Rev. Acad. Canar. Cienc., XVII (Núms. 1-2), 117-139 (2005) (publicado en agosto de 2006)

SOBRE LÓGICA Y MATEMÁTICAS: ALGUNAS OBSERVACIONES SOBRE LOS FUNDAMENTOS DE LA MATEMÁTICA

J. M. Almira

ABSTRACT. Several ideas related to the crisis on the foundations of mathematics which arose from the apparition of contradictions in set theory at the end of the XIX century are explained. We also focus our attention in the explanation of how the mathematical community faced a solution to these questions.

RESUMEN. Se explican algunas de las ideas vinculadas a la crisis de los fundamentos de la Matemática originada por las contradicciones que aparecieron en el seno de la teoría de conjuntos a finales del siglo XIX. También centramos nuestra atención en explicar cómo la comunidad matemática se enfrentó a la solución de estas cuestiones.

Este trabajo está dedicado al Prof. José Manuel Méndez Pérez,
con todo el cariño, de su alumno y amigo.

1. INTRODUCCIÓN: SOBRE LAS CRISIS EN MATEMÁTICAS

Existe, entre el público no especializado, el mito de que la matemática es una ciencia exacta y más precisamente, que se distingue del resto de las ciencias por expresar *verdades absolutas* (signifique esto lo que signifique). Gozamos, pues, de este privilegiado prestigio de pureza. Sin embargo, hemos pasado (como el resto de ciencias) por nuestras propias crisis. Detallo algunos ejemplos bien conocidos:

- Aparición de números irracionales.
- Fundamentos rigurosos para el Cálculo Infinitesimal.
- Creación de Geometrías No-Euclídeas.
- Crisis de los fundamentos asociada al desarrollo de la Teoría de Conjuntos.

En los ejemplos mencionados hay dos tipos de "crisis" bien diferenciados. De una parte, están aquéllas que, como en el caso del descubrimiento de los números irracionales o de la necesidad de introducir el rigor en numerosas partes del Cálculo Infinitesimal, se pueden resolver completamente mediante la introducción de nuevos conceptos matemáticos o, simplemente, mediante una revisión cuidadosa de lo que se conocía en la época. De otra parte, están las crisis que deben su origen a la aparición de paradojas lógicas y cuya solución, en algunos casos, aún no es completa. En particular, podemos destacar en este punto la crisis debida a la aparición de paradojas en el seno de la Teoría de Conjuntos (TC, abreviadamente).

El objetivo de este artículo es explicar las razones para dicha crisis, así como algunas de las direcciones en las que se han aportado soluciones (parciales). Finalmente, vamos a intentar cumplir con estos objetivos manteniendo un nivel elemental en la exposición.

2. QUÉ SON Y PARA QUÉ SIRVEN LOS NÚMEROS

La[1] naturaleza de los números reales no estuvo completamente clara[2] hasta finales del S. XIX y se logró, como resultado del esfuerzo de numerosos matemáticos, con la creación de un

[1]El título de esta sección hace una obvia alusión al famoso texto de Dedekind [9]

[2]Ya Euclides abordó el problema de la construcción de la recta real mediante su teoría de las proporciones.

proceso que luego se ha denominado Aritmetización del Análisis. Tras la creación del Cálculo Infinitesimal por Newton y Leibniz, y su desarrollo por Euler, Lagrange, Gauss y otros, se produjo una crisis. Primero Bolzano (1817) observó que las demostraciones (debidas a Gauss) del Teorema Fundamental del Álgebra no eran completamente rigurosas y estableció su propia demostración (basada de forma implícita en el axioma del supremo) de que si $f \in C[a,b]$ y $f(a)f(b) < 0$ entonces existe un $x \in (a,b)$ tal que $f(x) = 0$. Luego Cauchy (1821) redactó su famoso "Curso de Análisis" para "demostrar rigurosamente para las funciones continuas muchos resultados que se conocían verdaderos para los polinomios". Finalmente, Weierstrass, Heine, Cantor, Meray, etc. (1870-1872) lograron la aritmetización del Análisis, poniendo todo el peso de la verdad de las afirmaciones del Cálculo en la aritmética básica. Dicha reducción se logra básicamente de la siguiente forma: se introduce el conjunto $\mathbb{N}$ de los números naturales y a partir de él se dan los siguientes pasos: solución de ecuaciones $ax = \pm b$, $(a, b \in \mathbb{N})$, definición de valor absoluto, convergencia, sucesiones de Cauchy, etc. y construcción de $\mathbb{R}$ como el conjunto cociente formado por las clases de equivalencia de sucesiones de Cauchy de números racionales bajo la relación de equivalencia[3] $\{a_n\} \sim \{b_n\} \leftrightarrow \{a_n - b_n\} \to 0$. Ahora bien, si todo el Análisis se basa en la estructura de $\mathbb{N}$, podemos preguntarnos: ¿Qué es $\mathbb{N}$? No pensemos que estamos hablando de tonterías: $\mathbb{N}$ no fue fácil de definir sobre bases rigurosas. Probablemente el lector pensará que no podemos continuar este proceso de "bajada" de niveles indefinidamente: para poder avanzar en nuestra comprensión del mundo debemos fijar unas hipótesis mínimas sobre las que apoyarnos. Pero, ¿podemos suponer simplemente la existencia de los números naturales y partir de esta base para construir el resto de las matemáticas? Leopoldo Kronecker era de esta opinión[4]. Sin embargo, Georg Cantor, Gottlob Frege, Giussepe Peano, y otros, dedicaron bastante trabajo para lograr la fundamentación teórica del conjunto de los números naturales. Para lograr una definición formal del conjunto $\mathbb{N}$ se intentaron esencialmente las siguientes tres vías: El uso exclusivo de la Lógica (trabajo al que Frege dedicó su vida), el uso de la Teoría de Conjuntos, entendiendo que los conjuntos, en general, son objetos matemáticos más básicos o intuitivos que los números (esta vía fue explotada por Cantor y Dedekind) o, finalmente, partir de una concepción axiomática para $\mathbb{N}$. Esto significa que vamos a suponer que existe el conjunto $\mathbb{N}$ y que éste queda definido por iluminación, como el (único) objeto que satisface una serie de axiomas que hay que formular con total precisión. Este camino lo tomó G. Peano.

2.1. **¿Qué son los números naturales?** Como ya hemos comentado, ha habido varios intentos para resolver esta pregunta. Algunos, como el de Frege, están tan cerca de la filosofía que muchos lectores serán probablemente de la opinión de que "eso no son matemáticas". Otros, sin embargo, serán aceptados como "buenos" e incluso "ingeniosos" por un lector moderno. En esta sección vamos a comentar brevemente algunos de estos enfoques.

2.1.1. *Los números naturales según Frege.* Frege, en una primera aproximación, explica qué propiedades no puede tener un número, quizás con la idea de "cercar" el concepto lo más posible. Según Frege,

[3]Este proceso también fue denominado posteriormente *método genético* para la construcción de la recta real.

[4]Desafortunadamente, L. Kronecker se hizo famoso por su actitud agresiva contra G. Cantor y el uso de las técnicas desarrollas por él en su Teoría de Conjuntos, al realizar afimarciones del estilo de la siguiente: "Dios creó a los enteros, lo demás es obra del hombre". Sin embargo, no me resisto aquí a realizar una breve pero apasionada defensa de Kronecker. Él fue un gran matemático, y a él debemos algunos teoremas hermosos del Álgebra (más concretamente, de la Teoría de Números). Uno que me impresionó personalmente, cuando lo descubrí, afirma que si sobre un anillo A disponemos de un algoritmo de descomposición en producto de irreducibles, entonces también dicho algoritmo se puede extender para lograr la descomposición en irreducibles para los elementos de $A[x]$. Obsérvese que, en particular, este teorema de Kronecker proporciona un algoritmo para la descomposición en producto de polinomios irreducibles para los anillos $\mathbb{Z}[X_1, X_2, \cdots, X_n]$.

- Los números no son cosas materiales, ni agrupaciones de cosas materiales, ni propiedades de cosas materiales. Tampoco son algo subjectivo, ni se confunden con los signos que normalmente se utilizan para relacionarlos entre sí.
- Los enunciados numéricos dicen algo sobre ciertos conceptos, pero no sobre ciertos objetos. Por ejemplo, si decimos: "mesas que hay en esta sala", entonces bajo dicho concepto caen exactamente un cierto número de objetos (pero no importa, por ejemplo, el color de las mesas, o si éstas son de madera u otro material).

A partir de estas sencillas ideas, formuló los siguientes principios, para la definición de **número asociado a un concepto P**:

- El número 0 corresponde al concepto P si ningún objeto cae bajo P
- El número $n+1$ cae bajo el concepto P si hay un objeto $\mathcal{A}$ que cae bajo P y el número n cae bajo el concepto: "caer bajo P pero ser distinto de $\mathcal{A}$".

Si $\mathcal{C}$ es la clase de todos los conceptos, podemos definir:

Definición 1. *El concepto P es equipotente al concepto Q si existe una biyección entre los objetos que caen bajo P y los objetos que caen bajo Q. Los números cardinales son las clases de equivalencia asociadas a la relación anterior.*

Definición 2. *Una cosa es un número si y sólo si existe un concepto para el cual esta cosa es el número asociado a dicho concepto. Además, 0 es el número correspondiente al concepto: "distinto de sí mismo"; 1 es el número correspondiente al concepto "igual a cero". Finalmente, n es el siguiente de m significa que hay un concepto P y un objeto a que cae bajo P de modo que n es el número asociado a P y m es el número del concepto "cae bajo P y es diferente de a".*

De esta forma, los números que aparecen en la sucesión que empieza con 0 y continúa mediante el algoritmo que, dado x, calcula el siguiente a x, son (por definición) los elementos de $\mathbb{N}$.

G. Frege intentó formalizar el concepto de número natural basándose en la lógica. De hecho, podemos decir que los primeros avances significativos en lógica después de Aristóteles se deben a Frege, que creó la moderna lógica matemática. En particular, debemos a Frege la primera formulación precisa del cálculo de primer orden (introducción de los cuantificadores dentro de la lógica).

2.1.2. *Los números naturales según Cantor.* Por su parte, Cantor (1884) daba una definición de $\mathbb{N}$ a partir de la teoría intuitiva de conjuntos. Para ello, define:

Definición 3. *Los números naturales son los cardinales finitos. Un conjunto bien ordenado es finito si y sólo si su tipo de orden*[5] *es isomorfo a su tipo de orden inverso.*

Obviamente, la definición anterior deja bastante que desear pues, entre otras cosas, Cantor no dispone de una definición general de conjunto finito. (Su definición ni siquiera funciona para el tipo de orden de $\mathbb{Q}$).

Sin embargo, Dedekind daba una definición "buena" de infinito (y por tanto, de finito), que se puede utilizar para definir $\mathbb{N}$ en términos conjuntistas. Según Dedekind, A es infinito si existe $f : B \to A$ biyectiva con $B \subset A$, $B \neq A$.

2.1.3. *Peano y la axiomatización de* $\mathbb{N}$. Peano (1858-1932) publicó en (1889) sus "Principios aritméticos, expuestos según un nuevo método", donde formaliza el siguiente conjunto de axiomas para los números naturales $\mathbb{N}$:

[5]Como veremos más adelante, dos conjuntos bien ordenados tienen el mismo tipo de orden si existe una biyección entre ambos que conserva el orden. El tipo de orden inverso del orden $\leq$ es el dado por el orden $x \leq^* y \Leftrightarrow y \leq x$.

Axiomas de Peano

- 1 es un número natural.
- Todo número natural n tiene un sucesor $s(n)$.
- 1 no es el sucesor de otro número natural.
- Si $s(n) \neq s(m)$, entonces $n \neq m$.
- Sea $A \subset \mathbb{N}$. Si $1 \in A$ y además se tiene que $n \in A \Rightarrow s(n) \in A$, entonces $A = \mathbb{N}$.

