LA VERDAD EN LAS MATEMATICAS

José Luis Rubio de Francia

1. INTRODUCCION

Tradicionalmente se ha tenido a la Matemática como la más exacta de las ciencias. La Biología, la Física y las demás ramas científicas afirman sus métodos, añaden a la experimentación desarrollos teóricos sofisticados (frecuentemente matematizados) que conducen a una creciente certeza y fiabilidad de los resultados que se obtienen. Incluso, como ocurre en la Mecánica Cuántica y el Principio de Incertidumbre de Heisenberg, el inevitable margen de imprecisión llega a precisarse y acotarse en términos de probabilidades. Pese a ello, subsiste a todos los niveles —hombre de la calle, científico, matemático— la idea de que hay una diferencia esencial (y no sólo un mayor grado de certeza) entre la verdad de una afirmación matemática y la de cualquier ciencia experimental.

Mientras que las teorías científicas tienen una validez relativa, por cuanto que son modificadas o literalmente contradichas con el tiempo, e incluso en un mismo instante, una teoría es aceptada o no por distintas escuelas, las verdaderas matemáticas como el teorema de Pitágoras, la infinitud de los números primos, etc., parecen trascender del tiempo, de la geografía y de cualquier tipo de credo político, religioso o científico. Incluso, si nos dejamos llevar por un platonismo instintivo, diríamos que los conceptos y las afirmaciones matemáticas son independientes del propio universo físico y de la existencia de una mente racional. La verdad matemática aparecería así como absoluta, extra-espacial y extra-temporal, imposible de negar por cualquier persona juiciosa.

Esta concepción de la matemática ha prevalecido hasta comienzos de este siglo de manera casi unánime, y es así como uno ve la matemática de niño y quizás es éste uno de los motivos por los que se afi-

ciona a ella. Mi modesto propósito en esta charla es presentar un (incompleto) mosaico de realidades más o menos aisladas que pueden entrar en conflicto con cuanto acabo de exponer sobre la naturaleza absoluta de la verdad matemática, pero en modo alguno pretendo forzar una conclusión o convenceros de algo, ya que dentro de la comunidad matemática existen visiones muy distintas sobre esta cuestión y sobre la naturaleza de la realidad matemática, de la que tan poco sabemos pese a ser nuestro material de trabajo diario.

Queda así planteada la pregunta:

¿ES ABSOLUTA LA VERDAD MATEMATICA?

Para aproximarnos a una respuesta, pensemos en cómo se llega a un teorema matemático. Se parte de unos postulados básicos, y por un proceso deductivo que utiliza las normas de la Lógica, se llega a establecer la conclusión. Las críticas a la verdad matemática pueden apuntar por tanto en dos direcciones: el principio adoptado o el camino seguido, es decir, los *axiomas* que fundamentan la matemática o la *demostración*. Presentaré algunos elementos del mosaico en cada una de ambas direcciones.

2. SOBRE LA FUNDAMENTACION

El encadenamiento lógico que garantiza la veracidad de las afirmaciones matemáticas se sostiene sobre un grupo de axiomas cuya veracidad no se cuestiona ni se pretende demostrar. Desde la aparición de las Geometrías no euclídeas con Lobatchevsky, Bolyai, Gauss y Riemann, ha resultado obvio que distintas verdades matemáticas pueden obtenerse si se parte de postulados diferentes, y todas ellas son igualmente válidas y susceptibles de adecuarse eventualmente a la realidad material. A la fundamentación de la Geometría se añadió a comienzos de siglo el proyecto más ambicioso de fundamentar toda la Matemática sobre la noción de conjunto, lo que requiere:

i) Establecer un sistema preciso de axiomas que regule a qué cosa se le puede llamar conjunto (evitando las célebres paradojas de B. Russell y otros) y a qué manipulaciones podemos someter a nuestros conjuntos para obtener nuevos conjuntos.

ii) Urdir un complejo entramado (artificioso desde el punto de vista de la intuición, eficaz desde el punto de vista lógico) que permita expresar en términos de conjuntos todos los conceptos matemáticos.

a) La axiomática Z - F

Quizás no es de todo el mundo conocido lo que una axiomática conjuntista debe contener para cumplir el objetivo i) señalado anteriormente, por lo que me atrevo a citar la axiomática de Zermelo y Fraen-

kel con una explicación vulgarizada (espero que no demasiado) del contenido de sus axiomas (ver cuadro 1). Estos axiomas responden a nuestra intuición sobre lo que es un conjunto, y puede decirse que son universalmente aceptados por los matemáticos, pero he excluido deliberadamente un último postulado —el *axioma de elección*— mucho más controvertido y que aparece de hecho en el sistema de axiomas propuesto por Zermelo y Fraenkel o en las axiomáticas posteriores (y equivalentes) como la de Bernays, Gödel y Von Neumann. De él me ocuparé pronto.

