MISCELÁNEA MATEMÁTICA **31** (2000) 61–105 SMM

La Lógica Matemática en el Siglo XX

Carlos Torres Alcaraz
Departamento de Matemáticas
Facultad de Ciencias
Universidad Nacional Autónoma de México
México

cta@lya.fciencias.unam.mx

La lógica formal tiene una larga historia que se remonta a la Grecia antigua. Objeto de largos períodos de olvido, todo parecía indicar, como lo dijera Kant en un célebre pasaje de la *Crítica de la razón pura*, que tras la intervención de Aristóteles poco o nada quedaba por hacer en ella[1]. Nada más alejado de la verdad. Como prueba, el siglo XX nos reveló un mundo en el que en vez de la fría silogística encontramos una diversidad de nuevas teorías jamás imaginadas por Kant y sus contemporáneos. Sin lugar a dudas, una de las causas de tal florecimiento fue la incorporación de la lógica a las matemáticas, con la consiguiente adopción de sus métodos y procedimientos: una fuerte simbolización, el uso de conceptos mediante definiciones, novedosos métodos de prueba y el recurso al método axiomático. La lógica se matematizó, sobre todo en los trabajos de Bertrand Russell, Leopold Löwenheim y David Hilbert, y con ello ambas disciplinas se enriquecieron.

Y si bien en un principio el interés de esta naciente disciplina se centró esencialmente en el problema de los fundamentos de la matemática, en donde logró sorprendentes resultados, hoy en día desborda con mucho esa esfera, y se desarrolla básicamente en cuatro direcciones: la *teoría de la demostración*, la *teoría de modelos*, la *aritmética recursiva* y la *teoría de conjuntos*, con todas las reservas que un intento clasificatorio de esta naturaleza merece.

[1] ≪Que la lógica ha tomado este camino seguro desde los tiempos más antiguos es algo que puede inferirse del hecho de que no ha necesitado dar un paso atrás desde Aristóteles [...]. Lo curioso de la lógica es que tampoco haya sido capaz, hasta hoy, de avanzar un solo paso. Según todas las apariencias se halla, pues, definitivamente concluida≫. Kant, CPR, BVIII.

En este trabajo me propongo reseñar algunos resultados significativos que darán una idea de lo acontecido en esta disciplina en el siglo XX. Obviamente, por razones de espacio me he limitado a aquellos logros que considero de mayor relevancia, sin que ello signifique que veo con desdén muchos otros que merecidamente deberían figurar en un trabajo de mayor extensión. Mi propósito es tan sólo ofrecer un panorama de un vasto territorio que no puedo describir en su totalidad en un espacio tan reducido. Muchos temas se omitieron por completo, como por ejemplo las lógicas no clásicas, la lógica intuicionista, el análisis constructivo y las pruebas de consistencia para fragmentos de la matemática clásica. Incluso en las áreas que menciono no tengo la pretensión de decir todo lo que fue importante. Más bien la selección estuvo influenciada por mis preferencias y por la elegancia o simplicidad de los temas escogidos. Un caso aparte lo constituyen la teoría de conjuntos y todo lo relativo a las ciencias de la computación, temas de los que poco hablaré en virtud de que en este mismo número de *Miscelánea Matemática* el lector encontrará trabajos dedicados en exclusiva a estas disciplinas.

Como punto de partida, en los apartados §1 y §2 expongo las nociones y resultados básicos de la lógica y el cálculo de predicados, sustrato común a todos los desarrollos subsiguientes.

1 Lógica de proposiciones y lógica de predicados.

Aunque desde el siglo XIX ya se contaba con el álgebra de la lógica de George Boole y la teoría de la cuantificación de Gottlob Frege, una de las primeras tareas de la lógica en el siglo XX fue elaborar un cálculo adecuado para la deducción lógica. Para ello, fue necesario precisar un lenguaje de fácil manejo y abordar las cuestiones de consistencia, completud e independencia de los sistemas axiomáticos.

Un rasgo de la lógica matemática en el siglo XX es el uso de letras y combinaciones de letras para representar proposiciones. Estas letras, que hacen las veces de variables proposicionales, son su verdadero objeto de estudio, y no las proposiciones reales que supuestamente representan.

En la lógica de proposiciones una proposición se define como una variable p, q, $r, \ldots$ (con o sin subíndices) o alguna de las combinaciones $\ll$no $P\gg$, $\ll P$ y $Q\gg$, $\ll P$ o $Q\gg$, $\ll$si P entonces $Q\gg$ y

≪P si y sólo si Q≫, donde P y Q representan proposiciones.

Si bien en el siglo XX se adoptaron distintas notaciones para los *conectivos lógicos* ≪no≫, ≪y≫, ≪o≫, ≪implica≫ y ≪si y sólo si≫, todas ellas comparten la cualidad de seguir un orden lineal (a diferencia de Frege, que utilizaba esquemas bidimensionales). En la siguiente tabla presentamos los símbolos más frecuentes.