Obviamente, el siguiente paso sería la definición de las operaciones básicas de la aritmética, algo que podemos lograr fácilmente mediante una definición recursiva gracias al último de los axiomas anteriores (llamado principio de inducción matemática). Para ello, bastará hacer lo siguiente:

Definición 4. *Las operaciones aritméticas de suma "$+$", producto "$\cdot$" y potenciación de números naturales, están dadas recursivamente por las siguientes reglas:*

- $n + 1 := s(n)$; $n + s(m) = s(n + m)$.
- $n \cdot 1 = n$; $n \cdot s(m) = (n \cdot m) + n$.
- $n^1 = n$; $n^{s(m)} = n^m \cdot n$.

La lógica desarrollada por Frege en su Ideografía, era excesivamente compleja (requería de una escritura no lineal, muy diferente del lenguaje natural usual, y, por tanto, resultaba muy difícil familiarizarse con ella). Quizás por ello, Peano intentó construir su propia notación. Este sistema sí que tuvo éxito entre los lógicos y los matemáticos. De hecho, es esencialmente el que utilizamos ahora. Sin embargo, cuando Peano intentó llevarlo a la práctica en sus clases, encontró ciertas dificultades. En palabras de J. Mosterín (ver [27]):

> El interés de Peano por la matemática y por los lenguajes artificiales se fundió en la creación de su sistema de notación lógica. Quienes no lo aceptaron fueron sus estudiantes. Peano daba por entonces clases de matemáticas en la academia militar de Turín y, cuando comenzó a utilizar el nuevo formalismo notacional en sus clases y apuntes, los estudiantes se revelaron y exigieron su marcha (a pesar de que trató de aplacarlos, ofreciéndoles un aprobado general). Ni por esas: la insurrección sólo se calmó con la expulsión de Peano que, en 1890, aceptó una plaza en la Universidad de Turín

3. Teoría informal de Conjuntos

Antes de discutir las paradojas que surgieron en el seno de la Teoría de Conjuntos, vamos a recordar brevemente algunos de los resultados que lograron demostrar la belleza y la utilidad de dicha teoría. Por el momento, supondremos que se han definido correctamente los conceptos: conjunto finito (y por tanto, infinito) y conjunto numerable.

Teorema 1 (Cantor, Dedekind). *$\mathbb{Q}$ es numerable. Es más, el conjunto $\mathcal{A}$ de los números algebraicos reales, i.e. los ceros $\alpha \in \mathbb{R}$ de polinomios $p(x) \in \mathbb{Z}[x]$, es numerable*[6].

Demostración. Veamos que $\mathbb{Q}$ es numerable. Para ello, observamos antes que existe una biyección $\varphi : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$. Esto se consigue mediante las siguientes reglas:

- $\varphi(0) = (0,0)$ y $\varphi(1) = (0,1)$
- Si $\varphi(n) = (a,b) \notin \{0\} \times \mathbb{N} \cup \mathbb{N} \times \{0\}$ y $\varphi(n-1) = (a+1, b-1)$, entonces $\varphi(n+1) = (a-1, b+1)$.

[6]Aunque este resultado fue originalmente publicado por Cantor, lo cierto es que la prueba del mismo se debe a Dedekind, quien se la comunicó por carta. Cantor se limitó a utilizar este resultado (unido a su prueba de que $\mathbb{R}$ no es numerable) para demotrar la existencia de un conjunto infinito de números trascendentes. Cantor no mencionó a Dedekind en sus publicaciones y esto produjo cierto distanciamiento entre ambos matemáticos. A pesar de que Dedekind nunca se quejó abiertamente, Cantor sí que realizó posteriormente, en correspondencia con Hilbert, algunos comentarios sobre el deterioro de su relación con Dedekind (ver [7]).

- Si $\varphi(n) = (a,b) \notin \{0\} \times \mathbb{N} \cup \mathbb{N} \times \{0\}$ y $\varphi(n-1) = (a-1, b+1)$, entonces $\varphi(n+1) = (a+1, b-1)$.
- Si $\varphi(n) = (0,b)$ y $\varphi(n-1) \notin \{0\} \times \mathbb{N}$ entonces $\varphi(n+1) = (0, b+1)$. Si $\varphi(n) = (a,0)$ y $\varphi(n-1) \notin \mathbb{N} \times \{0\}$ entonces $\varphi(n+1) = (a+1, 0)$.

Ahora, podemos visualizar $\mathbb{Q}$ como subconjunto de $\mathbb{N} \times \mathbb{N}$ (basta considerar la aplicación $p/q \to (p,q)$) y por tanto, como subsucesión de $\{\varphi(n)\}_{n=0}^{\infty}$.

Para estudiar la numerabilidad del conjunto de los números algebraicos, bastará demostrar que $\mathbb{Z}[x]$ es numerable y que la unión numerable de conjuntos finitos (para cada polinomio hay un número finito de ceros) es numerable. Las ideas son, sin embargo, similares a las utilizadas para probar que $\mathbb{Q}$ es numerable. □

Teorema 2 (Cantor). $\mathbb{R}$ *no es numerable. Consecuentemente, existen infinitos números trascendentes.*

Demostración. Primero, es fácil encontrar biyecciones entre $\mathbb{R}$ y $]0,1[$. Por tanto, basta probar que $]0,1[$ no es numerable. La idea es el famoso principio de diagonalización de Cantor. Supongamos que, por el contrario, $]0,1[= \{x_n\}_{n=0}^{\infty}$, donde

$$x_n = 0.a_{n0}a_{n1}a_{n2}\cdots a_{nn}a_{n(n+1)}\cdots. \ (a_{nk} \in \{0,1,\cdots,9\} \text{ para todo } n,k).$$

Entonces podemos hacer

$$y = 0.b_0b_1b_2b_3\cdots b_nb_{n+1}\cdots,$$

donde: $b_k = 0$ si $a_{kk} \neq 0$ y $b_k = 1$ si $a_{kk} = 0$, para todo k. Obviamente, $y \in]0,1[\setminus \{x_n\}_{n=0}^{\infty}$. □

Teorema 3 (Cantor). *Existe una biyección entre* $\mathbb{R}$ *y* $\mathbb{R}^n$ *para todo* $n \geq 1$.

Demostración. Vamos a hacerlo para $n = 2$. (La idea es la misma para el caso general). Por supuesto, de nuevo podemos cambiar $\mathbb{R}$ por $]0,1[$. Definimos la aplicación $\varphi :]0,1[\times]0,1[\to]0,1[$ como:

$$\varphi(0.a_1a_2a_3\cdots, 0.b_1b_2b_3\cdots) = 0.a_1b_1a_2b_2a_3b_3\cdots.$$

Es fácil comprobar que φ es biyectiva. □

Otro resultado en la misma dirección del teorema anterior (pero mucho más difícil, y cuya prueba omitimos) es el siguiente:

Teorema 4 (Peano). *Existe una curva continua y sobreyectiva* $\alpha : [0,1] \to [0,1] \times [0,1]$.

Relacionada con estos resultados está la pregunta: ¿Serán $\mathbb{R}$ y $\mathbb{R}^n$ espacios homeomorfos con sus respectivas topologías usuales, para $n > 1$? La respuesta es: No. De hecho basta observar que $\mathbb{R} \setminus \{0\}$ no es conexo, aunque $\mathbb{R}^n \setminus \{\mathbf{x}\}$ sí lo es, para todo $\mathbf{x} \in \mathbb{R}^n$, siempre que $n > 1$.

Sin embargo, costó mucho trabajo demostrar que[7]

Teorema 5 (Brouwer, 1911). *Si* $n \neq m$ *entonces* $\mathbb{R}^n$ *y* $\mathbb{R}^m$ *no son, con sus respectivas topologías usuales, homeomorfos.*

Otro importante resultado de carácter topológico es el siguiente

Teorema 6. *Supongamos que se satisface el axioma de elección. Si* K *es un compacto Hausdoff no vacío que no contiene puntos aislados, entonces* K *no es numerable.*

[7]Este teorema de Brouwer es muy importante: proporciona la verdadera justificación para el concepto de dimensión en topología, y fue muy aplaudido.

Nota. Obsérvese que si no exigimos que el espacio sea Hausdorff entonces hay compactos sin puntos aislados cuyo cardinal es el que se desee (basta tomar sobre un conjunto S arbitrario la topología indiscreta).

Demostración. Para verlo, vamos a construir una aplicación inyectiva de $\{0,1\}^{\mathbf{N}}$ en K.

Para nuestra prueba, necesitamos hacer uso del siguiente resultado de topología (cuya demostración no hacemos, por no estar especialmente relacionada con los métodos de teoría de conjuntos):

Lemma 1. *Si K es compacto y Haussdorff, entonces para cada $x, y \in K$, $x \neq y$, existen entornos abiertos O_x de x y O_y de y tales que $\overline{O_x} \cap \overline{O_y} = \emptyset$.*

Para cada $S \in \{0,1\}^n$, $n \in \mathbb{N}$, definimos $p_S \in K$ y $O_S \subseteq K$, abierto, como sigue:

P.0 Puesto que K es no vacío y sin puntos aislados es evidente que podremos encontrar $p, q \in K$, $p \neq q$. Tomemos $p_{(0)} = p$ y $p_{(1)} = q$. Asimismo puesto que K es regular, existirán $O_{(0)}, O_{(1)} \subseteq K$ abiertos tales que $p_{(0)} \in O_{(0)}$, $p_{(1)} \in O_{(1)}$ y $\overline{O_{(0)}} \cap \overline{O_{(1)}} = \emptyset$.

P.n Una vez seleccionados p_S y O_S para cierto $S = (s_1, s_2, \ldots, s_n) \in \{0,1\}^n$, consideremos

$$S_0 = (s_1, s_2, \ldots, s_n, 0) \quad \text{y} \quad S_1 = (s_1, s_2, \ldots, s_n, 1).$$

Puesto que K es compacto Hausdoff sin puntos aislados, es inmediato encontrar $p_{S_0}, p_{S_1} \in O_S$ y $O_{S_0}, O_{S_1} \subseteq O_S$ abiertos tales que $p_{S_0} \in O_{S_0}$, $p_{S_1} \in O_{S_1}$ y $\overline{O_{S_0}} \cap \overline{O_{S_1}} = \emptyset$.

Siguiendo este proceso iterativo podemos elegir para cada $S \in \{0,1\}^n$, p_S y O_S.

Tomemos ahora $S = (s_1, s_2, \ldots) \in \{0,1\}^{\mathbf{N}}$ y consideremos para cada $n \in \mathbb{N}$, $S_n = (s_1, s_2, s_3, \ldots, s_n$ $\{0,1\}^n$. Asociado a S_n podemos tomar ahora p_{S_n} y O_{S_n} tal y como quedó definido en el proceso iterativo anteriormente indicado (para una notación más conveniente, aceptaremos también que $O_{S_0} = K$). Obtenemos de esta manera una sucesión $\{p_{S_n}\}_{n \in \mathbf{N}}$. Puesto que K es compacto, el conjunto $\{p_{S_n} : n \in \mathbb{N}\}$ ha de tener al menos un punto de acumulación en K. Seleccionemos uno de tales puntos de acumulación y denotémoslo p_S.