Veamos antes cómo se cumple el objetivo ii) una vez que tenemos la axiomática. Los números naturales se pueden definir:

$$0 = \phi; \quad 1 = \{\phi\}; \quad \ldots; \quad n + 1 = \{n, \phi\}; \quad \ldots$$

El par ordenado es: $(x, y) = \{x, \{x, y\}\}$, y a partir de aquí los números enteros y racionales se construyen como conjuntos de pares ordenados, cada número real es una «semirrecta racional» (método de Dedekind), cada función es un conjunto de un cierto producto cartesiano, etc. Todas estas construcciones son bien conocidas por cualquier matemático (desgraciadamente, se pretende que lo sean por cualquier niño impúber), por lo que no insistiré en ello.

CUADRO 1: *Aximática Z - F*

A 1. — AXIOMA DE EXTENSION:
$x = y \Leftrightarrow$ tienen los mismos elementos.

A 2. — AXIOMA DEL VACIO:
Existe un conjunto, ϕ, sin elementos.

A 3. — AXIOMA DE PARES NO ORDENADOS:
Si x, y son conjuntos, también lo es $\{x, y\}$.

A 4. — AXIOMA DE LA UNION:
Si x es un conjunto, su unión es un conjunto.

A 5. — AXIOMA DEL INFINITO:
Existe x tal que: $\phi \in x$ y además $z \in x \Rightarrow \{z\} \in x$.

A 6. — AXIOMA DEL CONJUNTO POTENCIA:
Si x es un conjunto, todos sus subconjuntos forman otro conjunto $P(x)$.

A 7. — AXIOMA DE SUSTITUCION:
Regula qué «propiedades» sirven para definir conjuntos.

A 8. — AXIOMA DE REGULARIDAD:
Prohíbe cosas como $x \in x$, etc.

b) Axioma de elección

Una primera y comprometida opción que un matemático debe de tomar, y que determinará qué verdades matemáticas va a poder demostrar, es la aceptación o no del axioma de elección, que puede formularse así:

(AC): «*Si* $\{A_i\}_{i \in I}$ *son conjuntos no vacíos, puede formarse un conjunto* $C = \{(i, x_i)\}_{i \in I}$ *tal que* $x_i \in A_i$ *para todo* $i \in I$.»

La idea de que puede elegirse un elemento de cada conjunto y formar así un nuevo conjunto es tan natural e intuitiva que uno difícilmente cuestiona la validez de este axioma la primera vez que se enfrenta a él. La diferencia con los restantes axiomas es que, en los conjuntos formados de acuerdo con (A 1) - (A 7) uno sabe perfectamente qué elementos pertenecen al conjunto, mientras que en (AC) no existe una regla que defina C y nos encontramos con que, si nos dan un elemento $x \in \cup A_i$ fijo, no podemos decir si pertenece o no a C. Una parodia, debida a B. Russell, que ilustra acertadamente el contenido de este axioma es la siguiente:

«Un lord inglés infinitamente rico tenía infinitos trajes, zapatos, sombreros, etc. Como era tremendamente caprichoso, un día ordenó a su mayordomo:

— Walter, quiero que pongas una fila de zapatos en el pasillo, de forma que haya un zapato de cada uno de mis pares.

Naturalmente, el pasillo era infinitamente largo. Walter quedó pensativo, y en seguida ordenó a los infinitos criados que tomaran de cada par de zapatos el correspondiente al pie izquierdo, y que los pusieran en fila en el pasillo. Así cumplió Walter la orden, pero al día siguiente, el lord se lo puso más difícil:

— Walter, quiero que pongas en el pasillo un calcetín de cada uno de mis pares de calcetines.

Después de reflexionar, Walter respondió cabizbajo:

— My lord, para hacer eso necesito el axioma de elección.»

El axioma de elección tiene consecuencias importantes que no pueden derivarse de los axiomas (Z - F), algunas de las cuales son útiles —lo que hace «conveniente» aceptar (AC)—, mientras que otras resultan sorprendentes y anti-intuitivas —lo que abona el terreno de los cons-

tructivistas, que aceptan únicamente (Z - F) sin (AC)—. He aquí un pequeño muestrario de tales consecuencias:

1. — Todo conjunto admite un buen orden (esto resulta mucho más duro de creer que (AC), pese a ser equivalente a él).

2. — Paradoja de Banach-Tarski: Dos esferas A —muy grande— y B —muy pequeña— pueden dividirse en N partes disjuntas

$$A = A_1 \cup A_2 \cup \ldots \cup A_N \quad ; \quad B = B_1 \cup B_2 \cup \ldots \cup B_N$$

de modo que A_1 es congruente con B_1 (i.e., hay un movimiento que transforma A_1 en B_1), A_2 es congruente con B_2, etc.

3. — Puede definirse $1(A)$ = longitud de A para todo $A \subset \mathbf{R}$, de forma que 1 sea finitamente aditiva y $1([a, b]) = b - a$. Lo análogo en $\mathbf{R}^3$ es falso, pues en la paradoja de Banach-Tarski, si pudiéramos definir el volumen de A_i, B_i para todo $i = 1, 2, \ldots, N$, deduciríamos que volumen (A) = volumen (B), lo que es absurdo.

4. — Existen subconjuntos de $\mathbf{R}$ no medibles en el sentido de Lebesgue. El primero de tales ejemplos (siempre no constructivos) fue dado por Vitali.

