}$ como suma de las medidas de sus subconjuntos unitarios es nula, con lo cual quedaría destruida gran parte de las matemáticas. Por tanto, la lógica matemática de primer orden de la teoría de la computabilidad es insuficiente para el desarrollo y estudio de las matemáticas. Por otra parte, la gran acogida filosófica que

ha tenido el teorema de Gödel en condiciones generales que se salen de su marco primitivo, impulsa a estudiar su generalización dentro del análisis matemático.

Ahora vamos a dar, por fin, la idea de la anunciada demostración clásica del primer teorema de incompletitud de Gödel. La idea central es sencilla, bella y profunda. La parte complicada consiste en codificar realmente las reglas de inferencia del sistema formal, y también el uso de sus diversos axiomas, en operaciones aritméticas. Consideremos ahora las funciones proposicionales que dependen de una sola variable. Sea P_n la n-ésima de estas funciones proposicionales. Si $P_n(w)$ es sintácticamente correcta será algún enunciado aritmético concreto perfectamente bien definido que concierne a los dos números naturales n y w. Cuál sea exactamente este enunciado dependerá de los detalles del sistema de numeración específico que hayamos elegido. Esto pertenece a la parte complicada del argumento y no nos interesa aquí. Las cadenas de proposiciones que constituyen una demostración de algún teorema en el sistema pueden ser etiquetadas también mediante números naturales utilizando el esquema de ordenación elegido. Denotaremos por Π_n la n-ésima demostración.

Consideremos ahora la siguiente función proposicional que depende del número natural w:

$$\neg\, \exists\, x\,[\Pi_x \text{ demuestra } P_w\,(w)]$$

El enunciado dentro del paréntesis cuadrado se da parcialmente en palabras, pero es un enunciado perfecta y exactamente bien definido. Afirma que la x-ésima demostración es realmente una demostración de la proposición que constituye $P_w(.)$ aplicada al propio valor w. El cuantificador existencial negado, fuera del paréntesis, sirve para eliminar una de las variables («no existe x tal que...»), de modo que nos queda una función proposicional aritmética que sólo depende de una sola variable w. La expresión global afirma que no existe demostración de $P_w(w)$.

John von Neumann.

Como hemos indicado, todas las funciones proposicionales que dependen de la variable w se pueden codificar, de modo que la que acabamos de escribir debe tener asignado un número natural n. Por consiguiente:

$$\neg\, \exists\, x\,[\Pi_x \text{ demuestra } P_w\,(w)] = P_n\,(w)$$

Examinemos ahora esta función para el valor particular $w = n$. Entonces:

$$\neg\, \exists\, x\,[\Pi_x \text{ demuestra } P_n\,(n)] = P_n\,(n)$$

La función específica $P_n(n)$ es un enunciado perfectamente bien definido en la aritmética (sintácticamente correcto). Aunque $P_n(n)$ es sólo una proposición aritmética, la hemos construido de modo que afirma lo que se ha construido en el lado izquierdo: «no existe demostración dentro del sistema, de la proposición $P_n(n)$». Entonces no puede haber ninguna demostración de esta $P_n(n)$ dentro del sistema. En efecto, si hubiera tal demostración, el significado del enunciado que $P_n(n)$ realmente afirma, a saber, que no existe demostración, sería falso, de modo que $P_n(n)$ tendría que ser falsa como proposición aritmética. Así hemos encontrado una proposición verdadera que no tiene demostración dentro del sistema. Es claro que siendo entonces $\neg P_n\,(n)$ una proposición falsa no se puede demostrar tampoco dentro del sistema. Así, ni $P_n(n)$ ni su negación $\neg P_n\,(n)$ son demostrables dentro del sistema.

El primer hecho descubierto por Gödel fue que el conjunto S de (los números de Gödel de) las proposiciones verdaderas en $\mathbb{N}$ de la aritmética no era definible, dentro del modelo estándar $\mathbb{N}$, por una fórmula aritmética con una sola variable libre. El motivo estaba en la posibilidad de construir una proposición aritmética cuyo significado era «esta proposición es falsa en $\mathbb{N}$», con lo que se caía en la misma contradicción que en la antigua *paradoja de Epiménides*. Este resultado se conoce hoy como metateorema de Tarski de indefinibilidad de la verdad dentro de un lenguaje formal adecuado.