Lo que realmente hemos hecho en el párrafo anterior es definir la aplicación

$$\begin{aligned} \Phi : \{0,1\}^{\mathbf{N}} &\to T \\ \Phi(S) &= p_S \end{aligned}.$$

Veamos ahora que esta aplicación es inyectiva. Para ello tomemos $S = (s_1, s_2, \ldots)$, $R = (r_1, r_2, \ldots) \in \{0,1\}^{\mathbf{N}}$, $S \neq R$. Sea $\alpha \in \mathbb{N}$ la primera posición en la que S y R difieren, es decir, $\alpha = \min\{n \in \mathbb{N} : S_n \neq R_n\}$. Por construcción, es evidente que $p_{S_\alpha}, p_{R_\alpha} \in O_{S_{\alpha-1}} = O_{R_{\alpha-1}}$, también que $O_{S_\alpha}, O_{R_\alpha} \subseteq O_{S_{\alpha-1}} = O_{R_{\alpha-1}}$, que $\overline{O_{S_\alpha}} \cap \overline{O_{R_\alpha}} = \emptyset$ y finalmente que para cualquier $n \geq \alpha$, $p_{S_n} \in O_{S_\alpha}$, $p_{R_n} \in O_{R_\alpha}$. De la última condición se sigue que cualquier punto de acumulación de las sucesiones $\{p_{S_n}\}_{n \in \mathbf{N}}$ y $\{p_{R_n}\}_{n \in \mathbf{N}}$ estará respectivamente en $\overline{O_{S_\alpha}}$ y $\overline{O_{R_\alpha}}$ con lo que $p_S \in \overline{O_{S_\alpha}}$ y $p_R \in \overline{O_{R_\alpha}}$ y como ambas clausuras son disjuntas deducimos que $\Phi(S) = p_S \neq p_R = \Phi(R)$. □

Teorema 7 (Cantor). *Sea X un conjunto. Entonces $\mathcal{P}(X) := \{A : A \subseteq X\}$ no es equipotente a X. Además, $\mathcal{P}(X)$ es equipotente a $\{0,1\}^X$.*

Demostración. Supongamos que existe $\varphi : X \to \mathcal{P}(X)$ sobreyectiva. Consideremos el conjunto:

$$A = \{a \in X : a \notin \varphi(a)\}.$$

Como $A \in \mathcal{P}(X)$ y φ es sobreyectiva, tenemos que existe $b \in X$ tal que $\varphi(b) = A$. Entonces se tiene que $b \in A$ si y sólo si $b \notin \varphi(b) = A$, lo que es absurdo. Se sigue que φ no puede ser sobreyectiva.

La segunda afirmación del teorema es fácil de probar. Basta observar que la aplicación que lleva $A \subset X$ a $\psi(A) = \psi_A : X \to \{0,1\}$, donde $\psi_A(x) = 0$ si $x \notin A$ y $\psi_A(x) = 1$ si $x \in A$, es biyectiva. □

Nota. Si $w = \#A$, donde $\#$ denota el cardinal, se suele denotar $\#\mathcal{P}(A) = 2^w$. (En el caso de conjuntos finitos, se produce la igualdad como consecuencia del Teorema del binomio de Newton y el concepto de número combinatorio).

Teorema 8 (Cantor-Bernstein). *Si existen aplicaciones inyectivas $f : M \to N$ y $g : N \to M$, entonces N y M son equipotentes.*

Corollary 2 (Cantor). *$\mathbb{R}$ y $\mathcal{P}(\mathbb{N})$ son equipotentes.*

Demostración. Las aplicaciones $f : \mathcal{P}(\mathbb{N}) \to (0,1)$ y $g : (0,1) \to \mathcal{P}(\mathbb{N})$ dadas por

$$\begin{aligned} f(A) &= 0,00\cdots01^{(a_1}0\cdots01^{(a_1+a_2}0\cdots; \\ &\quad \text{para } A = \{a_1 < a_2 < \cdots < a_n < \cdots\} \end{aligned}$$

y

$$g(0, b_1b_2b_3\cdots b_n\cdots) = \{1b_1, 2b_2, \cdots nb_n, \cdots\}$$

(donde, para la segunda función, nb_n denota el entero que se obtiene de añadir por la derecha el dígito $b_n \in \{0,1,\cdots,9\}$ al número n) son inyectivas □.

Demostración del Teorema de Cantor-Bernstein.

Sean $f : M \to N$ y $g : N \to M$ aplicaciones inyectivas. Definimos, para cada $A \subset M$ el conjunto

$$F(A) := M \setminus g(N \setminus f(A))$$

Supongamos que existe $A_0 \subset M$ tal que $F(A_0) = A_0$. Entonces $g(N \setminus f(A_0)) = M \setminus A_0$ y, por tanto,

$$f : A_0 \to f(A_0) \text{ y } g : N \setminus f(A_0) \to M \setminus A_0 \text{ son biyectivas.}$$

Se sigue que $\varphi(x) = f(x)$ (si $x \in A_0$) y $(= g^{-1}(x)$ si $x \notin A_0)$ es una biyección.

Para probar el teorema bastará, por tanto, demostrar que existe A con $F(A) = A$.

Lemma 3. *Sea $\{A_k\}_{k=0}^{\infty} \subset \mathcal{P}(M)$. Entonces*

$$F(\bigcap_{k\geq 0} A_k) = \bigcap_{k\geq 0} F(A_k)$$

Nota. El Lema se sigue de forma rutinaria de las leyes de Morgan.

Tomemos ahora $A_0 = \bigcap_{k=0}^{\infty} F^k(M)$. Claramente, $F^{k+1}(M) \subset F^k(M)$ para todo k. Usando el Lema 3, tenemos que:

$$F(A_0) = \bigcap_{k=0}^{\infty} F(F^k(M)) = \bigcap_{k=0}^{\infty} F^{k+1}(M) = A_0. \ \square$$

Nota. Se sigue que $\mathbb{R}$ no es numerable y que existe una sucesión infinita de números cardinales transfinitos distintos. ¿Es $\aleph_0 := \#\mathbb{N}$ el más pequeño? ¿Hay algún conjunto cuyo cardinal esté estrictamente entre $\mathbb{N}$ y $\mathbb{R}$, o todos los subconjuntos de $\mathbb{R}$ son forzosamente numerables o equipotentes a $\mathbb{R}$?

Nota. Otra consecuencia del Teorema de Cantor-Bernstein es que podemos ordenar la clase de los conjuntos (Clase Universal). En otras palabras, podemos ordenar cualquier familia de conjuntos. Para ello basta definir: $m \leq n$ (n,m números cardinales) si existe una aplicación inyectiva $f : X \to Y$, donde X, Y satisfacen $m = \#X$, $n = \#Y$.

4. Las paradojas

Hasta ahora sólo hemos descrito brevemente algunos resultados básicos de TC que en todo caso podrían servir para demostrar que la TC es interesante, y que contiene (a pesar de su planteamiento original, sencillo) numerosos resultados sorprendentes. Ahora vamos a explicar cómo surgen las paradojas en el seno de la TC.

La primera paradoja descubierta data de 1895 y se debe al propio Cantor (aunque éste no le dio demasiada importancia, probablemente[8] porque la paradoja surgió en una parte muy especializada de TC). Se trata de la imposibilidad de considerar el cardinal del conjunto de todos los conjuntos. Imaginemos que X denota dicho conjunto. Entonces, según un teorema anterior (debido a Cantor), $\#\mathcal{P}(X) < \#X$, pero por otra parte, si A es un conjunto arbitrario, $\#A < \#\mathcal{P}(A) \leq \#X$ (pues X contiene copias de $\mathcal{P}(A)$ por su propia definición) y, por tanto, tomando $A = X$ llegamos a que $\#\mathcal{P}(X) \leq \#X$, un absurdo. En esencia, podemos decir que la paradoja de Cantor consiste en observar que no es posible pensar en un número cardinal que sea mayor que todos los demás.

En 1897, Burali-Forti (que era asistente de Peano), descubrió una paradoja análoga a la de Cantor, pero esta vez relativa a los números ordinales.

En 1902 Russell escribía una carta a Frege en la que argumentaba lo siguiente: Existen clases (i.e., extensiones de conceptos) que no se pertenecen a sí mismas (e.g., la clase de los animales de granja no es un animal de granja) y otras que sí (e.g., la clase de los conceptos abstractos es un concepto ¿¡DEFANGED.3140 abstracto). Consideremos, pues, el siguiente concepto P: "ser una clase que no se pertenece a sí misma". Consideremos la clase R definida por P. ¿Cae R bajo P? La respuesta, evidente, es: R cae bajo P si y sólo si R no cae bajo P, lo que constituye una paradoja.

Esta paradoja estaba enraizada directamente en la suposición por parte de Frege de que dado un concepto (o propiedad), éste delimita perfectamente un conjunto, que es llamado su extensión y que consta precisamente de los objetos que poseen dicha propiedad. Frege admitió inmediatamente el error e intentó resolverlo. Es más, dedicó algún tiempo a intentar resolverlo e incluso lo reconoció públicamente en sus escritos. Al final de su vida, Frege escribía:

> Me he visto obligado a abandonar la idea de que la aritmética sea una rama de la lógica y por tanto que todo pueda ser demostrado lógicamente.

Con estas cosas, Frege sufrió mucho, llegando a padecer una crisis nerviosa considerable, y pasó el resto de sus días sumido en la amargura. Sobre este hecho, también al final de su vida, Russell escribía:

> Cuando pienso en actos de gracia e integridad, me doy cuenta de que no conozco nada comparable a la dedicación de Frege a la verdad. Estaba Frege dando cima a la obra de toda su vida, la mayor parte de su trabajo había sido ignorado en beneficio de hombres infinitamente menos competentes que él, su segundo volumen estaba a punto de ser publicado, y al darse cuenta de que su supuesto fundamental era erróneo, reaccionó con placer intelectual, reprimiendo todo sentimiento de decepción personal. Era algo casi inhumano, y un índice de aquello de lo que los hombres son capaces cuando están dedicados al trabajo creador y al conocimiento, y no al crudo afán de dominar y hacerse famosos.

Hay otras paradojas. Una de las más conocidas (y curiosas) se debe a Berry (un amigo de Russell, que era bibliotecario y aficionado a la lógica). Dice lo siguiente: Consideremos el conjunto A de los números naturales que no pueden definirse (en español) utilizando menos de cien palabras. (Este conjunto es no vacío porque el número de posibles definiciones en español que poseen menos de 100 palabras, es finito). Sea n el mínimo de dicho conjunto. Entonces

[8]Sobre este aspecto, no hay total acuerdo. No podemos saber a priori si Cantor sabía que esta paradoja iba más allá de ser un simple detalle técnico, o si afectaba o no al resto de la TC

n es "el menor número natural que no puede definirse (en español) utilizando menos de cien palabras" y, como lo hemos definido con menos de 100 palabras, $n \notin A$, pero esto contradice que $\mathbb{N}$ está bien ordenado. Esta paradoja es interesante porque su formulación no requiere (a primera vista)[9] una alusión directa a conjuntos demasiado grandes... ya que se basa completamente en la aritmética clásica.

Russell propuso una teoría para evitar las paradojas anteriores: la teoría de los tipos. Se trata de un argumento un tanto enrevesado, que permite clasificar los diferentes conjuntos que se puedan definir en términos de "tipos", de manera que se eviten definiciones que den lugar a círculos viciosos[10] (las definiciones circulares tienen como efecto aumentar "el tipo" de los conjuntos que definen).... Pero a pesar de que desarrolló su teoría bastante en sus famosos Principia Mathematica, su teoría siempre despertó cierta desconfianza en la comunidad matemática. La verdadera "solución" al problema de las paradojas ha sido la creación de las diferentes teorías axiomáticas de conjuntos, desarrolladas a principios del S. XX por Zermelo, Fraenkel y luego por Neumann, ¿¡DEFANGED.3141 Bernays y Gödel.