5. — Por último, teoremas muy utilizados como el de Tychonoff en Topología, el de Hahn-Banach y sus variantes en Análisis Funcional, etc., así como la fundamentación del Análisis No-Standard, requieren (AC).

He de aclarar que algunos de los enunciados de esta muestra son de hecho equivalentes al axioma de elección, mientras que otros son estrictamente más débiles, pero todos son esencialmente no constructivos, es decir, no derivables de (Z - F).

¿Debe o no aceptarse el axioma de elección, y con él todas sus consecuencias? Como ya he indicado, la opción es personal, pero es justo señalar que la inmensa mayoría de la comunidad matemática lo acepta y utiliza en la actualidad, no sé si por íntimo convencimiento o porque su negación arrastraría a la ruina una importante parte del edificio matemático que nos resistimos a perder. En todo caso, es éste un axioma que no se mantiene en pie de igualdad con los postulados de (Z - F): Primeramente, porque sigue enfrentado a una pequeña pero activa minoría constructivista (incluyendo a los seguidores de Brower, intuicionistas, cuya actividad es aún más radical), y en segundo lugar, porque subsiste entre los «usuarios» de (AC) un cierto complejo de culpabilidad que les hace limitar su aplicación todo lo posible. Así, no es extraño que un teorema interesante cuya demostración original utilizaba (AC) vuelva a ser probado por métodos estrictamente constructivos (por lo general mucho más complejos), y ello es siempre aplaudido por la comunidad matemática, que celebra que tal teorema pase definitivamente al terreno de lo constructivo e incuestionado.

c) Lo indecidible

¿Puede ocurrir que la axiomática (Z - F) sea contradictoria? No conozco a ningún matemático profesional que crea seriamente en tal posibilidad. Este es un argumento sociológico para defender la consistencia interna de (Z - F), pero debo admitir que no es muy sólido, pues nadie acostumbra a creer que el edificio en el que vive vaya a derrumbarse, pese a que tales derrumbamientos ocurren de hecho. Si he expuesto un argumento tan endeble, es porque no puedo ofrecer otro: Se desprende del teorema de Gödel (1931), que nunca podremos garantizar la consistencia *interna* de (Z - F) ni de cualquier otro sistema que contenga al menos la axiomática del número natural. He aquí la espada de Damocles que pende sobre nosotros. Alguien, algún día, podría despertarnos diciendo que de (Z - F) se deduce que una cierta proposición (p) es cierta y que su negación ($-p$) es cierta también, y que en consecuencia, (Z - F) es absurda y toda la matemática construida sobre ella no es menos absurda. El matemático debe acostumbrarse a vivir (y a dormir) con esta realidad, y ante tal estado de cosas, el argumento sociológico se torna fuerte y coherente, y uno se abraza a él como a su osito de peluche.

En el mismo trabajo de 1931, Gödel nos obsequió con otro concepto preocupante, el de *proposición indecidible*. Supongamos que creemos firmemente en (Z - F) con (AC) y en la consistencia de este sistema axiomático, y nos planteamos la validez o no de una proposición determinada que pueda formularse en este sistema axiomático, como, por ejemplo, la *hipótesis del continuo* de Cantor:

> (CH): «*Todo subconjunto infinito de* **R** *es numerable (tiene el cardinal de* **N***) o tiene la potencia del continuo (el cardinal de* **R***).*»

Con la concepción tradicional (platónica) de la matemática, diríamos que (CH) es verdadera o falsa, aunque la demostración de una u otra cosa haya escapado a nuestros intentos. Así lo creyeron Cantor, al enunciar su conjetura, y Hilbert, al proponerla como uno de los problemas de su célebre lista en 1900. Pero Gödel observó que procedía contemplar otra posibilidad (que más tarde resultó ser la adecuada al caso concreto de (CH) (ver cuadro 2) al probar que «*En todo sistema axiomático* $\mathcal{A}$ *que contenga la axiomática del número natural, pueden formularse infinitas proposiciones* (p) *que son indecidibles, es decir, tales que, si* $\mathcal{A}$ *es consistente, lo sigue siendo después de añadirle* (p) *así como después de añadirle* ($-p$) *=negación de* (p)». Si (p) es indecidible, nunca podremos probar a partir de la axiomática que (p) es falso

—porque sería contradictorio con la axiomática consistente «$\mathcal{A} \in (p)$»— ni tampoco que (p) es verdadero —pues también «$\mathcal{A} \in (-p)$» es consistente—. El hecho de que en un esquema tan simple como el del número natural **N** con los axiomas de Peano quepa una infinitud de proposiciones indecidibles, abre la posibilidad de que algunas de las conjeturas clásicas de la teoría de números, que han sido refractarias a los esfuerzos de generaciones de matemáticos, resulte indecidible.