Un análisis de la demostración del primer teorema de incompletitud de Gödel condujo a éste y, de manera independiente a Von Neumann, al llamado segundo teorema de incompletitud. En efecto, la formalización del primer teorema muestra que la única hipótesis sobre el sistema lógico es su propia consistencia, de modo que, si la consistencia de una aritmética suficientemente fuerte o exigente fuera demostrable dentro de esa misma aritmética, entonces la proposición indecidible sería demostrable a

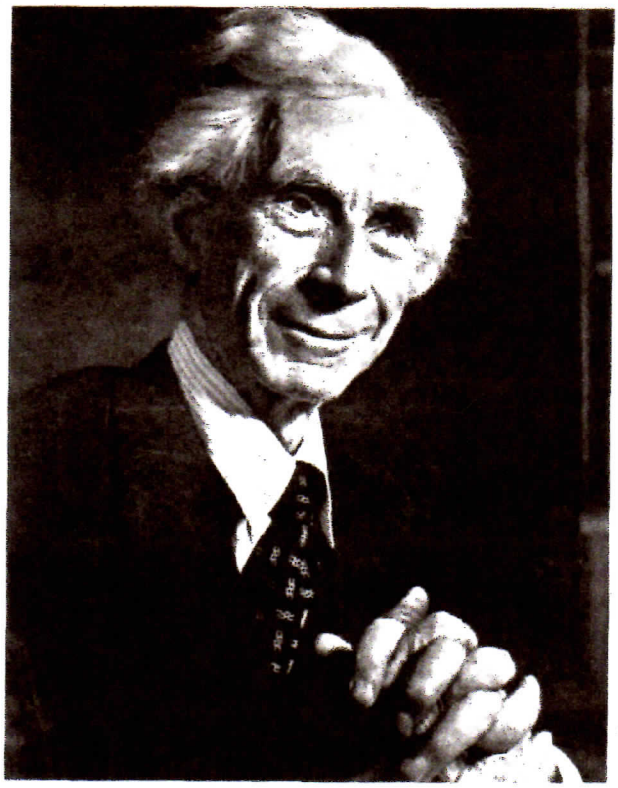
su vez. La consecuencia es inmediata: si la aritmética en cuestión es consistente, entonces dentro de ella misma no es demostrable esa consistencia. Este profundo resultado venía a resolver negativamente el problema planteado por Hilbert de demostrar por métodos finitarios la consistencia de la aritmética, puesto que los métodos finitarios quedan incluidos dentro de la aritmética.

La veracidad dada a las proposiciones aritméticas varía desde un carácter absoluto a un carácter relativo relacionado con su consistencia, pero ya hemos visto que existen algunos sistemas lógicos consistentes que contienen proposiciones no verdaderas. Más aún, B. Russell interpretó la demostración del teorema de Gödel como una prueba de la inconsistencia de la aritmética. En efecto, con las notaciones empleadas anteriormente, podríamos haber interpretado $P_n(n)$ como una proposición falsa que se puede demostrar mediante una Π_x. Pero esto nos lleva a un mundo caótico en el que evidentemente no estamos. Es más, nuestra intuición matemática nos lleva a dar un carácter absoluto a la veracidad de las proposiciones aritméticas.

Como Hilbert, pensamos que nadie puede expulsarnos del paraíso que Cantor ha creado, mejor encontrado, para nosotros. Pero tampoco puede quitarnos las ideas que sugieren los teoremas de incompletitud de Gödel. Efectivamente, antes de Cantor, había el *Homo sapiens*, pero con los números transfinitos surge el *Homo trans-sapiens*. Por ello vamos a dar una idea de los números ordinales transfinitos. Empecemos para ello poniendo a continuación de los números naturales $1, 2, ..., n, ...$ el elemento o número ordinal ω y a continuación $\omega + 1, ..., \omega + n, ..., 2\omega, ..., n\omega, ..., \omega^n, ...$, de modo que si hemos construido un segmento S de ellos, pondríamos a continuación un nuevo ordinal α. De esta forma, el conjunto S_α de los números ordinales menores que α tiene la propiedad que todo subconjunto no vacío de S_α tiene un primer elemento, propiedad que caracteriza a los conjuntos bien ordenados. Pues bien, la entrada a este paraíso está prohibida al formalismo porque los números ordinales no se admiten en él como proposiciones verdaderas.

Es corriente identificar todo número ordinal α con el conjunto formado por todos sus anteriores. Veamos cómo se pueden obtener dichos números dentro de las ideas de Gödel.