5. Teorías Axiomáticas de Conjuntos

Vamos a explicar el papel de las teorías axiomáticas de conjuntos en palabras del profesor J. Sanmartín (ver [33]):

> Desde el descubrimiento de las paradojas en el seno de la teoría cantoriana de conjuntos se ha impuesto una manera de "pasarlas por encima": las teorías axiomáticas de conjuntos. Las paradojas nacen del empleo de un principio de comprehensión que permite afirmar como existente cualquier reunión de un todo de objetos (perceptibles o pensables) que satisfagan cierta propiedad. A una reunión tal se denomina "conjunto". Por el principio mencionado, se supone una perfecta correspondencia entre conjuntos y propiedades. Russell mostraría que hay al menos una propiedad, $x \notin x$, que no determina ningún conjunto, si no se quiere caer en contradicción. La consecuencia: 1) hay que fijar condiciones sobre qué propiedades son admisibles para "determinar" conjuntos, o 2) ensayar, como ocurre en las teorías axiomáticas de conjuntos, la creación de un sistema de principios a través de los cuales la noción primitiva de conjunto sea en cierta forma "iluminada" ("definida implícitamente", como se dice en ocasiones). Este segundo camino conlleva la obligación de dar una prueba de consistencia del sistema axiomático en cuestión. Dos de tales sistemas son cultivados hoy día preferentemente: Zermelo-Fraenkel (abreviado, ZF) y von Neumann-Bernays-Gödel (abreviado, NBG). Para ninguno de los dos ha sido dada una prueba tal de consistencia. Todo lo más que puede decirse es que en ellos no ocurren las paradojas de tipo ruselliano por evitarse en ellos la posibilidad de afirmar como existentes los conjuntos omnicomprehensivos (el conjunto de todos los conjuntos que ...). Pero ello no significa que tales sistemas se hayan librado en general de paradojas. De ahí nuestra frase del principio, pues, sólo si hubiera una prueba de consistencia tal, podría decirse con sentido que los sistemas axiomáticos eliminan las paradojas, y una prueba tal de consistencia para ellos ni la hay ni, por Gödel, parece que pueda haberla.

En otras palabras: la necesidad de resolver las paradojas que habían sido descubiertas entre 1895 y 1905 en TC, tuvo como consecuencia una nueva revisión de los fundamentos de la matemática, y se llegó a la conclusión de que el camino más firme para avanzar en matemáticas pasaba por el establecimiento de una axiomática para TC similar a las conocidas para la Geometría, así como por la justificación del uso de dicha axiomática (y no otra), lo que dio lugar a la definición y el estudio de una serie de propiedades "básicas" que debe satisfacer cualquier sistema de axiomas que se tome (i.e., consistencia, completitud, adecuación, coherencia, etc.) Como ya hemos mencionado, hubo varias propuestas de axiomáticas para TC. Por otra parte,

[9]En realidad, esto no es así. Pienso que: "ser definible, en español, con menos de cien palabras" no es una propiedad expresable en el lenguaje de la aritmética... ¿o me equivoco?

[10]Para más detalles sobre Russell y la teoría de tipos, recomiendo consultar [25].

D. Hilbert (que en 1899 había publicado una axiomática completa para la Geometría Euclídea -mucho más solida que la ofrecida por Euclides en la antigua Grecia-), desarrolló los conceptos necesarios para el estudio de las propiedades formales de las axiomáticas: es lo que entonces se llamó "teoría de la prueba" y actualmente conocemos como "metamatemática".

En esta sección vamos a presentar los axiomas ZF y NBG de TC, a explicar algunos resultados relacionados con el Axioma de Elección (abrev., AC) y la hipótesis del contínuo (abrev., HC), así como a abordar los conceptos fundamentales de la metamatemática desarrollada por Hilbert. Finalmente, daremos cuenta de los resultados obtenidos por Gödel y Cohen.

5.1. **Axiomas de Zermelo-Fraenkel y de Newman-Bernays-Gödel.** Comenzamos detallando los axiomas para la teoría de Zermelo y Fraenkel y para la teoría de Neumann, Bernays y Gödel. ¿¡DEFANGED.3142

5.1.1. *Axiomas de Zermelo-Fraenkel.* En este caso, los conceptos primitivos son: "conjunto" ,"$\in$" y "=". Los axiomas son los siguientes:

ZF1 (Axioma de Extensión) Si a y b son conjuntos y para todo conjunto x se tiene que $x \in a \Leftrightarrow x \in b$, entonces $a = b$.

Nota. Escribimos $a \subseteq b$ si $x \in a \Rightarrow x \in b$.

ZF2 (Esquema de Axiomas de los subconjuntos) Para todo conjunto a y toda propiedad p, existe un conjunto b tal que $x \in b$ si y sólo si $x \in a$ y $p(x)$ (i.e., x tiene la propiedad p).

Nota. Hay que recalcar que **ZF2** supone una restricción importante sobre el principio de extensionalidad de Frege, por la razón de que se fija a priori el conjunto a. Así, se evita la paradoja de Russell de la siguiente forma: con la propiedad $\notin$, sólo podemos formar conjuntos de la forma: $b = \{x \in a : x \notin x\}$. Ahora, se sigue que $b \in b$ no es posible (pues $b \in b$ implica $(b \in a) \wedge (b \notin b)$, lo que llevaría a contradicción). Se sigue que $b \notin b$ y, de la definición de b, $b \notin a$. El esquema de axiomas no produce contradicción y, lo que es más, sirve para probar que dado un conjunto a, hay otro conjunto b tal que $b \notin a$.

ZF3 (Axioma de la formación de pares) Si a y b son conjuntos, entonces existe otro conjunto c tal que $a \in c$ y $b \in c$.

Nota. Se sigue que, con la notación del axioma, podemos formar el conjunto $\{x \in c : x = a \vee x = b\}$. Dicho conjunto se suele denotar por $\{a, b\}$. Ahora podemos definir $< a, b >= \{a, \{a, b\}\}$.

ZF4 (Axioma de la unión) Si a y b son conjuntos, entonces existe otro conjunto c tal que si $x \in a$ o $x \in b$, entonces $x \in c$.

ZF5 (Axioma de las partes) Si a es un conjunto, entonces existe un conjunto b tal que si $x \subseteq a$ entonces $x \in b$.

Nota. Podemos, por tanto, definir $\mathcal{P}(a) = \{x \in b : x \subseteq a\}$ (que no depende de la elección de b). Pero es también interesante observar que, gracias al axioma **ZF5** podemos definir productos cartesianos: para ello necesitamos, dados a y b conjuntos, encontrar un conjunto c tal que, si $(x \in a) \wedge (y \in b)$, entonces $(x, y) \in c$ (en tal caso, definiríamos $a \times b = \{(x, y) \in c : (x \in a) \wedge (y \in b)\}$). Pero si $(x \in a) \wedge (y \in b)$ entonces $(x, y) = \{x, \{x, y\}\} \in \mathcal{P}(a \cup b)$ y, por tanto, podemos tomar $c = \mathcal{P}(a \cup b)$.

Una vez se ha definido el producto cartesiano de conjuntos, se pueden introducir los conceptos de relación, función, etc.

ZF6 (Axioma del infinito) Existe un conjunto a que tiene la siguiente propiedad:

$$(\emptyset \in a) \wedge (\forall x \in a, x \cup \{x\} \in a).$$

(Estos conjuntos se dicen "inductivos". Si x es un conjunto, denotamos $x^+ = x \cup \{x\}$).
Nota. A partir de **ZF6**, se puede definir

$$\mathbb{N} = \{x \in a : x \in b \text{ para todo conjunto inductivo } b\}$$

En particular, podemos definir $0 = \emptyset$, $1 = 0^+ = \{\emptyset\}$, $2 = 1^+ = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$, $3 = 2^+ = \{0, 1, 2\}$, etc.

ZF7 (Axioma de elección) Para todo conjunto a existe una aplicación $\varphi : \{x \in \mathcal{P}(a) : x \neq \emptyset\} \to a$ tal que $\varphi(x) \in x$ para todo $x \in \mathcal{P}(a) \setminus \{\emptyset\}$.
Nota. Téngase en cuenta que $\emptyset$ está bien definido a partir de **ZF2** (una vez suponemos que existe algún conjunto a), pues $\emptyset = \{x \in a : x \neq x\}$. Otra notación usual para **ZF7** es AC. Aún no hay pleno acuerdo sobre si incluir AC o no en la axiomática. Sobre ello, discutiremos ampliamente en otras secciones.

ZF8 (Esquema de los axiomas de Sustitución) Si p es una propiedad de pares de conjuntos tal que para todo $x \in a$, la afirmación de dicha propiedad para (x, y) y (x, z) implica $y = z$, entonces existe un conjunto b tal que $y \in b$ si y sólo si existe $x \in a$ tal que (x, y) verifica p.

ZF9 (Esquema de los axiomas de Restricción) Si p es una propiedad de conjuntos tal que existe un conjunto a que la verifica, entonces existe un conjunto b que verifica p tal que $\forall x \in b : \neg p(x)$.

Si admitimos todos los axiomas anteriores, nos referimos a la correspondiente axiomatización como[11] ZFC. Si eliminamos el axioma de elección, nos referimos a la correspondiente teoría como ZF.

Por otra parte, es interesante observar que si cambiamos el axioma **ZF6** por su negación, es decir, si negamos la existencia de conjuntos infinitos aún a pesar de admitir conjuntos finitos de tamaño tan grande como se desee, lo que equivale a rechazar la existencia de un infinito actual manteniendo la validez de un infinito potencial, entonces lo que obtenemos es una teoría axiomática equivalente a la aritmética de Peano. La "verdadera" teoría de conjuntos empieza, por tanto, cuando asumimos el axioma del infinito (ver [23] para una interesante discusión de estos temas).

5.1.2. *Axiomas de Neumann-Bernays-Gödel.* En este caso, los conceptos primitivos son: "clase", "conjunto" y la relación de pertenencia "$\in$". Remitimos a [16, pp.234-238], [30] para ver la axiomática completamente formalizada.

5.2. **Primera aproximación al axioma de elección. Paradoja de Banach-Tarski.** Una pregunta importante, que surge de forma natural una vez se ha definido la relación $\leq$ para los cardinales, es la siguiente: Dada una familia de conjuntos $\{A_i\}_{i \in I}$, ¿es $\leq$ un orden total? (En tal caso, diremos que se satisface la propiedad de buena ordenación de cardinales).

La respuesta, sorprendentemente, es que la buena ordenación de cardinales es equivalente al axioma de elección.

Teorema 9. *Son equivalentes:*

(AC) *Axioma de elección.*
(LZ) *Lema de Zorn (i.e., existencia de elementos maximales para los conjuntos cuyas cadenas*[12] *poseen maximales)*
(AZ) *Axioma de Zermelo (i.e. todo conjunto puede ser bien ordenado)*
(BO) *Buena ordenación de cardinales*

[11] De: Zermelo, Fraenkel y "Choice" (i.e., elección)
[12] Una cadena de A es un subconjunto totalmente ordenado de A.

Se sigue que el axioma de elección, aunque de enunciado muy sencillo y "creible", es equivalente a varios resultados cuya evidencia no es en absoluto patente. Piénsese, por ejemplo, que aún no se conoce un buen orden para $\mathbb{R}$.

A continuación vamos realizar un esbozo de la demostración de uno de los resultados más sorprendentes (por anti-naturales) que existen gracias al uso del axioma de elección. Se trata de la famosa paradoja de Banach-Tarski y tiene que ver obviamente con la existencia de conjuntos no medibles (i.e., con la imposibilidad de asignar una medida a todos los subconjuntos de $\mathbb{R}^3$).