Equivalente en español	Russell y Whitehead	Hilbert y Ackermann	Notación polaca	Escuela de Münster	Otras notaciones
p y q	$p \cdot q$	$p\&q$	Kpq	$p \wedge q$	pq
p o q	$p \vee q$	$p \vee q$	Apq	$p \vee q$	$p + q$
Si p entonces q	$p \supset q$	$p \rightarrow q$	Cpq	$p \rightarrow q$	$p \Rightarrow q$
no p	$\sim p$	$\overline{p}$	Np	$\overline{p}$	$p', -p, \neg p$
p si y sólo si q	$p \equiv q$	$p \sim q$	Epq	$p \longleftrightarrow q$	$p \iff q$

Lógica proposicional.

Estrictamente hablando, la *lógica proposicional* es aquella parte de la lógica que trata con argumentos cuya validez sólo depende del modo en que las proposiciones se combinan mediante los conectivos, no de su estructura interna. Por ejemplo, el argumento

$$\frac{p \vee q, p \rightarrow r, q \rightarrow s}{r \vee s}$$

es válido independientemente de la estructura interna de las proposiciones p, q, r y s. La teoría semántica de la lógica proposicional exige que cada proposición sea verdadera o falsa. Por tanto, las variables proposicionales sólo pueden adoptar dos valores, que por comodidad denotamos con 1 y 0 y denominamos *valores de verdad.* Dada un proposición compuesta, podemos determinar el valor de ésta a partir del valor de las variables que la integran, conforme a las siguientes tablas para los conectivos, conocidas como *tablas de verdad* [2]:

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \longleftrightarrow q$
1	1	0	1	1	1	1
1	0	0	0	1	0	0
0	1	1	0	1	1	0
0	0	1	0	0	1	1

¿Cómo se determinaron las tablas? En general, analizando el uso de los conectivos en el lenguaje ordinario, con la excepción de la implicación ≪$\rightarrow$≫, para la que el uso común no era suficiente. En efecto,

[2] Quizá el lector está familiarizado con este método, desarrollado por Emil Post y Ludwig Wittgenstein, y con nociones tales como las de *tautología y contradicción.* Véase, Mendelson, 1979, cap. 1.

éste nos dice que una proposición verdadera no implica nada falso (lo cual da cuenta de los dos primeros renglones de la tabla), pero no indica qué ocurre cuando el antecedente es falso. La elección de la tabla se hizo con base en la idea de que de una proposición falsa se sigue cualquier cosa, falsa o verdadera[3].

La tabla de una proposición formada con dos variables distintas tiene cuatro renglones. Dado que en cada renglón podemos llenar la casilla correspondiente con uno de dos valores posibles, es claro que hay $2^4 = 16$ funciones de verdad de dos variables. Generalizando este resultado tenemos que para una proposición compuesta por n variables distintas hay 2^n combinaciones de valores de verdad para sus componentes (verdadera $= 1$, falsa $= 0$), y que por lo tanto hay 2^{2^n} funciones de verdad de n argumentos. Este hecho posibilita el análisis exhaustivo de las fórmulas proposicionales mediante las tablas de verdad, y es un rasgo distintivo de esta lógica. En resumen, si denotamos con V al conjunto $\{1, 0\}$, veremos que toda proposición con n variables proposicionales distintas se identifica con una *función de verdad* de V^n en V.

Entre las funciones de verdad, dos clases llaman la atención: la de las *tautologías*, cuyo valor es siempre 1, y la de las *contradicciones*, cuyo valor es siempre 0. A la primera pertenecen todas aquellas proposiciones que son verdaderas en virtud de su estructura, independientemente de lo que pudieran significar, y son de especial interés para la lógica. A la segunda pertenecen aquellas proposiciones que son falsas al margen de toda circunstancia.

En general el comportamiento de las funciones de verdad corresponde al de un álgebra de Boole y han sido utilizadas con éxito en el diseño de circuitos eléctricos, donde cada letra representa un interruptor eléctrico, y los valores 1 y 0 indican simplemente si el interruptor se encuentra cerrado (pasa corriente) o abierto (no pasa corriente). Esto último nos deja ver que los valores 1 y 0 asignados a las letras p, q, r, etc. son objetos abstractos y no "la verdad" y "la falsedad".

[3]En el lenguaje coloquial hay un uso que respalda esta elección. Por ejemplo, cuando queremos ridiculizar las hipótesis en que se basa un argumento, calificándolas como "falsas", decimos "Sí, claro, si mi abuelita tuviera ruedas, sería bicicleta", dando a entender que de algo falso se sigue cualquier cosa.

Cálculo proposicional de Hilbert y Ackermann.

Pasemos de la teoría semántica a la teoría sintáctica de la lógica proposicional. En este dominio uno de los primeros objetivos fue desarrollar un *cálculo* deductivo para probar tautologías. Para ello fue necesaria una definición sintáctica de lo que es una proposición, seleccionar ciertas proposiciones como axiomas y establecer reglas de inferencia también sintácticas conforme a las cuales procede la deducción lógica.

Aunque desde Frege se conocía un cuadro de axiomas consistente y completo para las tautologías, en esta ocasión hemos seleccionado, con leves modificaciones, el sistema axiomático HA de Hilbert y Wilhelm Ackermann para la lógica de proposiciones (1928)[4].

Denotemos con L_{HA} el lenguaje indicado al comienzo de §1, con la salvedad de que sólo se consideran los conectivos $\neg$ y $\vee$ (los otros se puede definir con base en ellos)[5].