Sea S_0 el sistema lógico de la aritmética. Entonces, como todas las proposiciones de S_0 son verdaderas, se intuye que el enunciado T_1 de la consistencia de S_0 es verdadero. Sea S_1 el sistema lógico definido por el sistema de axiomas formado por las proposiciones de S_0 y T_1. Procediendo por inducción, supuestos construidos $S_0, ..., S_{n-1}$ y las proposiciones verdaderas $T_1, ..., T_{n-1}$, se define T_n como el enunciado de la consistencia de $\bigcup_{k<n} S_k$, el cual también por la veracidad de la aritmética debe ser una proposición verdadera, y se define S_n como el conjunto de los teoremas de $\bigcup_{k<n} S_k \cup \{T_n\}$. Este proceso se puede extender por inducción transfinita definiendo para cada ordinal α un sistema lógico S_α de modo que cada T_α es el enunciado de la consistencia de $\bigcup_{\beta<\alpha} S_\beta$ y cada S_α es el conjunto de los teoremas de $\bigcup_{\beta<\alpha} S_\beta \cup \{T_\alpha\}$, tratado formalmente T_α como si fuera una proposición. Entonces el sistema total $S = \bigcup_\alpha S_\alpha$, que por ser sugerido por Gödel llamaremos gödelización de la aritmética, debe existir y ser consistente por la veracidad de la aritmética, de modo que llamaremos proposición verdadera a toda $P \in S$. La intuición gödeliana nos dice que ningún S_α debe ser un sistema lógico completo y, por tanto, la familia (S_α) debe ser estrictamente creciente.



Bertrand Russell.

Se puede demostrar utilizando la codificación de Gödel y ordenaciones lexicográficas que S se puede bien ordenar de modo que a cada proposición $P \in S$ se puede asignar inyectivamente un número ordinal $o(P)$. Como consecuencia de ello se puede demostrar la siguiente generalización esperada del teorema de Gödel:

> El enunciado $E(A)$ de la consistencia de un conjunto $A \subset S$ de axiomas es una proposición verdadera que no es un teorema de A.

Dicha demostración se basa en el principio de inducción transfinita, pero se pueden dar otras demostraciones utilizando el lema de Zorn o bien sólo la axiomática de Zermelo-Fraenkel.

El proceso anterior aplicado al sistema lógico S_0 de la aritmética se puede generalizar aplicándolo a un sistema lógico S'_0 no disjunto con S_0, que sea un conjunto con tal que se admita el anterior teorema generalizado de Gödel. Entonces se obtiene un sistema lógico total S'. Pues bien,

el resultado más destacado es que $S' = S$; en otras palabras, que sólo hay una verdad en las matemáticas, ya que las proposiciones verdaderas de S y S' son las mismas.

Vamos a dar una idea de la demostración de dicha unicidad. Si $S'' = S \cap S'$ es un conjunto, se sigue la contradicción de que el enunciado $E(S'')$ de la consistencia de $S'' = S \cap S'$ es una proposición verdadera en S y S' y, por tanto, perteneciente a S'', que no es un teorema de S'', lo cual no es posible por ser S'' un sistema lógico. Entonces, $S'' = S \cap S'$ no es un conjunto, de donde teniendo en cuenta que es S'' un sistema lógico tal que $E(P) \in S''$ para toda proposición $P \in S''$, se sigue del teorema generalizado de Gödel que $S = S'' = S'$.

Así, si existe la verdad, la verdad es única. Pero la verdad se intuye y es un don: no se demuestra ni se puede demostrar. Es más, si se pudiese demostrar la existencia de la verdad, ella sería seguramente falsa porque está muy por encima de nuestras mentes. Lo que hemos dicho para la verdad, podríamos decirlo para Dios.

Justamente, Hilbert había descubierto que con respecto a una axiomática general la verificación de la consistencia interna en cuanto al contenido sólo podría ser relativa; es decir, sólo podría ser decidida mediante la construcción de un modelo. Pero como a su vez los elementos de este modelo son de tipo matemático, la consistencia de una teoría se reduce a la de otra. Nosotros decididamente, como hemos visto, siguiendo las ideas de Gödel profundizamos y repetimos indefinidamente este proceso en el transfinito teniendo como fruto la consistencia de los sistemas construidos, que todos son iguales, esto es, que no hay más que una sola verdad en las matemáticas. Resultando como consecuencia de la buena ordenación del sistema total S, que el axioma de Solovay no pertenece a S, lo cual expresaremos diciendo que es falso.