Algunos ejemplos concretos de proposiciones indecidibles notables dentro de la axiomática (Z - F) se recogen en el cuadro 2. En cada uno de tales ejemplos, el teorema que afirma la indecidibilidad de (p) consta de dos partes:

i) Si (Z - F) es consistente, también lo es (Z - F) $\in (p)$.

ii) Si (Z - F) es consistente, también lo es (Z - F) $\in (-p)$. El hecho de que, asumiendo sólo (Z - F), que es la parte no controvertida de la axiomática conjuntista, el axioma de elección resulte indecidible, deja

CUADRO 2: *Algunos indecidibles*

INDECIDIBLES EN (Z - F)	
Ej. 1:	(AC) es indecidible.
	(Z - F) $\in$ (AC) es consistente (Gödel, 1938).
	(Z - F) $\in$ (— AC) es consistente (Cohen, 1963).
Ej. 2:	(CH) es indecidible.
	(Z - F) $\in$ (CH) es consistente (Gödel, 1938).
	(Z - F) $\in$ (— CH) es consistente (Cohen, 1963).
Ej. 3:	(S): «*Todo* $A \subset \mathbf{R}$ *es medible Lebesgue.*»
	(Z - F) $\in$ (S) es consistente (Soloway, 1965).
	(Z - F) $\in$ (— S) es consistente.

en posición de equilibrio (desde el punto de vista lógico) a quienes argumentan a favor o en contra de (AC), por lo que, como ya advertí antes, cada matemático puede optar libremente. En lugar de negar (AC), pueden adoptarse axiomas concretos que estén en contradicción con él, como el axioma (S) propuesto por Soloway, que impone que todo subconjunto de **R** sea medible en el sentido de Lebesgue. (El ejemplo de Vitali prueba que (AC) $\in$ (S) es absurdo). Una vez más, es una decisión personal si (S) responde a la intuición o a alguna realidad material, pero es lógicamente lícito partir de (Z - F) $\in$ (S) para construir

una matemática que encuentra resultados tan chocantes para un analista funcional convencional como qué espacios de dimensión infinita puedan tener todas sus formas lineales continuas. Naturalmente, no es (S) el único axioma contradictorio con (AC) que puede fijarse, y como ocurrió con el postulado de las paralelas de Euclides, nos encontramos ante un punto de ramificación del que surgen universos matemáticos incompatibles unos con otros y cuya posibilidad de adecuación al universo físico sólo su exploración podrá confirmar o descartar.

Espero que cuanto llevo dicho haya abierto el camino a la preocupación fructífera, que no al desánimo. Si los fundamentos no son inamovibles, habrá que convenir que la matemática pretende únicamente dar *demostraciones absolutas* de *verdades relativas*. La validez y seguridad de las conclusiones no podrá superar a la de los principios, y es en la demostración inapelable donde debemos recurrir para sostener el carácter de una verdad matemática esencialmente distinta de la certeza experimental.

3. SOBRE LA DEMOSTRACION

En rigor, un teorema debería considerarse demostrado y aceptado como tal si su enunciado se obtiene a partir de los axiomas mediante una manipulación lógicamente correcta de los símbolos. Esta exigencia convierte de hecho la matemática en algo casi ilegible, como la experiencia de B. Russell y A. N. Whitehead con su libro «Principia Mathematica» (Cambridge Univ. Press, 1910) muestra de forma elocuente. En la práctica, se hace necesario aceptar como demostración todo aquello que *claramente podría* escribirse en esa forma si se tomase suficiente tiempo y paciencia.

El determinar si una demostración podría o no escribirse en tales términos introduce un elemento de subjetividad en la aceptación de tal demostración como válida.

Esto nos lleva a considerar que todo teorema aceptado como cierto lo será excepto por una pequeña probabilidad: La de que cuantos revisaron la demostración hayan pasado por alto un error de razonamiento. Tal posibilidad de error parece difícil de contemplar cuando uno piensa en enunciados sencillos, como la irracionalidad de $\sqrt{2}$, cuya demostración hemos asimilado globalmente de manera tan profunda que diríamos que está impresa en nuestro espíritu individual. Pero las Matemáticas del último cuarto de siglo contienen demostraciones de enorme longitud y complejidad, con saltos nada triviales en el razonamiento y con afirmaciones o definiciones imprecisas que sólo dentro de un argot especializado cobran un significado ajustado. En Topología de baja dimensión y en Análisis de Fourier podrían citarse ejemplos recientes de esta circunstancia. Sin tener que acudir a los teoremas

más difíciles, la cantidad de resultados publicados anualmente (ver cuadro 3) y la especialización excesiva de las áreas de investigación, conducen a la situación que acertadamente describen P. J. Davis y R. Hersh en su libro «The Mathematical Experience» (Birkhauser, 1981):

«Los matemáticos de cualquier área se basan en el trabajo de otros, se citan unos a otros; la confianza mutua que les permite hacer esto, está basada en la confianza en el sistema social del que forman parte. No se limitan a utilizar resultados que ellos mismos pueden probar a partir de los principios de partida. Si un teorema ha sido publicado en una revista respetable, si el nombre del autor es familiar, si el teorema ha sido citado y utilizado por otros matemáticos, se considera establecido. Cualquiera que tenga necesidad de utilizarlo será libre de hacerlo. Esta confianza mutua es perfectamente razonable y apropiada. Pero desde luego, viola la noción de verdad matemática como algo indudable.»