Los axiomas del sistema son todas las fórmulas con alguna de la siguientes formas:

1) $(A \vee A) \to A$ 2) $A \to (A \vee B)$
3) $(A \vee B) \to (B \vee A)$ 4) $(B \to C) \to ((A \vee B) \to (A \vee C))$.

La única regla de inferencia es *modus ponens*: de A y $A \to B$ se infiere B.

En este contexto una *prueba* es una sucesión finita de fórmulas cada una de las cuales es un axioma, o se infiere por *modus ponens* de fórmulas anteriores a ella en la sucesión.

Consistencia y completud.

Con el método de las tablas de verdad no es difícil comprobar que todos los axiomas son tautologías, y que si A y $A \to B$ son tautologías, entonces B también lo es, de donde se sigue que *todas las proposiciones demostrables en HA son tautologías.*

Esto significa, por ejemplo, que $p \wedge \neg p$ no es derivable en HA, pues no es una tautología. Es más, dado que la negación de una tautología

[4]V. Hilbert y Ackermann, 1928, §10.

[5]En este sistema los conectivos $\wedge, \to$ y $\longleftrightarrow$ se pueden definir con base en el conjunto $\{\neg, \vee\}$ como sigue:

$A \to B \equiv_{def} \neg A \vee B; A \wedge B \equiv_{def} \neg(\neg A \vee B)$ y $A \longleftrightarrow B \equiv_{def} (A \to B) \wedge (B \to A)$.

es una contradicción, resulta que si una proposición A es derivable en HA, su negación $\neg A$ no es derivable, por lo que el sistema axiomático se dice que es *consistente* (es imposible derivar en él una fórmula y su negación).

Aun más notable es el hecho de que el recíproco del enunciado anterior también es cierto: *todas las tautologías son demostrables en HA*, es decir, HA es *completo* respecto a las tablas de verdad. Esto lo demostró Emil Post en 1921 para el sistema de Russell y A.N. Whitehead de *Principia Mathematica*, el cual resulta equivalente.

Otra propiedad interesante del sistema HA, conocida como *teorema de la deducción*, fue demostrada por Jacques Herbrand en 1930: *si al añadir una proposición A a los axiomas de HA se puede inferir una proposición B, entonces la proposición $A \rightarrow B$ es derivable en HA.*

Métodos de decisión.

Las tablas de verdad proporcionan un procedimiento mecánico para decidir si una proposición es una tautología o no. Dado que las proposiciones derivables en HA coinciden con las tautologías, se sigue que las tablas de verdad constituyen un *procedimiento de decisión* para la demostrabilidad en HA, lo cual se expresa diciendo que HA es *decidible.* Como veremos, esta propiedad no la comparten otros sistemas axiomáticos más complejos que éste. De hecho, el problema de la decisión se convirtió en un tema de intensa investigación en el siglo XX, y lo podemos resumir así: *dado un conjunto de axiomas y reglas de inferencia, determinar un procedimiento mecánico para decidir si una fórmula de su lenguaje es deducible o no de los axiomas.*

Lógica de predicados.

La *lógica de predicados* es aquella parte de la lógica que trata con argumentos cuya validez no sólo depende del modo en que las proposiciones se combinan mediante los conectivos, sino de su estructura interna, y es una extensión de la lógica de proposiciones. Por ejemplo, el siguiente argumento no se puede justificar con base en la tablas de verdad[6]:

Todos los hombres son mortales, Sócrates es un hombre
Sócrates es mortal

[6]La representación de este argumento en la lógica proposicional es demasiado simple para dar cuenta de él: $\frac{p,q}{r}$

Para expresar la estructura interna de las proposiciones, en el siglo XX se introdujeron, además de variables y constantes para individuos, los cuantificadores *existencial* y *universal*. En la siguiente tabla presentamos los símbolos más frecuentes para estos operadores:

Equivalente en español	Russell y Whitehead	Hilbert y Ackermann	Kleene	Otras notaciones
Para todo x, $p(x)$	$(x)p(x)$	$(x)p(x)$	$\forall x p(x)$	$\wedge_x p(x), \prod_x p(x)$
Existe un x tal que $p(x)$	$(\exists x)p(x)$	$(Ex)p(x)$	$\exists x p(x)$	$\vee_x p(x), \sum_x p(x)$

Con esta notación podemos expresar el silogismo anterior así:

$$\frac{\forall x(h(x) \to m(x)), h(s)}{m(s)}$$

La semántica de la lógica de predicados es mucho más compleja y menos satisfactoria que la de la lógica de proposiciones. Como su nombre lo indica, en ella las proposiciones se analizan en sujeto y predicado, donde el término *predicado* lo utilizamos en un sentido general hasta abarcar no sólo propiedades de individuos, sino propiedades de conjuntos finitos y ordenados de individuos, como cuando se dice ≪6 es el mínimo común múltiplo de 2 y 3≫.

Para representar predicados la nueva lógica se valió de la notación funcional $f(x), g(x,y), h(x,y,z)$, etc. para funciones de uno o más argumentos. Esta notación, tomada del análisis por Frege, se extendió rápidamente a principios del siglo XX y desde entonces se utiliza para denotar funciones proposicionales, es decir, funciones que tiene como dominio un conjunto de individuos y como imágenes proposiciones acerca de dichos individuos. Por ejemplo, podemos representar la relación ≪x es el mínimo común múltiplo de y y z≫ con una función $m(x,y,z)$ de tres argumentos, de modo que la proposición ≪6 es el mínimo común múltiplo de 2 y 3≫ se escribe $m(6,2,3)$[7]. Esta notación trajo consigo un cambio significativo, y pronto mostró su eficacia en el análisis de la estructura lógica de las teorías matemáticas.