Como consecuencia de estos resultados, llamaremos orden de inconsistencia de un sistema lógico S'_0 al menor ordinal α, si existe, tal que, con notaciones análogas a las anteriores, S'_α es inconsistente. En el caso que todo sistema lógico S'_α sea consistente diremos que S'_0 es casi verdadero, reservando el nombre de verdadero cuando además S'_0 contiene los axiomas de la aritmética. De manera análoga se llama orden de inconsistencia de un sistema de axiomas A el orden de inconsistencia, si existe, del sistema lógico $T(A)$ de los teoremas de A.

Vamos a examinar esto. Dada una proposición P, sea S'_0 el sistema lógico generado por P y los axiomas A_0 de la aritmética. Entonces, si existe un ordinal α tal que S'_α es inconsistente, resulta que P es una proposición falsa; esto es, no pertenece a S. Por el contrario, si todo sistema lógico S'_α es consistente, siendo $S' = \bigcup_\alpha S'_\alpha = S$, se sigue que $P \in S$, es decir, que P es una proposición verdadera.

En particular, si P es el axioma de Solovay, como P es inconsistente con la buena ordenación de $\mathbb{R}$, resulta que el orden de inconsistencia de P es menor o igual que el primer ordinal α tal que el cardinal de $\{\beta : \beta < \alpha\}$ es igual que el cardinal c de $\mathbb{R}$.

Desde luego, la verdad es inaccesible al lenguaje y a la razón del hombre, pero la intuición nos aproxima mucho a ella. El hecho de que suponiendo realizable la gödelización S de la aritmética se tenga en las condiciones indicadas la unicidad $S' = S$ de la verdad matemática, nos indica que efectivamente estamos en el camino adecuado señalado por la intuición. Lo importante es conocer la verdad, no el camino por el que se llega a ella, aunque este camino puede ser interesante. El preocuparse de los métodos seguidos en las demostraciones es importante, pero no debe ser una barrera para llegar a la verdad. Para esto nos bastan una intuición bien adiestrada, una reflexión rigurosa y una belleza profunda.

La aparición de paradojas cuando se emplea la verdad absoluta hay que atribuirla a que se emplea en un sentido abstracto. La verdad absoluta sólo tiene sentido cuando se aplica en un sentido concreto. Esto se ve de manera muy clara con el axioma de las paralelas de la geometría que no es cierto ni falso, todo depende de la geometría que se considere. Igualmente, el argumento empleado por B. Russell en su paradoja se debe a que se aplica a universos abstractos, no concretos. El carácter abstracto de las matemáticas tiene muchas ventajas, porque con él se alcanza gran generalidad, pero es causa de paradojas. Esto justifica el platonismo de las matemáticas, no olvidando que los objetos matemáticos tienen un significado sin el cual las verdades pueden dejar de serlo.

El planteamiento de esta conferencia está de acuerdo con la perspectiva platónica de las matemáticas. Mientras que un formalista es libre de crear cualquier sistema lógico consistente, un platónico como Gödel sostenía que sólo un sistema de axiomas captaba las verdades que existían en el mundo platónico. Nuestros resultados, obtenidos utilizando la generalización del segundo teorema de incompletitud de Gödel para conjuntos basados en la intuición gödeliana con la que se establece el que llamamos «axioma de la consistencia», confirman dicha opinión. Y es que el carácter absoluto de la verdad matemática y la consistencia platónica de los conceptos matemáticos son esencialmente una misma cosa.

Nuestro espíritu debe ser como el que Hilbert manifestó en su *Debemos saber. Sabremos*, incorporando a la ciencia y a las matemáticas el paraíso de Cantor y también el sugerido por las ideas de Gödel.

BIBLIOGRAFÍA

1. Barrow, J. D. (1996) *La trama oculta del universo. Crítica.* Ed.: Grijalbo Mondadori, S. A., Barcelona.
2. Gödel, K. (1986) *Collected Works-Volume I: Publications 1929-1936.* Ed.: Oxford Univ. Press.
3. Penrose, R. (1991) *La nueva mente del emperador.* Ed.: Mondadori España, Madrid.
4. Rodríguez-Salinas, B. (Preprint) *A proof of fundamental theorem of Mathematics.*
5. Rodríguez-Salinas, B. (Preprint) *There is only one truth in Mathematics.*