El creciente volumen de «matemática nueva» producida queda medido groseramente en el cuadro 3 por el grosor de los correspondientes volúmenes de «Mathematical Reviews», revista que dedica una breve recensión descriptiva y/o crítica a cada uno de los artículos de investigación aparecidos en la práctica totalidad de las publicaciones matemáticas periódicas. Incidentalmente, uno puede encontrar, aunque es poco frecuente, recensiones del tipo siguiente: «En este trabajo, el autor pretende probar que..., lo que es manifiestamente falso, ya que...»

Como complemento a esta exposición de carácter general, revisaremos ahora algunas demostraciones especialmente conflictivas de teoremas relevantes obtenidos durante los últimos años:

CUADRO 3: *Medida de volumen de publicaciones*

MATHEMATICAL REVIEWS

Período	*Grosor M. R.*
1940-44	19 cm.
1945-49	24,5 cm.
1950-54	36 cm.
1955-59	48,5 cm.
1960-64	81 cm.
1965-69	108 cm.
1970-74	122 cm.
1975-79	184 cm.

a) Teorema de los cuatro colores

Se desea colorear un mapa político en el plano, de forma que cualesquiera dos países con una línea (no reducida a un punto) de frontera común tengan distinto color. ¿Cuál es el mínimo número de colores necesario? En las figura F1 y F3, basta con tres colores, mientras que F2 y F4 requieren cuatro. La experiencia acumulada por pruebas en mapas mucho más complicados parecía confirmar que cuatro colores bastaban en cualquier caso, y en 1878, A. Cayley propuso como problema el demostrar rigurosamente que tal conjetura era cierta. Un año después, se publicaba en la London Mathematical Society una solución afirmativa a tal conjetura debida a A. B. Kempe, lo que dio el problema por resuelto durante once años, hasta que en 1890 se descubrió un error en el argumento que volvió a dejar abierto el problema casi un siglo. Antes de proseguir, examinemos el esquema de la «demostración» de Kempe:

i) *Todo mapa puede colorearse con no más de cinco colores.* Esta primera aproximación al problema fue observada pronto, y su demostración es reminiscente del teorema de Euler sobre las caras, aristas y vértices de un poliedro. Si un mapa necesita justamente cinco colores, se llama *5-cromático.* La conjetura consiste en probar que no existen mapas 5-cromáticos.

ii) *Todo mapa «normal»* (este adjetivo excluye los mapas con cuatro o más países en un vértice o con un país rodeado por otro) *contiene un país con menos de seis vecinos.* En la terminología creada al efecto, esto significa que {F1, F2, F3, F4} es un *conjunto inevitable* de configuraciones, es decir, una de tales configuraciones aparece necesariamente en cualquier mapa normal.