Comenzamos introduciendo alguna notación:

Definición 5. *Decimos que dos conjuntos $A, B \subset \mathbb{R}^3$ son congruentes si existe un movimiento rígido del espacio $T \in \mathbf{Iso}(\mathbb{R}^3)$ tal que $T(A) = B$. En tal caso, utilizamos la notación $A \equiv B$. Por otra parte, decimos que $A \equiv^n B$ si existen familias de conjuntos disjuntos $\{A_i\}_{i=1}^n$ y $\{B_i\}_{i=1}^n$ tales que $A = \cup_{i=1}^n A_i$, $B = \cup_{i=1}^n B_i$ y $A_i \equiv B_i$ para $i = 1, \cdots, n$. Finalmente, decimos que $A \equiv_<^n B$ si existe $B' \subset B$ tal que $A \equiv^n B'$.*

Es fácil comprobar la siguiente propiedad:

- Supongamos que $A \cap C = \emptyset$, $D \cap B = \emptyset$. Entonces $A \equiv^n B$ y $C \equiv^m D$ implican $A \cup B \equiv^{n+m} C \cup D$. La misma propiedad se satisface para las relaciones $\equiv_<^n$ y $\equiv_<^m$.

Un poco más sorprendente es el siguiente resultado:

- Supongamos que $A \equiv_<^m B \equiv_<^n A$. Entonces $A \equiv^{n+m} B$.

Ya podemos establecer el resultado principal de esta sección:

Teorema 10 (Paradoja de Banach-Tarski). *Sean $\mathbf{B}_i \subset \mathbb{R}^3$ $(i = 1, 2)$ dos bolas unitarias de $\mathbb{R}^3$, disjuntas. Entonces $\mathbf{B}_1 \equiv^9 \mathbf{B}_1 \cup \mathbf{B}_2$.*

Para demostrar este teorema, necesitamos algunos resultados que enunciamos sin probar:

Lemma 4. *Sea $\mathbb{D} \subset \mathbb{R}^2$ el disco unitario cerrado. Entonces*

$$\mathbb{D} \equiv^{n+2} \mathbb{D} \cup \bigcup_{k=1}^{n} \{k\} \times (0, 1]$$

Lemma 5. *Sea $\mathbf{S}^2 \subset \mathbb{R}^3$ la esfera unitaria con centro en el origen de coordenadas y sea $D \subset \mathbf{S}^2$ un subconjunto numerable y $D' = \mathbf{S}^2 \setminus D$ su complementario. Entonces $\mathbb{S}^2 \equiv^2 D'$.*

Demostración de la Paradoja de Banach-Tarski. Sea $\mathbf{B}_1 \subset \mathbf{R}^3$ la bola unitaria de centro el origen 0 y sea $\mathbf{S}_1^2 = \partial \mathbf{B}_1$ la esfera unitaria. Tomemos α la rotación de π radianes respecto del eje xz y β una rotación de $2\pi/3$ radianes respecto de un cierto eje del plano oxz que elegimos de forma que las únicas relaciones que hay en el grupo (generado, mediante la composición de funciones, como subgrupo de $\mathbf{Iso}(\mathbb{R}^3)$) $G =< \alpha, \beta >$ son las obvias: $\alpha^2 = 1_d$ y $\beta^3 = 1_d$. (Esto se puede hacer porque hay un conjunto no numerable de ejes a elegir en el plano oxz).

Obviamente, si $\gamma \in G \setminus \{1_d\}$, entonces, bien

$$\gamma = \alpha\beta^{\epsilon_1}\alpha\beta^{\epsilon_2}\cdots (\text{ donde el producto es finito y } \epsilon_i \in \{1, 2\} \text{ para todo } i),$$

o bien,

$$\gamma = \beta^{\epsilon_1}\alpha\beta^{\epsilon_2}\alpha\beta^{\epsilon_3}\cdots (\text{ donde el producto es finito y } \epsilon_i \in \{1, 2\} \text{ para todo } i).$$

Además, si $\gamma \in G \setminus \{1_d\}$, entonces γ es una rotación respecto de algún eje y, por tanto, podemos considerar el conjunto D de los puntos de $\mathbf{S}_1^2$ que pertenecen a alguno de estos ejes. Oviamente, $D \subset \mathbf{S}_1^2$ es numerable. Además $\delta(D) = D$ para todo $\delta \in G$ (pues, si x pertenece al eje asociado a γ, entonces $\gamma(x)$ pertenece al eje asociado a $\delta\gamma\delta^{-1}$). Además, si $D' = \mathbf{S}_1^2 \setminus D$ y $x \in D'$, $\gamma \in G \setminus \{1_d\}$, entonces $\gamma(x) \neq x$.

Consideremos, por tanto, las órbitas $S_x = \{\gamma(x) : \gamma \in G\}$. Si $S_x \neq S_y$, $x, y \in D'$, entonces es claro que $S_x \cap S_y = \emptyset$ y, por tanto, disponemos de una relación de equivalencia $\sim$ sobre D'. **Podemos usar entonces el axioma de elección para seleccionar un elemento de cada clase de equivalencia del conjunto $D'/\sim$, formando el conjunto $T \subset D'$ de los representantes de dichas clases.** A continuación, procedemos de la siguiente forma: Definimos los conjuntos:

$$\begin{aligned} A &= \{\gamma(t) : t \in T \text{ y } \gamma = 1_d \text{ o bien } \gamma = \alpha\beta^{\epsilon_1}\cdots\} \\ B &= \{\gamma(t) : t \in T \text{ y } \gamma = \beta\alpha\beta^{\epsilon_2}\cdots\} \\ C &= \{\gamma(t) : t \in T \text{ y } \gamma = \beta^2\alpha\beta^{\epsilon_2}\cdots\} \end{aligned}$$

Entonces es fácil comprobar que $D' = A \cup B \cup C$. Además $\beta(A) = B$, $\beta(B) = C$, $\beta(C) = A$ y $\alpha(B) \cup \alpha(C) \subset A$ (en sentido propio, pues no estamos utilizando la identidad). Se sigue que $B \cup C \equiv^1_< A$, $A \equiv^1 B$, $B \equiv^1 C$ y $C \equiv^1 A$. Por tanto, teniendo en cuenta el Lema 5,

$$D' = A \cup (B \cup C) \equiv^2_< B \cup (C) \equiv^1_< A,$$

lo que nos lleva a afirmar que $D' \equiv^2_< A$. De forma análoga, se ve que $D' \equiv^2_< B$.

Por otra parte, utilizando el Lema 5, se tiene que $\mathbf{S}^2_1 \equiv^2 D' \equiv^2_< A$ y, por tanto, $\mathbf{S}^2_1 \equiv^4_< A$.

Si denotamos por $\mathbf{B_2}$ una bola unitaria disjunta de $\mathbf{B_1}$ y por $\mathbf{S}^2_2$ su borde (que es una esfera unitaria), es claro que $\mathbf{S}^2_2 \equiv^1_< B$. Se sigue que $\mathbf{S}^2_1 \cup \mathbf{S}^2_2 \equiv^8_< A \cup B$.

Definamos los conjuntos

$$\begin{aligned} \overline{A} &= \{x \in \mathbf{B}_1 \setminus \{0\} : \frac{x}{\|x\|} \in A\} \\ \overline{B} &= \{x \in \mathbf{B}_1 \setminus \{0\} : \frac{x}{\|x\|} \in B\}. \end{aligned}$$

Ahora es claro que

$$\mathbf{B}_1 \setminus \{0\} \cup \mathbf{B}_2 \setminus \{\mathbf{O}\} \equiv^8_< \overline{A} \cup \overline{B},$$

donde $\mathbf{O}$ es el centro de $\mathbf{B_2}$. Si llevamos ahora el origen 0 sobre sí mismo y el punto $\mathbf{O}$ sobre cualquier punto de $\mathbf{B}_1 \setminus (\overline{A} \cup \overline{B})$, obtenemos que

$$\mathbf{B}_1 \cup \mathbf{B}_2 \equiv^9_< \mathbf{B}_1.$$

Pero $\mathbf{B}_1 \equiv^1_< \mathbf{B}_1 \cup \mathbf{B}_2$ y, por tanto,

$$\mathbf{B}_1 \cup \mathbf{B}_2 \equiv^9 \mathbf{B}_1,$$

que es lo que queríamos demostrar. □

Una de las consecuencias obvias del teorema que se acaba de demostrar (y que tiene importancia en varias ramas de las matemáticas) es que, si aceptamos el axioma de elección (y por tanto el teorema anterior es cierto), entonces es imposible extender la medida de Lebesgue (exigiendo aditividad finita) a todos los subconjuntos del espacio $\mathbb{R}^3$. Es interesante observar que esta afirmación no es cierta en $\mathbb{R}^2$. Además, si se exige la propiedad de aditividad numerable, entonces ni siquiera es posible extender la medida a todos los subconjuntos de la recta real. Esto fue probado por Lebesgue en 1903.

5.3. **Conjuntos finitos y conjuntos numerables: el problema de Souslin.** Uno de los primeros escollos importantes que nos encontramos en el desarrollo de la teoría de conjuntos es la definición de conjunto finito. Aunque esto podría parecer sorprendente a cualquiera, ya que más o menos todo el mundo tiene claro qué entiende por "finito", resulta que en TC aprenderemos rápidamente que nada es tan sencillo como podría parecer a primera vista. De hecho, el axioma

de elección juega un papel importante (estabilizador) en relación con el concepto de conjunto finito.

Evidentemente, si se parte de que conocemos el conjunto $\mathbb{N}$ de los números naturales[13], no habrá problemas para definir los conjuntos finitos. Se procede de la siguiente forma:

Definición 6. *Decimos que $S \subset \mathbb{N}$ es un segmento inicial de $\mathbb{N}$ si $S = \{x \in \mathbb{N} : x \leq n\}$ para cierto $n \in \mathbb{N}$. Un conjunto (ahora arbitrario) A será finito si y sólo si es equipotente a algún segmento inicial de $\mathbb{N}$.*

Sin embargo, podríamos abordar el problema de la finitud de otra forma. La idea, sencilla, es: busquemos alguna propiedad que caracterice los conjuntos finitos definidos anteriormente, pero que no requiera utilizar el conjunto $\mathbb{N}$. Es decir: buscamos una propiedad abstracta que caracterice completamente la propiedad que nosotros conocemos intuitivamente como "ser finito", y utilicemos esta propiedad para nuestra definición. (Después de todo, esto es una técnica bastante habitual en matemáticas). Esta idea ha dado lugar a varias definiciones de "conjunto finito". El papel que juega el axioma de elección en este tema es fundamental: todas las definiciones de "finito" que se conocen son equivalentes bajo AC, pero no todas son equivalentes si excluimos AC de nuestro sistema de axiomas. Por tanto, si AC no se asume en nuestra axiomática, habrá varios conceptos (o niveles) de "finitud" y, por tanto, en dicho contexto muchos conceptos matemáticos (como, por ejemplo, la compacidad) deben ser analizados con cuidado (ver [8]). El siguiente teorema resume algunos de los conceptos de finitud más importantes que existen en la literatura especializada:

Teorema 11. *Supongamos que se satisface el axioma de elección y sea $A \neq \emptyset$. Entonces son equivalentes las siguientes afirmaciones:*

- *A es equipotente a un segmento inicial de $\mathbb{N}$.*
- **(Dedekind, 1888)** *No existen un subconjunto propio $B \subset A$ y una aplicación $f : B \to A$ tal que f es biyectiva.*
- **(Tarsky, 1924)** *Cada familia de subconjuntos de A tiene un elemento minimal respecto de la inclusión $\subseteq$*
- **(Levy, 1981)** *Existe alguna relación de orden total en A y todo orden total para A es un buen orden.*
- **(Klaua, 1979)** *Existe alguna relación de buen orden en A cuya inversa es también una relación de buen orden.*

Por otra parte, si admitimos como cierto el axioma de elección, entonces tendremos problemas con el estudio de las propiedades básicas de los conjuntos numerables. Para verlo, comenzamos planteando una pregunta aparentemente inocente. Si $(X, \leq)$ es un conjunto sobre el que se ha definido un orden parcial $\leq$, entonces asociados a dicho orden se pueden introducir dos tipos de subconjuntos de X especialmente interesantes: las cadenas y las anticadenas. Una cadena es un subconjunto $S \subset X$ que está totalmente ordenado por el orden de X y una anticadena es un subconjunto $A \subset X$ con la propiedad de que sus elementos son, con el orden de X, incomparables dos a dos. No es difícil probar el siguiente resultado

Teorema 12. *El conjunto parcialmente ordenado $(X, \leq)$ es finito si y sólo si todas sus cadenas y anticadenas son conjuntos finitos.*

Pero entonces podríamos formular de manera natural la siguiente pregunta: ¿será cierto que un conjunto parcialmente ordenado $(X, \leq)$ es contable (i.e., numerable o finito) si y sólo si todas sus cadenas y anticadenas son conjuntos contables? Sorprendentemente, la respuesta a esta

[13]Podemos suponer, por ejemplo, que hemos definido $0 = \#\emptyset$, $1 = \#\{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$, etc.

pregunta es un rotundo no. Para verlo, basta comprobar que si tomamos sobre $\mathbb{R}$ el orden de Sierpinski $a \leq_s b \Leftrightarrow (a \leq b \text{ y } a \leq_* b)$, donde $\leq$ representa el orden usual de $\mathbb{R}$ y $\leq_*$ es un buen orden para $\mathbb{R}$, entonces todas las cadenas y anticadenas de $(\mathbb{R}, \leq_s)$ son numerables.