En la teoría semántica de la lógica de predicados se supone dado un conjunto U de individuos, denominado *dominio* de interpretación. Dado un predicado $P(x_1,\ldots,x_n)$ de n argumentos, una *interpretación* I de P es una asignación P^I de valores de verdad a todos los individuos de U^n. La idea es que un conjunto de individuos $(a_1,\ldots,a_n)$ de

[7]En la lógica moderna la notación funcional se utiliza también para representar funciones en el sentido usual de la palabra, es decir, operaciones con individuos (suma, producto, etc.). Por ejemplo, la suma de dos números naturales a y b la podemos representar con $f(a,b), +(a,b)$, o incluso $a+b$, como es usual.

U^n está en la "relación" P^I si y sólo si $P^I(a_1, \ldots, a_n) = 1$. Las reglas que determinan el valor de verdad para las fórmulas construidas con los conectivos y los cuantificadores son obvias. En este contexto decimos que una fórmula es *satisfactible* sobre un dominio si hay una interpretación que la hace verdadera para algunos individuos.

Un problema que se presenta en este punto es que cuando el dominio U es infinito, no podemos generar todas las interpretaciones posibles de un predicado P, de modo que el concepto de la *totalidad de interpretaciones* permanece como algo impreciso. De hecho, en muchos casos al establecer una interpretación resulta imposible indicar para un predicado el valor de verdad correspondiente a cada conjunto de argumentos.

Lo anterior se debe a que, además de los conectivos, la lógica de predicados incluye los operadores $\forall$ y $\exists$ para expresar la universalidad y la existencia. Cuando el dominio de interpretación es finito, digamos $D = \{d_1, \ldots, d_n\}$, el uso de los cuantificadores es en cierto sentido superficial. Por ejemplo, podemos añadir al lenguaje constantes individuales $a_1, \ldots, a_n$ para representar a los elementos de D, de modo que $\forall xP(x)$ será verdadera bajo una interpretación I si y sólo si la fórmula $P(a_1) \wedge \cdots \wedge P(a_n)$ también lo es bajo I. En cambio, cuando el dominio U es infinito no podemos hacer esto último, y cabe la posibilidad de que no podamos decidir si la propiedad P^I es válida o no para todos los individuos, o si lo es para alguno de ellos, es decir, no podamos decidir si $\forall xP(x)$ y $\exists xP(x)$ son verdaderas o no. No obstante, la teoría semántica de la lógica de predicados pasa por alto tales dificultades, y pretende que todas las fórmulas cerradas (sin variables libres) tienen sentido incluso cuando no hay manera de verificarlas.

El concepto de modelo.

La noción semántica más importante de la lógica de predicados es la noción de *modelo*. De hecho, una rama de la lógica matemática, la *teoría de modelos*, se ocupa de ella con sorprendentes resultados. Introducimos el concepto en relación al lenguaje de Hilbert y Ackermann, que denotamos por L_{HAP}.

El lenguaje L_{HAP} es muy simple. Consiste en un conjunto infinito de variables individuales x, y, z, x_1, y_1, z_1,...; un conjunto infinito de predicados F, G, H, F_1, G_1, H_1,..., cada uno de los cuales tiene asociado un número natural llamado *orden o grado* del predicado (número de argumentos), los conectivos $\neg$ y $\vee$; los cuantificadores $\forall$ (para todo) y $\exists$ (existe); y los símbolos de puntuación ")" y "(".

Adicionalmente, el lenguaje puede contar con un conjunto de constantes individuales tomadas del conjunto $a, b, c, a_1, b_1, c_1, \ldots$ y el símbolo $=$ para la igualdad (de grado 2).

Sea I una interpretación de todos los predicados del L_{HAP}. Con base en la tablas de verdad y la idea de que una fórmula $\forall xA$ $[\exists xA]$ es verdadera en caso de que A lo sea para todos [algunos] elementos de U, I determina un valor de verdad para todas las fórmulas cerradas (fórmulas sin variables libres, o *enunciados*) de L_{HAP}. En particular, si todas las fórmulas de un conjunto de enunciados Γ son verdaderas bajo I, decimos que I es un *modelo* de Γ.

A su vez, de una fórmula A decimos que es *válida* cuando es verdadera bajo todas las interpretaciones de L_{HAP}, en cuyo caso escribimos $\models A$. Las fórmulas válidas son verdaderas en virtud de su estructura lógica, no por lo que pudieran significar.

Con base en estos conceptos la noción de *consecuencia lógica* se definió así: una fórmula A es *consecuencia lógica* de un conjunto de fórmulas Γ si A es verdadera en todos los modelos de Γ (es decir, si A es verdadera siempre que todos los elementos de Γ lo son), en cuyo caso se escribe $\Gamma \models A$[8].