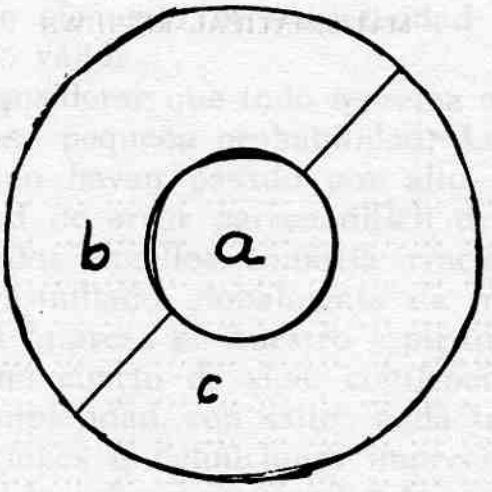

Figura 1

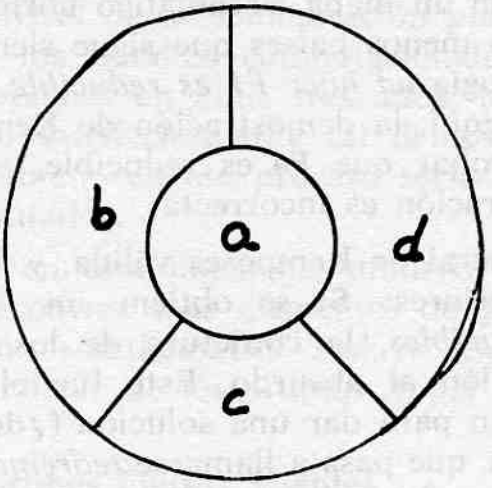

Figura 2

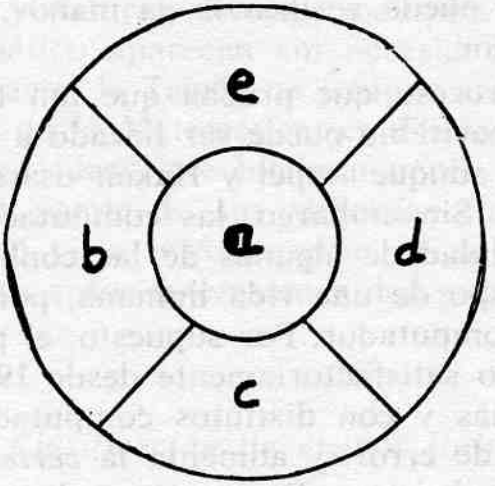

Figura 3

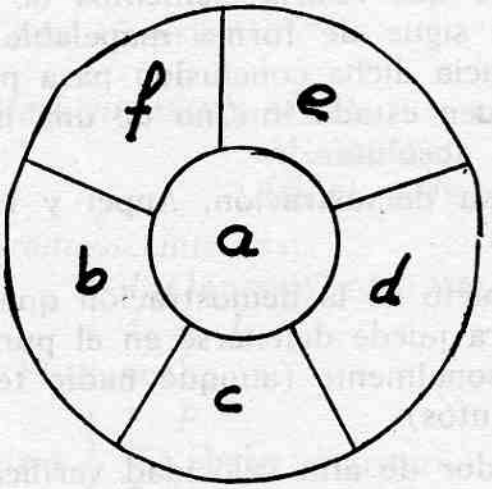

Figura 4

iii) Si F1 está en un mapa 5-cromático normal, dicho mapa puede reducirse a otro con menos países que sigue siendo normal y 5-cromático. En la terminología *ad hoc*: *F1 es reducible.* También F2 y F3 son reducibles, y hasta aquí, la demostración de Kempe es correcta. Finalmente, pretendió probar que F4 es reducible, pero es en este punto en el que la demostración es incorrecta.

La estrategia general de Kempe es válida, y ha sido mantenida por investigadores posteriores: Si se obtiene un *conjunto inevitable* de *configuraciones reducibles,* la conjetura de los cuatro colores queda probada por reducción al absurdo. Este fue el método seguido por K. Appel y W. Haken para dar una solución (¿definitiva?) al problema de los cuatro colores, que pasa a llamarse *teorema de los cuatro colores,* pero las diferencias con la «prueba» de Kempe son algo más que anecdóticas: Appel y Haken construyeron un conjunto inevitable de más de mil configuraciones reducibles, alguna de las cuales es tan complicada que su reducibilidad no puede verificarse «a mano», sino que requiere el uso de un computador.

El complicado proceso que prueba que tan tremendo conjunto de configuraciones es inevitable puede ser llevado a cabo por una persona en unos dos meses, aunque Appel y Haken usaron también el computador en esta parte. Sin embargo, las computaciones requeridas para verificar la reducibilidad de algunas de las configuraciones no pueden realizarse en el tiempo de una vida humana, por lo que es imprescindible la ayuda del computador. Por supuesto, el programa de computador ha sido realizado satisfactoriamente desde 1976 por varios equipos diferentes de personas y con distintos computadores, lo que casi elimina la posibilidad de error, y aumenta la *certeza* del resultado, pero la pregunta básica subsiste: ¿Es esto una demostración matemática?

Para algunos filósofos y lógico-matemáticos, el aceptar el teorema de Appel y Haken supondría cambiar (debilitándolo) el concepto de demostración, puesto que habría elementos de duda razonable sobre si la conclusión se sigue de forma inapelable de las hipótesis. En efecto, el camino hacia dicha conclusión pasa por circuitos eléctricos, y se apoya en el buen estado interno de una máquina, sobre el cual nunca hay garantías absolutas.

En defensa de su demostración, Appel y Haken emplean los siguientes argumentos:

i) El plan completo de la demostración queda expuesto ante todo el mundo. Cualquiera puede detenerse en el punto concreto que desee y comprobarlo personalmente (aunque nadie tendrá tiempo de comprobar *todos* los puntos).

ii) Un computador de alta velocidad verifica más detalles en una hora que un hombre en toda su vida, pero ello no cambia el concepto de demostración matemática, sino sólo su práctica.

iii) Si el plan general de la demostración pudiera simplificarse un tanto, haciendo que los detalles computacionales fueran verificables por un equipo de personas en unos tres años, los objetores filósofos y lógicos se sentirían satisfechos ante tal demostración, pero la probabilidad de error humano en ese proceso sería mucho mayor que la de error por el computador.

Lejos de abundar en esta polémica, prefiero dejar el veredicto al oyente, que podrá encontrar más elementos de juicio en la obra editada por L. A. Steen: «Mathematics Today» (Springer-Verlag, 1978), la cual contiene un artículo de los propios Appel y Haken.

b) Clasificación de Grupos Finitos Simples

El concepto de grupo, familiar para todos vosotros, es uno de los pocos conceptos abstractos cuya motivación no plantea problemas: Su definición es sencilla y natural, diversos ejemplos de grupos conocidos por cualquier matemático aparecen sin necesidad de forzar la imaginación, y, por otra parte, la Teoría de Grupos encuentra aplicación en casi todas las ramas de la Matemática, en Física Teórica, en Cristalografía, etc. Una de las ideas que hicieron nacer esta teoría fue la de estudiar un objeto a partir de sus simetrías (las cuales forman un grupo). Este punto de vista está presente ya en la Teoría de Galois, y al igual que en otros casos interesantes, los grupos que aparecen allí son finitos.

CUADRO 4: *Clasificación de grupos finitos simples*

SERIES
- *Grupos alternados: An* ($n \geq 5$).
- *Grupos tipo Lie:* 16 series.