Evidentemente, el ejemplo anterior resulta un tanto forzado, entre otras cosas, porque nadie conoce un buen orden para $\mathbb{R}$ (aunque la existencia de dicho orden se sigue del axioma de elección). Podríamos preguntar, por tanto, si añadiendo algún tipo de restricción natural sobre el orden $\leq$ de X, la numerabilidad de X se sigue de la numerabilidad de sus cadenas y sus anticadenas. En particular, ¿será cierto esto si $(X, \leq)$ es un árbol? Recordemos que el conjunto parcialmente ordenado $(X, \leq)$ es un árbol si para cada $x \in X$ sus predecesores $\mathbf{P}_x = \{y \in X : y \leq x\}$ están bien ordenados por el orden de X. Sorprendentemente, la existencia de árboles con cardinal superior al de $\mathbb{N}$ y cuyas cadenas y anticadenas son numerables (conjuntos que llamamos en lo sucesivo árboles de Souslin en honor al matemático ruso M. Souslin) es un problema cuya solución depende del modelo de TC con el que se trabaje. En particular, se sabe que los axiomas de ZFC (i.e., Zermelo-Fraenkel más el axioma de elección) no tienen suficiente fuerza como para probar o desmentir que existen árboles de Souslin. Por otra parte, se puede demostrar con cierta facilidad [32] que el estudio de este problema concreto es equivalente a la siguiente importante cuestión sobre la naturaleza de $\mathbb{R}$ como estructura ordenada (y que es, en verdad, el problema planteado originalmente por Souslin). Supongamos que $(L, \leq)$ verifica las siguientes condiciones:

(a) $\leq$ es un orden total en L y L no tiene ínfimo ni supremo en dicho orden.

(b) L tiene la topología del orden inducida por $\leq$ y, con dicha topología, es conexo.

Entonces se sabe que L es topológicamente homeomorfo a la recta real $\mathbb{R}$ si y sólo satisface además la siguiente condición:

(S) Existe un subconjunto de L que es denso y numerable (i.e., L es separable).

El problema de Souslin [36] consiste en averiguar si la condición (S) anterior se puede sustituir por la siguiente condición

(c) Toda familia de intervalos abiertos disjuntos dos a dos de L debe ser forzosamente numerable.

o si, por el contrario, existen conjuntos $(L, \leq)$ que verifican $(a), (b), (c)$ y no son separables. Un tal conjunto L se llamará recta de Souslin.

Podemos, por tanto, resumir el contenido de la discusión anterior en el enunciado del siguiente resultado:

Teorema 13. *Las siguientes afirmaciones son equivalentes:*

- *Existen árboles de Souslin.*
- *Existen rectas de Souslin.*

Además, ambas afirmaciones son formalmente indecidibles en el seno de ZFC.

Finalmente, se sabe [22] que si se admite el axioma de Martin (un axioma bastante complejo de enunciar pero que tiene importantes consecuencias en TC) y que $\aleph_1 < 2^{\aleph_0}$, entonces se puede probar que no existen rectas de Souslin.

5.4. **Cardinales y Ordinales.** Es lógico, a estas alturas, que algún lector "sospeche" de la "definición" de número cardinal, pues ésta hace referencia a una clase muy grande de conjuntos. Recuérdese que sólo hemos establecido bajo qué circunstancias dos conjuntos poseen el mismo cardinal, suponiendo que un cardinal es, por tanto, una clase de equivalencia sobre la clase de todos los conjuntos, y esto no parece razonable en ZF (¿Quizás sí vale para NBG?). Resumiendo: nos gustaría que los números cardinales fuesen objetos concretos de TC y, a ser posible, fuesen

conjuntos. ¿Cómo se logra esto? La solución que vamos a proponer aquí pasa por la definición de los números ordinales.

La definición de Cantor de número ordinal, como la de número cardinal, hace referencia a una relación de equivalencia en cierta clase de conjuntos muy grande[14] y, por tanto, puede dar lugar a ciertas dificultades. En 1923, J. von Neumann propuso resolver esta cuestión de la siguiente forma: En vez de identificar $\mathbf{tipo}(A, \leq)$ con una clase enorme, tomamos un representante concreto de dicha clase (ver [27]).

Definición 7 (J. von Neumann, 1923). *El conjunto vacío es un ordinal. Cada ordinal es el conjunto de los ordinales que le preceden. Un ordinal límite es uno que no tiene predecesor inmediato.*

Nota. De esta forma, obtenemos nuevamente que $0 = \emptyset$, $1 = \{\emptyset\} = 0$, $2 = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$, etc.

Sin embargo, la definición anterior no es lo suficientemente clara: ¿cómo se construyen, de verdad, todos los ordinales, incluyendo los ordinales transfinitos de todos los tamaños posibles? La idea de la definición anterior, que luego sería mucho mejor desarrollada por el propio Neumann en 1929, es utilizar el principio de inducción transfinita. Lo explicamos en palabras de J. Mosterín:

> En la teoría de conjuntos tenemos que cuantificar con frecuencia sobre todos los conjuntos, pero no tenemos una intuición suficientemente clara de qué sean los conjuntos, de cómo se formen, de en qué consista el universo conjuntista (...) Von Neumann en 1929 y, sobre todo, Zermelo en 1930 propusieron considerar que los conjuntos son el conjunto vacío y los resultados de iterar un número cualquiera (finito o infinito) de veces las operaciones "conjunto de las partes de" y " unión de". Esta concepción iterativa nos proporciona una cierta intuición de cómo es y cómo se construye el universo conjuntista. Según esta manera de verlo, el universo conjuntista estaría estratificado de un modo jerárquico y acumulativo: jerárquico porque todo conjunto tendría un rango determinado, se situaría a cierto nivel; acumulativo porque cada nivel abarcaría a todos los anteriores.

y, claro, no es difícil ahora utilizar un principio de inducción transfinita para definir funciones, etc., sobre la clase de todos los ordinales.

En 1937, R. Robinson propuso una definición más sencilla (pero equivalente a la de Neumann) de número ordinal:

Definición 8 (Robinson, 1937). *Un conjunto X se dice transitivo si $x \in X \Rightarrow x \subseteq X$. Un ordinal es un par $(\alpha, \in)$, donde α es un conjunto transitivo tal que la relación $\in$ (restringida a α) define un buen orden sobre α.*

Otros conceptos que surgen de forma natural son los siguientes:

Definición 9. *Dado un ordinal x, llamamos sucesor de x al ordinal $x^+ = x \cup \{x\}$. Decimos que el ordinal λ es un ordinal límite si no existen ordinales x verificando que $x^+ = \lambda$.*
Dados dos ordinales α y β, decimos que $\alpha < \beta$ si $\alpha \in \beta$. Decimos que $\alpha \leq \beta$ si $(\alpha < \beta) \vee (\alpha = \beta)$.
Si α es un ordinal y $x \in \alpha$, entonces el segmento determinado por x es el ordinal $\alpha_x = \{y \in \alpha : y < x\}$.

En particular, es obvio que si α es un ordinal (según Robinson) entonces se satisface la relación: $\alpha = \{\beta : \beta$ es un ordinal y $\beta < \alpha\}$ (y por tanto, α es un ordinal de los definidos por Neumann). Además, con la definición de Robinson, se puede probar también fácilmente que todo conjunto bien ordenado $(A, \leq)$ es similar a un único ordinal (por supuesto, dicho ordinal se suele llamar

[14] Dos conjuntos bien ordenados tienen el mismo tipo de orden, o el mismo ordinal, si existe una biyección entre ambos que preserva el orden

"ordinal de $(A, \leq)$" o, si se quiere, "tipo de orden de $(A, \leq)$"). Otro resultado importante para la clase de los ordinales[15] es el siguiente:

Teorema 14. *Sea X un conjunto arbitrario de números ordinales. Entonces*

- $\bigcap X$ *y* $\bigcup X$ *son ordinales.*
- $\bigcap X \leq x \leq \bigcup X$ *para todo* $x \in X$.
- $\bigcap X \in X$ *(aunque podría suceder que* $\bigcup X \notin X$*).*
- *Si* γ *es un ordinal que verifica* $x \leq \gamma$ *para todo* $x \in X$*, entonces* $\bigcup X \leq \gamma$.

En particular, $(X, \leq)$ es un conjunto bien ordenado.

Otro teorema muy importante (debido a Neumann) para la teoría de ordinales es el llamado principio de inducción transfinita. Lo enunciamos a continuación:

Teorema 15. *Supongamos que $P(x)$ es una propiedad de conjuntos y que se verifican las siguientes afirmaciones:*

- $P(0)$ *se satisface.*
- *Si se verifica* $P(\alpha)$*, entonces también se verifica* $P(\alpha^+)$.
- *Si* λ *es un ordinal límite,* $\lambda > 0$*, y* $P(\beta)$ *se satisface para todo* $\beta < \alpha$*, entonces se verifica también* $P(\alpha)$.

Entonces $P(\gamma)$ se satisface para todo ordinal γ.

El resultado anterior resulta muy útil a la hora de definir "funciones" (e.g., las operaciones aritméticas) sobre la clase Ω de los ordinales.

Ya podemos dar una definición precisa de número cardinal[16].

Definición 10. *Un número cardinal es un ordinal α con la propiedad de que si β es otro ordinal equipotente a α, entonces $\alpha \leq \beta$.*

Nota. Si se asume el axioma de elección, entonces todo conjunto se puede bien-ordenar y, por tanto, todo conjunto tiene asociado su cardinal (que es el menor de los ordinales que son equipotentes al conjunto dado). En otro caso, la definición anterior no es válida.

Terminamos esta sección demostrando, sin hacer uso de AC, que hay conjuntos bien ordenados de tamaño tan grande como se desee:

Teorema 16 (Hartogs, 1915). *Sea A un conjunto infinito cualquiera. Entonces existe un conjunto B bien ordenado que no se puede inyectar en A, aunque sí que se puede inyectar en* $2^{2^{2^A}} := \mathcal{P}(\mathcal{P}(\mathcal{P}(A)))$.

Demostración. Sea A un conjunto infinito. Consideremos entonces el conjunto

$$E = \{N \subseteq \mathcal{P}(A) : (N, \subseteq) \text{ es un conjunto bien ordenado }\}.$$

Como cada conjunto $N \in E$ es un conjunto bien ordenado (por definición de E), entonces podemos particionar E en clases de conjuntos similares:

$$N \sim M \Leftrightarrow \exists \varphi : N \to M \text{ biyección que preserva la inclusión,}$$

formando un conjunto cociente $B = E/\sim$. Este conjunto se puede interpretar de forma obvia como un conjunto de números ordinales y, por tanto, podemos bien-ordenarlo. Además, es obvio que $B \subseteq \mathcal{P}(\mathcal{P}(\mathcal{P}(A)))$. Veamos que B no se puede inyectar en A. Supongamos, por el contrario,

[15] A propósito, la clase de los ordinales la representamos con la letra Ω.