Las nociones de *verdad* y *validez* son altamente no constructivas, ya que en general no podemos decir si un enunciado es verdadero en un dominio infinito, y la noción de "todos los dominios" no tiene un sentido muy preciso. Esta fue una de las razones para desarrollar una teoría sintáctica para la lógica de predicados, en la que la prueba formal adoptó el mismo carácter constructivo que en el cálculo proposicional. De hecho, una de las conquistas más grandes de la lógica en el siglo XX fue el establecimiento de un vínculo preciso entre la noción de *prueba* en una teoría formal, y la noción de *consecuencia lógica*. Esto se logró a través de la construcción de un cálculo deductivo que es consistente y completo respecto a la clase de la fórmulas válidas, hecho que demostró Gödel en 1930[9]. En el siguiente apartado mostramos, con

[8]En relación a la noción de consecuencia lógica, las fórmulas válidas son consecuencia lógica de cualquier conjunto de hipótesis Γ, incluyendo al conjunto vacío $\emptyset$. Es por ello que se dice que su verdad es incondicionada. Por ejemplo, las siguiente fórmulas son válidas: $\exists x \forall y H(x,y) \rightarrow \forall y \exists x H(x,y)$ y $\forall x F(x) \longleftrightarrow \neg\exists x \neg F(x)$; en cambio, la recíproca de la primera de ellas no lo es: $\forall y \exists x H(x,y) \rightarrow \exists x \forall y H(x,y)$; piénsese en el siguiente ejemplo: si bien todos los individuos tienen un padre, no hay un individuo que sea el padre de todos los demás.

[9]La *sintaxis* trata con la estructura formal de los lenguajes, y comprende nociones tales como las de *deducibilidad formal y consistencia.* La semántica, por el contrario, se refiere a la interpretación o significado de los símbolos y comprende nociones tales como las de *satisfacción, verdad y validez.* Aquí, por conjunto de fórmulas

leves modificaciones, un sistema axiomático para la lógica (restringida) de predicados debido a Hilbert y Ackermann.

Cálculo restringido de predicados de Hilbert y Ackermann (1928).

La formalización de la lógica de predicados es análoga a la de la lógica de proposiciones: se seleccionan ciertas fórmulas como axiomas y establecen reglas de inferencia.

Consideremos el lenguaje L_{HAP} de la sección anterior. Los axiomas del sistema HAP son los del cálculo proposicional más todas las fórmulas con alguna de la siguientes formas:

5) $\forall vA(v) \to A(t)$ donde A es cualquier fórmula y t un término libre para v en A[10].
6) $A(t) \to \exists vA(v)$ donde A es cualquier fórmula y t un término libre para v en A.

Las reglas de inferencia son el *modus ponens* y las siguientes reglas para la introducción de cuantificadores:

$$I_\forall : \frac{K \to A(v)}{K \to \forall vA(v)} \qquad I_\exists : \frac{A(v) \to K}{\exists vA(v) \to K}$$

en ambos casos la variable v no figura libre en K.

No es difícil verificar que los axiomas son fórmulas válidas y que las reglas de inferencia conservan la validez, de donde se sigue que *todas las fórmulas demostrables en HAP son válidas.*

De lo anterior se sigue, por ejemplo, que $\forall y \exists xH(x,y) \to \exists x\forall yH(x,y)$ no es derivable en HAP, pues no es válida. Dado que la negación de una fórmula válida no lo es, resulta que si un enunciado A es derivable en HAP, su negación $\neg A$ no es derivable, por lo que el sistema axiomático es *consistente.*

El *teorema de la deducción* también se cumple para el sistema HAP, aunque con algunas restricciones: *si al añadir una proposición A a*

consistente se entiende un conjunto de fórmulas Γ del que no es posible deducir fórmulas contradictorias, es decir, para el que no hay una fórmula A tal que $\Gamma \vdash A$ y $\Gamma \vdash \neg A$.

[10]Es decir, si t es una variable, al sustituir t en vez de v en la fórmula A ninguna de las presencias sustituidas está dentro del alcance de un cuantificador en t. Por ejemplo, z es libre para x en $\exists yF(x)$, pero no en $\forall zG(x,z)$.

los axiomas de HAP podemos inferir una proposición B, entonces la proposición $A \to B$ es derivable en HAP siempre que en la derivación no hayamos aplicado ninguna de las reglas $I_\forall$ o $I_\exists$ respecto a una variable que figure libre en A.

Finalmente, para obtener el cálculo restringido de predicados con igualdad debemos añadir a los axiomas anteriores ciertas fórmulas cuya presentación diferimos hasta exponer una teoría formal para la aritmética.

Otras propiedades del sistema HAP serán expuestas en la siguiente sección.

2 Teoría de modelos.

El primer teorema importante en la teoría de modelos fue demostrado por Leopold Löwenheim en 1915; en él establece la posibilidad de satisfacer en el dominio de los números naturales cualquier enunciado que sea satisfactible en un dominio infinito: *si un enunciado tiene un modelo infinito, entonces tiene un modelo numerable*[11].

En 1920 Toralf Skolem generalizó este resultado. Por el *cardinal* de un lenguaje L entendemos la cardinalidad del conjunto de símbolos de L. Como los lenguajes para la lógica de predicados siempre cuenta con un conjunto numerable de variables, su cardinalidad es al menos $\aleph_0$ (son al menos numerables). Skolem demostró el siguiente teorema: *si un conjunto de enunciados pertenecientes a un lenguaje L (de cardinalidad λ) tiene un modelo infinito de cardinalidad α, también tiene un modelo de cardinalidad β para todo número transfinito β* que satisfaga $\lambda \leq \beta \leq \alpha$ (*teorema de Löwenheim-Skolem*).