ESPORÁDICOS (26)
- *Grupos de Mathieu* (1860): M_{12} M_{12} M_{22} M_{23} M_{24} (p. ej., $|M_{24}| = 244.823.040$).
- *Grupos esporádicos «nuevos»*:
  - Janko: J_1 (Janko-Ward, 1966; $|J_1| = 175.560$); J_2, J_3, J_4
  - ... (otros 13 grupos)
  - Fisher-Griess: F_5, F_3; F_2: «baby monster»; F_1: «monster» $|F_1| \simeq 10^{55}$

Cuando un grupo finito G tiene un subgrupo normal H, el estudio de G puede reducirse al de dos grupos menores, y previsiblemente más sencillos, que son H y el grupo cociente G/H. De ahí que los grupos finitos llamados que para $n = 5, 6, 7, \ldots$ son grupos simples. Los grupos de tipo Lie se llaman así porque corresponden a algunos grupos de Lie clásicos cuando se sustituye el cuerpo **R** o **C** por un cuerpo finito. Pero uno de los aspectos más excitantes del problema de la clasificación ha sido la aparición sucesiva de hasta 26 *grupos esporádicos*, que no entran en ninguna serie de grupos finitos simples. Los cinco primeros de tales grupos fueron descubiertos ya en el siglo pasado por Mathieu, y hubieron de pasar más de cien años antes de que Janko descubriera el siguiente grupo esporádico, J_1, que había pasado sorprendentemente desapercibido pese a su tamaño relativamente pequeño (175.560 elementos, unas 1.400 veces más pequeño que el mayor de los grupos de Mathieu). A partir de allí, y a un ritmo de dos nuevos grupos por año, la lista de esporádicos fue aumentando, haciendo temer que pudiera haber una infinidad de tales grupos, lo que habría hecho inalcanzable la clasificación completa. Afortunadamente, la lista se cierra con el espectacular grupo F_1, conocido como *monstruo* («monster») de Fisher-Griess, que tiene, aproximadamente, 10^{55} elementos.

Otro aspecto curioso de los grupos esporádicos es la manera como son hallados, que recuerda el descubrimiento de partículas elementales en Física Atómica. Contemplando y desechando posibilidades de cara a la clasificación de grupos simples, uno llega a enunciar cosas como ésta: «Si un grupo tiene una involución con centralizador de *tal* o *cual forma*, y además contiene subconjuntos con *tales* propiedades, entonces es un grupo con *tantos* elementos, sus caracteres verifican *esto* y *lo otro*, etc.». A partir de aquí, las sofisticadas técnicas (teoría de caracteres, análisis local, ...) de Teoría de Grupos permiten deducir propiedades internas que tal grupo, si existiera, debería cumplir, y si todo ello no da lugar a ninguna contradicción, se da casi por hecho que el grupo existe y se le bautiza: J_1 (primer grupo de Janko), F_2 («baby monster» o «monstruito» de Fisher), etc. Queda por probar, efectivamente, que tal grupo existe y es único, lo cual ha sido posible en todos los grupos esporádicos no mucho después de su «descubrimiento». El último de ellos, F_1, fue construido por Griess en 1980 como un grupo de matrices complejas de unas 200.000 filas y columnas, y su unicidad fue probada por Northon y Thompson en febrero de 1981, dándose por concluida «oficialmente» la clasificación de grupos finitos simples. Digamos para terminar esta descripción somera, que el mayor conocimiento de F_1 permite apuntar la posibilidad de una aproximación más sensata a la clasificación, puesto que él sólo contiene de una u otra forma a la mayoría de los grupos esporádicos. Ello junto a la aparente conexión que el «monstruo» podría tener con ramas tan lejanas como la teoría de funciones elípticas, ha constribuido a rehabilitar la imagen

de F_1, para quien se sugiere ahora el nombre de «nuestro amigo el gigante».

Volviendo a nuestra preocupación inicial, la dificultad en aceptar como demostrado el teorema sobre la clasificación de grupos finitos simples —dicho teorema afirma que todo grupo finito simple es isomorfo a alguno de los de la (incompleta) tabla del cuadro 4— radica en que la demostración completa ocupa unos 500 artículos con casi 10.000 páginas en total. El reciente libro de D. Gorenstein: «Finite Simple Groups. An Introduction to their Classification» (Plenum Press, 1982) al que seguirán dos más prometidos por el autor, no pretende demostrar el teorema, sino dar una introducción al mismo y mostrar esquemáticamente los métodos y dificultades que aparecen. En el comentario a este libro hecho por W. Feit en el Bulletín de la A.M.S. (enero 1983) se leen las siguientes frases:

«Los grupos finitos simples han sido *aparentemente* clasificados... Ninguna persona ha recorrido toda la demostración y comprobado todos los detalles. Esta no es una situación totalmente satisfactoria. Sin embargo, la mayoría de los expertos están convencidos de que la demostración es *esencialmente* correcta..., no se espera que ningún error cambie el resultado final, es decir, conduzca a nuevos grupos simples.»