[16] Esta definición también se la debemos a Neumann

que existe $\hat{A} \subset A$ equipotente a B. Entonces el buen orden de B induce un buen orden en $\hat{A}$, que es similar al de B. Se sigue que, si Σ denota el conjunto de los segmentos de $\hat{A}$, entonces

$$\mathbf{ord}\ \Sigma = \mathbf{ord}\ \hat{A} = \mathbf{ord}\ B$$

(donde **ord** X denota el número ordinal del conjunto bien ordenado X). Ahora, como Σ es un conjunto de subconjuntos de A que está bien ordenado por la inclusión, entonces $\Sigma \in E$ y, por tanto, Σ pertenece a alguna de las clases de similaridad de B. Denotemos dicha clase por K. Se sigue que el segmento de B determinado por K es similar a Σ y, en consecuencia, B es similar a uno de sus segmentos, lo que no puede ser. El resto de la demostración es fácil. □

5.5. **Teoría de la prueba de Hilbert.** La idea de Hilbert para su "Teoría de la Prueba" era verdaderamente brillante. Se trataba esencialmente de conseguir una completa formalización de la matemática (en particular, de la TC o de la Aritmética), de manera que, al unir al cálculo lógico una correcta interpretación formal de los axiomas de una teoría matemática concreta, podríamos formalizar completamente cualquier afirmación de dicha teoría (en particular, cualquier demostración) como una ristra finita de fórmulas abstractas, cuyos símbolos, aislados y sin interpretación, carecen de significado por sí mismos. ¿Por qué es esto deseable? Algunas de las razones son las siguientes:

- Al carecer las sentencias formales que se puedan deducir en el cálculo lógico descrito anteriormente de un significado concreto, podremos olvidarnos (en nuestras deducciones formales) del contenido transfinito de la TC clásica, de manera que evitaremos la aparición de las paradojas que se conocían entonces.
- Una vez formalizado nuestro sistema, si pudiésemos demostrar dentro de éste que el sistema es consistente, obtendríamos una demostración finitaria (i.e., de aquellas que satisfacen a todas las escuelas de pensamiento matemático, incluidos los intuicionistas) de que no hay peligro en utilizar los conceptos que en principio parecían problemáticos en TC, siempre que nos ciñamos al uso del sistema axiomático para el cual se ha probado la consistencia.
- Todo lo que se demuestre en el seno de un sistema formal fijado, funciona como verdadero para cualquier interpretación que se realize de éste.

Nota. Por supuesto, hubo una amplia (y a veces agria) discusión sobre la utilidad del formalismo. Por ejemplo, Poincaré atacó con sarcasmo los éxitos de la escuela formalista.

> "Pero, si hacen falta veintisiete ecuaciones para establecer que 1 es un número, ¿cuántas no harán falta para demostrar un teorema de verdad?". La carcajada de Poincaré resuena, todavía hoy, devastadora, contra la pretensión de escribir matemática en un lenguaje simbólico y se transmite en el invencible desagrado del matemático por todo lo que tiene que ver con lenguajes simbólicos y lógica. Poincaré protestaba contra la falta de sentido y la escasa confianza que merecen los textos formales entendidos como vectores del discurso matemático[17]

Es curioso, porque Poincaré argumentaba precisamente contra las mismas ideas con las que la escuela formalista pretendía defender su postura: la precisión, la seguridad, el logro de un cálculo lógico que debía liberar a la mente de pensar directamente las cosas, y aún así, tener total seguridad de certeza....

Vamos a precisar algunos de los conceptos básicos introducidos por Hilbert:

Definición 11. *Un sistema formal S consta de los siguientes elementos:*

- *Un conjunto numerable de signos primitivos, que determina el conjunto de sus hileras o secuencias finitas de signos (con posibles repeticiones).*

[17] Ver [26].

- *Un conjunto (finito) de reglas combinatorias que determinan bajo qué condiciones podemos afirmar que una hilera de símbolos primitivos es (o no) una fórmula. El conjunto $\mathcal{L}$ de las fórmulas se denomina lenguaje formal del sistema.*
- *Un conjunto de reglas combinatorias que sirve para producir deducciones formales (i.e., determina qué secuencias de fórmulas constituyen una deducción en el sistema). Estas reglas normalmente incluyen la aceptación como verdaderas de un conjunto finito de sentencias (i.e., fórmulas sin variables libres) que reciben el nombre de axiomas del sistema.*
- *Las sentencias del sistema. Una sentencia se dice deducible si es la última fórmula que aparece en una secuencia de fórmulas que constituye una deducción. El conjunto de sentencias deducibles se llama Teoría Formalizada.*

Definición 12. *Sea un sistema formal S, cuyos axiomas están dados por A. Si φ es deducible en el sistema, decimos que φ es una consecuencia sintáctica del sistema y se denota como $A \vdash \varphi$. Si φ es una afirmación verdadera en cualquiera de las posibles interpretaciones del sistema formal, diremos que se trata de una consecuencia semántica de A y lo denotaremos como $A \models \varphi$*

Un sistema formal se dice que es consistente si en él no se pueden derivar (sintácticamente) proposiciones contradictorias. El sistema se dice coherente si las consecuencias sintácticas de éste son también consecuencias semánticas. El sistema se dice adecuado si todas las consecuencias semánticas son a su vez consecuencias sintácticas (i.e., si todas las verdades son deducibles) Finalmente, el sistema se dice completo si para cada proposición p de éste se tiene que bien p es deducible o bien $\neg p$ es deducible.

5.6. **Indecidibilidad. Teoremas de Gödel.** No vamos a demostrar los Teoremas de Incompletitud de Gödel, pero sí que vamos a establecerlos con precisión, y haremos algunos comentarios. Por otra parte, vamos a enunciar un resultado de G. Boolos, que está relacionado con los de Gödel.

Primero Descartes y luego Leibniz, estuvieron interesados en la creación de un método universal para el establecimiento de las leyes fundamentales del pensamiento. En el caso de Leibniz, dicho objetivo quebada descrito como la búsqueda de una lengua universal perfecta, un catálogo de ideas simples y de reglas para su combinación que debería servir para expresar todo pensamiento racional (i.e., una "gramática racional que refleje las conexiones lógicas entre las diferentes ideas"), liberando al hombre de la confusión omnipresente que hay en todo lenguaje natural. Siguiendo estas ideas, pero con un objetivo mucho menos ambicioso (consciente, quizás, de la imposibilidad material de la realización del sueño de Leibniz), en 1879 Frege publicaba el primer volumen de su Ideografía[18], en el que pretendía avanzar hacia los objetivos de Leibniz, pero en el ámbito mucho más restringido del pensamiento matemático y en particular, del pensamiento lógico. (Algo, por otra parte, mucho más razonable, si se tiene en cuenta que la matemática sería el modelo "ideal" de lenguaje racional, en el que toda ambigüedad sobra, etc.)

Frege produce en su ideografía el primer cálculo deductivo completo y correcto de lo que hoy se llama lógica de primer orden (Crea la moderna Lógica Matemática) y que consta de los siguientes axiomas:

- $p \Rightarrow (q \Rightarrow r)$
- $(p \Rightarrow (q \Rightarrow s)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow s))$
- $(p \Rightarrow (q \Rightarrow s)) \Rightarrow (q \Rightarrow (p \Rightarrow s))$
- $(p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)$
- $\neg\neg p \Rightarrow p$

[18]Ideografía. Un lenguaje de fórmulas similar a la aritmética.

- $p \Rightarrow \neg\neg p$
- $p = q \Rightarrow ((f(p) \Rightarrow f(q)) \;\&\; (f(q) \Rightarrow f(p)))$
- $p = p$
- $\forall x f(x) \Rightarrow f(p)$

y las siguientes reglas de inferencia:

- (Modus Ponens) De $p \Rightarrow q$ y p se deduce q.
- (Generalización) De p se deduce que $\forall x p(x)$.
- (Generalización condicional) De $p \Rightarrow q$ se deduce que $p \Rightarrow \forall x q(x)$.

El siguiente resultado garantiza que sistema formal que se acaba de describir es consistente.

Teorema 17. *El cálculo para lógica de primer orden es sintácticamente consistente.*

El sistema descrito anteriormente no es, sin embargo, sintácticamente suficiente. Esto significa que existen fórmulas bien formadas (i.e., con una gramática correcta) tales que ni ellas ni sus negaciones son tautologías y, por tanto, ni ellas ni su negación pueden ser teoremas del sistema y por tanto no pueden ser derivadas sintácticamente. Otra cosa diferente es la suficiencia semántica. En este caso, podemos preguntarnos si todas las fórmulas semánticamente válidas (i.e., aquellas que son tautologías: teoremas en cualquier interpretación natural de éstas) se pueden deducir en el cálculo lógico descrito.

Esta cuestión estuvo abierta durante mucho tiempo. De hecho, el primer resultado importante publicado por Gödel, y que fue precisamente el tema de su tesis doctoral, es el siguiente teorema

Teorema 18 (Gödel, 1930). *Cada fórmula válida de la lógica de primer orden es sintácticamente deducible.*

Por supuesto, este resultado alegró grandemente a los formalistas. Sin embargo, su alegría duró poco. En 1931 el mismo matemático (entonces un completo desconocido) que les había endulzado la boca con el resultado anterior, daría un golpe de efecto demoledor, al demostrar los siguientes teoremas:

Teorema 19 (Gödel, 1931). *Sea* **P** *el sistema formal de los Principia Mathematica, conjuntamente con la axiomática de Peano para la aritmética. Si* **P** *es consistente entonces es incompleto. Es más, esto sucede aunque completemos el sistema con un conjunto finito K de axiomas consistentes con* **P**

Nota. En realidad, Gödel supone que $\mathbf{P} \cup K$ es w-consistente, una hipótesis un poco más restrictiva que la consistencia. Sin embargo, en 1936, B. Rosser consiguió reducir esta hipótesis a la simple consistencia, con ideas similares a las de Gödel.

Teorema 20 (Gödel, 1931). *Si el sistema formal $\mathbf{P} \cup K$ es consistente, entonces es imposible demostrar su consistencia con sus propios medios.*

Finalizamos esta sección enunciando un teorema análogo al Teorema 19 anterior, que probó G. Boolos en 1986 (ver [6]). La idea es que podemos interpretar los sistemas fórmales como un tipo especial de algoritmos que generan proposiciones verdaderas (i.e., teoremas) de la aritmética.

Teorema 21. *No existe ningún algoritmo cuya salida contenga todos los enunciados verdaderos de la aritmética y ninguno falso.*

Los teoremas de incompletitud de Gödel se pueden aplicar, en particular a todas las axiomáicas conocidas de TC. El resultado es, por tanto, que no podemos aspirar a finalizar el programa formalista de Hilbert, pues no hay pruebas de consistencia internas para los sistemas formales que representan la TC. Ahora bien, como bien observan Newman y Nagel en [29], estos resultados

no dicen nada que impida la demostración de la consistencia de la aritmética mediante algún tipo de prueba que no sea formalizable dentro de la aritmética (y que, sin embargo, sea correcta). Claro que el problema para este tipo de pruebas es que hasta la fecha nadie ha tenido la idea brillante que ilumine el camino.

Por otra parte, la demostración de Gödel de la existencia de proposiciones formalmente indecidibles en el lenguaje de la aritmética se basa en la construcción efectiva de una de dichas proposiciones pero, desafortunadamente, ésta no es particularmente significativa en términos matemáticos (como podría serlo, por ejemplo, el axioma de elección o la conjetura de Goldbach). Este tipo de afirmaciones existen: se deben al trabajo de Paris y Harrington de 1977 (ver [21]).