Dado que la demostración de este teorema dependía del polémico axioma de elección, en 1922 Skolem ofreció una prueba de un caso especial sin recurrir a dicho principio: *si un conjunto de enunciados numerable tiene un modelo infinito, entonces tiene un modelo numerable* (es decir, un modelo de cardinalidad $\aleph_0$).

Una consecuencia de lo anterior es la llamada *paradoja de Skolem.* Con base en un lenguaje numerable podemos formalizar un fragmento T de la teoría de conjuntos y demostrar ahí el enunciado p que afirma que el sistema $\Re$ de los números reales no es numerable (es decir, que $\operatorname{card} \Re > \aleph_0$). Ahora bien, en caso de que T tenga un modelo (para lo cual, como veremos, basta con que sea consistente) por el teorema de

[11] La infinitud se refiere a la cardinalidad del dominio D de interpretación.

Skolem sabemos de la existencia de un modelo numerable, digamos M. ¡En M, el enunciado p es verdadero, a pesar de que todo lo que hay en M es numerable! Obviamente, se trata de un resultado adverso a nuestras expectativas, no de una contradicción. No hay inconsistencia por lo siguiente: la proposición que afirma que $\Re$ es no numerable se formaliza diciendo que ≪no existe una función $f\colon \Re \rightarrow N$ que sea uno a uno≫. Como sabemos, en M hay un objeto del dominio D que representa a los números reales (digamos $\Re'$), otro que representa a los números naturales (digamos N'), y muchos otros objetos que representan funciones. En este contexto decir que los reales no son un conjunto numerable significa simplemente que no hay en M un objeto que satisface la condición de ≪ser una función uno a uno de $\Re'$ en N'≫, aunque fuera de M podamos ver que sí existe tal función. La moraleja es la siguiente: el teorema de Löwenheim-Skolem nos muestra que ningún conjunto de enunciados en un lenguaje de primer orden que tenga un modelo infinito es capaz de determinar el cardinal de sus modelos: una limitación del método axiomático y del poder expresivo de esta clase de lenguajes[12].

En 1935 Alfred Tarski demostró una forma ascendente del teorema de Lówenheim-Skolem: *si un conjunto de enunciados pertenecientes a un lenguaje L (de cardinalidad $\lambda \geq \aleph_0$) tiene un modelo infinito, entonces tiene un modelo de cardinalidad α para cada $\alpha \geq \lambda$.*

Las dos formas del teorema de *Teorema de Löwenheim-Skolem* (ascendente y descendente) tienen notables consecuencias. La primera nos muestra que una teoría puede tener modelos inesperadamente grandes, y la segunda que puede tener modelos inesperadamente pequeños. Como un ejemplo de lo primero consideremos los axiomas de Peano para la aritmética de los números naturales N. Conforme a la forma ascendente del teorema de Löwenheim-Skolem, dicha teoría tiene modelos no numerables. Tales modelos son conocidos como *modelos no estándar para la aritmética.* Un ejemplo de lo segundo es el modelo numerable para la teoría de conjuntos recién mencionado.

El teorema de completud extendida.

Hacia 1930 las investigaciones en torno a la sintaxis y la semántica de los lenguajes de primer orden habían avanzado lo suficiente como

[12]Un lenguaje de primer orden es aquel en el que la cuantificación se limita a individuos, no permitiéndose cuantificar conjuntos de individuos, relaciones o funciones.

para precisar el vínculo entre la consistencia y derivabilidad formal por una parte, y la consecuencia lógica y los modelos, por la otra. Ese año Kurt Gödel demostró el que quizá sea el resultado más importante de la lógica matemática en el siglo XX. Nos referimos al *teorema de completud extendida*, según el cual *todo conjunto de enunciados consistente es satisfactible en el dominio de los números naturales* (asumiendo que el lenguaje es numerable)[13].

Lo sorprendente de este resultado es que establece un vínculo entre una noción sintáctica (la consistencia) y una noción semántica (la satisfactibilidad), mostrando que entre ellas reina una perfecta armonía. Y si bien su demostración no es constructiva (no indica cómo se construye el modelo), de él se siguen importantes consecuencias, como las siguientes:

1) *Un enunciado A es válido si y sólo si es válido en el dominio de los números naturales* (es decir, verdadero bajo todas las interpretaciones sobre N).

2) *Si un enunciado A no es derivable en HAP, entonces $\neg A$ es satisfacible en el dominio de los números naturales* (esto se debe a que en tal caso A es consistente con los axiomas de HAP).

3) *Si un enunciado $\neg A$ es inconsistente con los axiomas de HAP, entonces A es derivable en HAP.*

En efecto, al añadir $\neg A$ como axioma se obtiene un sistema inconsistente en el que toda fórmula es demostrable, incluyendo a A. Por tanto, por el teorema de la deducción, $\neg A \rightarrow A$ es derivable en HAP y por ende A (pues $(\neg A \rightarrow A) \rightarrow A$ es una tautología). En breve:

4) *Toda fórmula válida de L_{HAP} es derivable en HAP*, es decir, HAP es *completo* respecto a las fórmulas válidas (teorema de completud semántica).