«Excepto al nivel de fundamentos, las matemáticas no son materia de fe, por lo que no es sorprendente que el anuncio de la clasificación haya sido tratado con escepticismo entre los matemáticos. Sin embargo, no tendría objeto (y sería probablemente imposible) que cualquiera intentase ahora recorrer la demostración completa, porque tal demostración se revisa, simplifica y acorta continuamente. A este proceso se le ha calificado como *revisionismo*. No es irrazonable esperar que, en algo así como una década, quizás pueda escribirse un libro de longitud normal que contenga una demostración completa de la clasificación...»

Palabras de cautela sobre el uso del término «demostración» en este contexto aparecen también en la Introducción del libro citado de Gorenstein, y él mismo dice: «¿Cómo puede uno garantizar que la "criba" no ha dejado pasar una configuración que conduzca a otro grupo finito simple? Desgraciadamente, no hay garantías, uno debe de vivir con esta realidad.»

De nuevo, el matemático se enfrenta aquí con un teorema cuya demostración rompe drásticamente los moldes que para tal concepto tenía nuestra mente, y uno debe decidir si ampliar esos moldes para dar cabida a tales «macroteoremas» o mantener una postura de estricto rigor que limitaría las demostraciones válidas a aquéllas que una persona suficientemente entrenada puede entender globalmente por sí sola.

c) Criterios de primalidad

Como contrapunto a los dos ejemplos anteriores, quiero presentar ahora un caso que probablemente parecerá más frívolo e intrascendente. El problema consiste en determinar si un número n es primo, y para ello, el método de ensayar su divisibilidad por todos los números menores que $\sqrt{n}$ resulta impracticable cuando n es bastante grande. *Los criterios de primalidad* resultan, por lo general, más efectivos, aunque suelen dar únicamente condiciones necesarias. Así, el primero de tales criterios, debido a Fermat, establece: «*Si* n *es primo, y* a *es cualquier número natural, entonces* a^n *es congruente con* a, *módulo* n», es decir

$$(F)\ n \text{ primo} \Rightarrow a^n \equiv a \pmod{n}$$

Fijada una base a, el criterio (F) es fácil de verificar incluso para n grande. Si el criterio falla, sabemos que n es compuesto, pero desgraciadamente, si el criterio da resultado positivo, no podemos asegurar que n sea primo. Podemos probar con otra base b, y si ocurre que $a^n \equiv a \pmod{n}$ y que $b^n \equiv b \pmod{n}$, lo más *probable* es que n sea primo, pero ¿cómo mejorar la prueba para conseguir garantías absolutas de que n es primo? Existen números recalcitrantes —llamados de Carmichael— para los que el criterio (F) da resultado positivo cualquiera que sea la base elegida, y pese a ello, son compuestos.

En este punto, argumentos probabilísticos pueden ayudarnos a aumentar nuestra certeza sobre el carácter primo de n. Supongamos que n es muy grande, tomemos al azar sesenta números $a_1, a_2, \ldots, a_{60}$ menores que n, y ensayemos con cada uno de ellos el criterio (F). Si en todos los casos obtenemos resultado positivo, i.e.

$$a_j^n \equiv a_j \pmod{n}, \quad 1 \leq j \leq 60$$

entonces, la probabilidad de que n sea compuesto es menor que 10^{-18}. Podríamos asegurar que n es primo y la probabilidad de error al hacer esta afirmación sería de una entre un trillón. Desde luego, en estas circunstancias, yo apostaría todo mi dinero a que n es primo, pero ¿lo habríamos demostrado?

Me imagino que una mayoría es reticente a aceptar esto como demostración, porque si este proceso se aplicase sistemáticamente y calificáramos como primos a cuantos números verificasen satisfactoriamente la prueba de las sesenta bases, estaríamos dando como demostradas una infinidad de afirmaciones falsas (si bien, ciertamente, una infinidad muy minoritaria). Sin intentar extrapolar el proceso, pense-

mos, sin embargo, por un momento, en un solo número n que, por algún motivo, es importante saber si es primo o compuesto. Le aplico el criterio de las 60 bases aleatorias y da resultado positivo. ¿Puedo considerar demostrado que n es primo y utilizar esto en razonamientos ulteriores? Sigo intuyendo vuestra negativa, pero pensad que si yo afirmo que n es primo, la probabilidad de equivocarme es 10^{-18}, y os puedo asegurar que la probabilidad de error en el teorema de los cuatro colores o en la clasificación de grupos finitos simples es considerablemente superior.

Para quien acepte la demostración de los dos teoremas mencionados pero no el criterio probabilista de determinación de números primos, sugiero que la aparente contradicción que esta doble actitud comporta debiera superarse a la luz de una distinción nítida entre los términos *demostración* y *certeza*.

4. EPILOGO

Como ya advertí al comienzo de estas palabras, no está en mi ánimo el extraer conclusiones, pero quiero dejar patente que para mí, la verdad sigue siendo un atributo esencial de la Matemática y la piedra angular que la soporta y, junto a los móviles de la estética y la utilidad, le da sentido. La cuestión sobre la que he querido haceros reflexionar es: ¿qué tipo de verdad? Porque la VERDAD con mayúsculas no es sino una abstracción inalcanzable —quimérica, como decía hace medio siglo J. Barinaga en una conferencia con el mismo título que ésta—, y la Matemática es, acaso, «el templo más colosal que el espíritu humano ha erigido» a esta quimera.