El mismo Gödel, en vez de desanimarse, continuó activamente su trabajo sobre los fundamentos de la matemática. Incluso, podría decirse que algunas de sus contribuciones posteriores superan en dificultad a los teoremas de incompletitud. ¿Qué quedaba por hacer? Pues había que estudiar si la admisión de los postulados más conflicitivos de TC, como el axioma de elección o las hipótesis simple y generalizada del continuo, producen (o no) nuevas contradicciones en TC. Es decir, se debía estudiar la "consistencia relativa" de estos postulados respecto de las teorías axiomáticas clásicas (ZF y NBG). En 1938, Gödel proporcionó una solución positiva a este problema:

Teorema 22. *Si ZF es consistente, también lo son* $ZF \cup \{AC\}$ *y* $ZF \cup \{HGC\}$. *Lo mismo podemos afirmar para el sistema NBG.*

Finalmente, en 1963, el matemático estadounidense P. J. Cohen demostraría el siguiente resultado:

Teorema 23. *Si ZF es consistente, también lo son* $ZF \cup \{\neg AC\}$ *y* $ZF \cup \{\neg HGC\}$. *Lo mismo podemos afirmar para el sistema NBG.*

En consecuencia, AC y HGC, son proposiciones independientes del resto de postulados de ZG y NBG. (Se trata de algo similar a lo que sucede con las Geometrías Euclídea y no-Euclídeas). Todas estas demostraciones se basan en la Teoría de Modelos.

6. A MODO DE CONCLUSIÓN

Hace aproximadamente un siglo un grupo de importantes matemáticos alemanes, franceses, americanos, etc. estuvo inmerso en una discusión a fondo sobre los fundamentos de las matemáticas. Se trataba de eliminar una serie de paradojas que habían surgido en TC, pero también se discutió sobre lo que es o no aceptable en matemáticas.

Además de las paradojas lógicas, otra cuestión que produjo cierta incertidumbre en la comunidad matemática de la época es el hecho de que el axioma de elección posea consecuencias muy poco intuitivas, como el Lema de Zorn, el Axioma de Zermelo o la descomposición paradójica de Banach-Tarsky y por tanto, resultaba un poco "duro" admitir AC como axioma; pero por otra parte, si eliminamos AC de la TC entonces perderemos la oportunidad de demostrar muchos resultados importantes, como la existencia de cierres algebraicos o de bases de espacios vectoriales. Ahora bien: ¿No deberíamos tener ciertas garantías de que admitir AC no iba a producir nuevas contradicciones en el futuro? (Algo parecido sucedía con otros postulados, como la hipótesis del continuo).

Como resultado de estas discusiones surgieron varias escuelas de pensamiento que, desde entonces, se encuentran enfrentadas (formalistas, intuicionistas). Además, la demostración por parte de Gödel de ciertos resultados sobre incompletitud y consistencia de los sistemas formales que contienen la aritmética elemental, acabó con el sueño de Hilbert de establecer un consenso definitivo entre dichas escuelas.

A pesar de la naturaleza pesimista de los resultados de Gödel, hay que decir que su trabajo motivó el desarrollo posterior de teorías matemáticas muy interesantes, como son por ejemplo los diferentes conceptos de algoritmo, de computabilidad y de recursividad. Además, también debemos a Gödel algunos resultados optimistas, como son la suficiencia semántica de la lógica de primer orden y la consistencia de AC y HGC con el resto de axiomas de TC.

En los años sesenta, el matemático norteamericano P. Cohen completó los resultados de Gödel sobre AC y HGC, demostrando que ambos postulados son independientes del resto de axiomas de TC (de nuevo, tanto para ZF como para NBG), mediante el uso de técnicas propias de la teoría de modelos.

Sabemos, por Gödel, que no existen pruebas internas (finitarias) de la consistencia de ZF o NBG. Pero, ¿con esto se acaba todo?

En 1936 y 1938, G. Gentzen demostró, de dos formas distintas, la consistencia de la aritmética, utilizando inducción transfinita (i.e., por métodos no finitarios).

Desde el principio, la TC ha probado ampliamente su utilidad, al proporcionar herramientas no sólo para la homogeneización del lenguaje matemático, sino también para la demostración de resultados interesantes en otras áreas. Piénsese, por ejemplo, en la sencilla demostración por Cantor de la existencia de números trascendentes. También desde el principio TC contó con algunos detractores (e.g., Kronecker), pero con el tiempo ha quedado claro el papel central de ésta en la estructuración del conocimiento matemático. Probablemente aún hoy muchos matemáticos son de la opinión de que, por ejemplo, la teoría de los grandes cardinales no es especialmente interesante porque este tipo de conjuntos gigantescos no son frecuentes ni siquiera en las aplicaciones teóricas... pero es difícil que estos mismos matemáticos rechacen, por ejemplo, el valor estético y filosófico de esta teoría.

Actualmente hay muchos problemas de TC que están abiertos, y sobre los que quizás valdría la pena echar un vistazo.

Personalmente, me inclino a pensar que la matemática no contiene contradicciones. ¡Aunque no podamos demostrarlo usando un número finito de pasos! (¿Hay en matemáticas algo de aspecto más inofensivo que $\mathbb{N}$?)

Es probable que la preocupación por los fundamentos de la mayoría de los matemáticos modernos sea muy poca o, cuando menos, muy relativa. Sólo un grupo reducido de matemáticos (y filósofos) se ocupa actualmente de estas cuestiones. Aunque, obviamente, lo mismo podríamos decir de muchas de las diferentes "especializaciones" que existen hoy por hoy en matemáticas.

Me gustaría pensar que estas notas, escritas no por un experto sino por un "aficionado" como yo, sirvan de motivación para los lectores. Motivación para leer más sobre fundamentos. Además, debo decir que existe mucho material publicado en español sobre el tema, y una amplia gama de documentos (esta vez, la mayoría en inglés) cuyo acceso es libre en internet. La bibliografía que aparece a continuación es sólo una pequeña muestra.

Bibliografía

[1] M. Aigner, G. M. Ziegler, Proofs from The Book, Springer (2001).

[2] J. Avigad, E. H. Reck, Clarifying the nature of the infinite. the development of metamathematics and proof theory, Carnegie Mellon Technical Report CMU-PHIL-120, (2001) (Disponible en la página web http://www.andrew.cmu.edu/ avigad)

[3] D. W. Barnes, J. M. Mack, Una introducción algebraica a la lógica matemática, EUNIBAR (1978).

[4] E. Bishop, Foundations of Constructive Analysis, McGraw-hill, New-York (1967).

[5] E. Bishop, D. Bridges, Constructive Analysis, Springer-Verlag (1985).

[6] G. Boolos, Una demostración del Teorema de incompletitud de Gödel, La Gaceta de la R.S.M.E. **4** (3) (2001) 521-527. Traducción de Notices of the Amer. Math. Soc. **36** (1989) 388-390 y **36** (1989) 676.

[7] G. Cantor, Fundamentos para una teoría general de conjuntos. Escritos y correspondencia selecta, Edición a cargo de J. Ferreirós, en Clásicos de la ciencia y la tecnología, Editorial Crítica, 2006.

[8] O. De La Cruz, Three topics in Set Theory: Finiteness and Choice, Cardinality of Compact Spaces and Singular Jönson Cardinals, Ph. Thesis, University of Florida (2000).
[9] R. Dedekind, ¿Qué son y para qué sirven los números?, Alianza Ed. (1998).
[10] A. J. Durán, Historia, con personajes, de los conceptos del Cálculo, Alianza Universidad **861** Ed. Alianza (1996).
[11] H. D. Ebbinghaus et. al. Numbers, Readings in Mathematics **123**, Springer, 1995.
[12] J. Ferreirós, Labyrinth of thought: a history of set theory and its role in modern mathematics, Birkhauser Verlag (1999). (Aparece una reseña de este libro, por I. Jané, en La Gaceta de la R.S.M.E. **4** (3) (2001) 577-589).
[13] J. Ferreirós, El nacimiento de la Teoría de Conjuntos (1854-1908), Ed. de la Univ. Autónoma de Madrid (1992).
[14] A. R. Garciadiego Dantan, Bertrand Russell y los orígenes de las "paradojas" de la teoría de conjuntos, Alianza Universidad **714** Ed. Alianza (1992).
[15] L. Gillman, *Two classical surprises concernign the Axiom of Choice and the Continuum Hypothesis*, Amer. Math. Monthly **109** (2002) 544-553.
[16] K. Gödel, Obras completas, Alianza Universidad **286** Ed. Alianza (1989).
[17] K. Gödel, Sobre proposiciones formalmente indecidibles de los Principia Mathematica y sistemas afines, (con una introducción de R. B. Braithwaite), en Cuadernos Teorema **8** (1980).
[18] R. A. Gordon, *The use of tagged partitions in Elementary Real Analysis*, Amer. Math. Monthly **111** (2003) 107-114.
[19] I. Grattan-Guinness (compilador), Del cálculo a la teoría de conjuntos, 1630-1910, Alianza universidad **387** Ed. Alianza (1984).
[20] P. Halmos, Naive Set Theory, Princeton, Van Nostrand (1960).
[21] L. Harrington, J. Paris, A mathematical incompleteness in Peano arithmetic, HandBook on Mathematical Logic (J. Barwise, ed.) North-Holland (1977).
[22] T. Jech, Set Theory, (3rd edición, revisada), Springer (2003).
[23] T. Jech, The infinity, Jahrbuch 1990 der Kurt-Gödel-Gesellschaft, Wien, 1991, pp.36-44. (También disponible en la página web http://www.math.psu.edu/jech/preprints)
[24] T. Jech, On Gödel second incompleteness theorem, Procceedings of the Amer. Math. Society **121** (1994) 311-313 (También disponible en la página web http://www.math.psu.edu/jech/preprints)
[25] W. Kneale, M. Kneale, El desarrollo de la lógica, Estructura y Función **38**, Ed. Tecnos (1980).
[26] G. Lolli, La máquina y las demostraciones, Ed. Alianza (1991).
[27] J. Mosterín, Los lógicos, Espasa Forum, Ed. Espasa (1999). (Aparece una reseña por J. M. Almira en Matemáticas En Breve **2** (1) (2003) 5)
[28] J. R. Newman (compilador), Matemática, Verdad, Realidad, Ed. Grijalbo (1969).
[29] E. Nagel, J. R. Newman, El Teorema de Gödel, Ed. Tecnos (1994).
[30] M. de J. Pérez Jiménez, Teoría de clases y conjuntos, Ediciones y Distribuciones Universitarias, 1988.
[31] R. Penrose, La nueva mente del emperador, Ed. Mondadori (1991).
[32] M. E. Rudin, Souslin's conjecture, Amer. Math. Monthly, **76** (1969) 1113-1119.
[33] J. Sanmartín, Una introducción constructiva a la teoría de modelos, Ed. Tecnos (1983).
[34] M. Scheffer, The theory of the foundations of Mathematics: 1870-1940. Disponible on line en http/www.rsme.es
[35] E. Sechter, Constructivism is difficult, Amer. Math. Monthly **108** (2001) 50-54.
[36] M. Souslin, Probleme 3, Fund. Math. **1** (1920) 223.
[37] S. Wagon, The Banach-Tarsky paradox, Enciclopedia of Mathematics and its Applications **24** Cambridge University Press (1985).
[38] E. Zermelo, Investigations in the foundations of set theory I. (1908). [transl. in From Frege to Gödel, van Heijenoort, Harvard Univ. Press, 1971.]

J. M. Almira
Departamento de Matemáticas.
E.U.P. Linares, Universidad de Jaén.
23700 Linares (Jaén).
email: jmalmira@ujaen.es