Además de estos teoremas, Gödel demostró una extensión del teorema anterior en que vincula las nociones de *consecuencia lógica y deducibilidad a partir de hipótesis*:

5) *Una fórmula A de L_{HAP} es deducible en HAP a partir de un conjunto Γ de hipótesis si y sólo si A es consecuencia lógica de Γ.*

De este modo, en la lógica de predicados las nociones de ≪consecuencia lógica≫ y ≪deducibilidad formal≫ coinciden plenamente. Los lógicos se refieren a la parte ≪si $\Gamma \models_{HAP} A$, entonces $\Gamma \vdash A$≫

[13]No se debe confundir este resultado con los *teoremas de incompletud* demostrados por Gödel en 1931 y que más adelante veremos, quizá los más celebrados en la historia de la lógica.

como *corrección*, y a la parte ≪si $\Gamma \models_{HAP} A$, entonces $\Gamma \vdash A$≫ como *completud* (semántica). Otra consecuencia notable del teorema de completud es el *teorema de finitud o compacidad*:

5) *Un conjunto* Γ *de enunciados tiene un modelo si y sólo si todo subconjunto finito* Γ_0 *de* Γ *tiene un modelo.*

El primer matemático en demostrar este teorema para lenguajes no numerables fue Anatoli Maltzev en 1941. Se trata de un resultado con importantes consecuencias, como por ejemplo, la existencia de una extensión del sistema de los números reales en la que se incluyen números infinitesimales, o la imposibilidad de caracterizar la noción de orden ≪$x < y$≫ entre números reales mediante un conjunto de axiomas[14]. De algunas de estas cuestiones nos ocuparemos más adelante.

3 La aritmética recursiva.

Tras pasar lista a los sustratos fundamentales de la lógica en el siglo XX, consideremos una de las ideas más importantes que se hicieron presentes en este dominio. Nos referimos a la *definición por recurrencia*, noción que se halla presente en las investigaciones en torno a los sistemas formales, el fundamento de las matemáticas, la teoría de la calculabilidad, el problema de la decisión y las ciencias de la computación. Si bien esta idea ya se encuentra en algunos trabajos de Richard Dedekind, el primero en valorarla y desarrollarla plenamente fue Skolem en un trabajo publicado en 1923 bajo título ≪Fundamentos de la aritmética elemental por medio del método recursivo de pensamiento, sin uso de variables aparentes sobre dominios infinitos≫. Dicho escrito marcó el inicio de una disciplina fundamental, comparable en importancia con el álgebra o la geometría, y que hoy en día conocemos como *teoría de las funciones recursivas.*

Por ≪método recursivo de pensamiento≫ Skolem entiende una forma de razonamiento iterativo que marcha en paralelo con la inducción matemática, y sobre cuya base pretende reconstruir la aritmética elemental. Esta idea le sobrevino tras la lectura de *Principia Mathematica* de Russell y Whitehead, como una reacción a la teoría de tipos y la teoría de la cuantificación. Su intención era abordar el problema del infinito en matemáticas desde una perspectiva constructiva, valiéndose de métodos tan seguros que nadie podría dudar de sus conclusiones, y

[14]La imposibilidad de caracterizar el predicado ≪ $x < y$ ≫ para los números naturales se puede demostrar con el teorema de finitud para lenguajes numerables.

evitando de paso el problema planteado por las paradojas de la teoría de conjuntos.

Skolem procedió de manera informal, sin recurrir al método axiomático y evitando a toda costa la teoría de la cuantificación (es decir, el uso de variables aparentes sobre dominios infinitos, como reza el título). Supone como entendidas las siguientes nociones: *número natural, sucesor de x, sustitución de iguales por iguales y modo recursivo de pensamiento.* De estas nociones sólo la última requiere explicación. Se trata de las pruebas por inducción matemática y las definiciones por recursión, que podemos aclarar con un ejemplo. Supongamos que queremos definir la operación *suma de números naturales.* Podemos hacer esto definiendo una función f de dos argumentos mediante el siguiente esquema:

1)	$f(x, 0) = x$	(es decir, $x + 0 = x$)
2)	$f(x, sy) = sf(x, y)$	(es decir, $x + sy = s(x + y)$)

donde las dos ecuaciones a la derecha son las mismas que las de la izquierda, escritas en la notación usual. Debemos entender este esquema como un sistema de reglas que nos dicen cómo calcular la suma de dos números cualesquiera. Por ejemplo, para calcular la suma de 4 y 3 procedemos como sigue (recordando que $4 = ssss0$ y $3 = sss0$, donde $\ll sx \gg$ simboliza al sucesor de x):

	regla utilizada	escritura abreviada
$ssss0 + sss0 =$		$4 + 3 =$
$s(ssss0 + ss0) =$	(2)	$s(4 + 2) =$
$ss(ssss0 + s0) =$	(2)	$ss(4 + 1) =$
$sss(ssss0 + 0) =$	(2)	$sss(4 + 0) =$
$sss(ssss0) =$	(1)	$sss(4) =$
$sssssss0$	substitución de iguales	7

Una vez definida la suma, con su ayuda podemos definir recursivamente el *producto* de dos números naturales como sigue:

$$x \cdot 0 = 0\,; \qquad x \cdot sy = x \cdot y + x$$

A su vez, con esta última función podemos definir la *función exponencial:*

$$x^0 = 1\,; \qquad x^{sy} = x^y \cdot x$$

Nótese que la posibilidad de iterar el procedimiento queda abierta en todo momento, de modo que las funciones ya definidas sirven como base para generar nuevas funciones. Una característica de estas funciones es que sólo se definen explícitamente para el primer número natural, proveyéndose para los demás números una regla que permite calcular el valor $f(sx)$ en términos de $f(x)$. De ahí el nombre de *recursivas* (es decir, *recurrentes, que vuelven atrás*).

Funciones recursivas.

La importancia de las funciones recursivas deriva también de su relación con las nociones de *algoritmo y procedimiento efectivo*[15]. De hecho, la noción de *función recursiva* nació del intento por hacer de la noción intuitiva de *función calculable* algo más preciso.

En un sentido estricto, la *clase de la funciones recursivas* se determina de la siguiente manera: primero, ciertas funciones iniciales, consideradas como calculables de inmediato, son llamadas *recursivas*; segundo, se especifica un conjunto de reglas para generar nuevas funciones recursivas a partir de las ya obtenidas. Las siguientes funciones se suelen tomar como iniciales:

i) $C(x) = 0$ para toda x (función constante cero)
ii) $s(x) = x + 1$ (función sucesor)
iii) $I_{i,n}(x_1, \ldots, x_n) = x_i$ (funciones identidad, con $i \leq n$)

A su vez, las reglas para generar nuevas funciones son las siguientes:

iv) $f(x_1, \ldots, x_n) = h(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$ (sustitución)
v) $f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n)$
$f(x_1, \ldots, x_n, y + 1) = h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y))$ (recursión)
vi) Si g es una función de grado $n + 1$ tal que para todos los números $x_1, \ldots, x_n$ hay al menos un número y tal que $g(x_1, \ldots, x_n, y) = 0$, y la expresión $\ll \mu y[(g(x_1, \ldots, x_n, y) = 0] \gg$ denota al menor número y que es un cero de la función, entonces la ecuación

$$f(x_1, \ldots, x_n) = \mu y[g(x_1, \ldots, x_n, y) = 0]$$

define una función de grado n (minimalización).

Una definición estricta establece que una función aritmética es *recursiva* si y sólo si se puede obtener a partir de las funciones iniciales mediante un número finito de aplicaciones de las reglas (iv), (v) y (vi).

[15] Si bien los algoritmos se habían utilizado desde la antigüedad (piénsese, por ejemplo, en el algoritmo de Euclides para hallar el máximo común divisor de dos números), no fue sino hasta el siglo XX que se intentó una definición de este concepto, y la aritmética recursiva resultó el instrumento adecuado.

Además, si en el proceso de definición sólo se utilizan las reglas (iv) y (v), se dice que la función es *recursiva primitiva* (RP)[16].

Para concluir con esta sección diremos tres cosas: primero, que no es necesaria una teoría de las relaciones recursivas paralela a la teoría de las funciones recursivas, pues una relación aritmética $R \subseteq N^n$ es *recursiva* cuando su función característica lo es[17]; segundo, que la teoría de la división, la del máximo común divisor y la de la descomposición en factores primos se mueve enteramente en el espacio de la aritmética recursiva; y tercero, que todos los procedimientos de definición de funciones calculables que se han intentado conducen a los mismos resultados, no conociéndose a la fecha ninguna función calculable que no sea recursiva.

4 La aritmética de Peano.

Si bien la noción de número natural es tan antigua como la matemática, el estudio crítico de la misma no tuvo lugar sino hasta el último cuarto del siglo XIX en manos de matemáticos como Dedekind y Frege, quienes intentaron una definición lógica de los números naturales y una prueba de la validez del principio de inducción. Casi al mismo tiempo, Giuseppe Peano, siguiendo una línea de pensamiento más cercana a la matemática, construyó un sistema axiomático para el sistema de los números naturales, que dio a conocer en 1889. A diferencia de Frege y Dedekind, Peano no intentó definir los números naturales ni probar la validez del principio de inducción, sino que los postuló, estableciendo de esta manera sus propiedades básicas. En el siglo XX sus axiomas fueron la base de prácticamente todas las investigaciones formales en torno a la noción de número natural. En lo que sigue exponemos un conjunto de axiomas AP para los números naturales que se convirtió en un estándar en el siglo XX, sobre todo a partir de los trabajos de Hilbert en los años veinte. Obviamente, el sistema se inspira directamente en el de Peano, aunque con algunas modificaciones.

[16]No todas las funciones calculables son RP. Por ejemplo, se puede probar que si a partir de la suma generamos una sucesión de funciones iterando repetidamente la última función que se ha formado, de modo que a la suma le sigue el producto, a éste la exponenciación, y así sucesivamente, entonces la función $f(i, x, y)$ cuyo valor en (i, x, y) es el valor de la i-ésima función de la sucesión en (x, y), no es RP (el ejemplo se debe a Roza Péter).

[17]La función característica de R es la función $C_R : N^n \to \{1, 0\}$ tal que $C_R(X) = 0$ si y sólo si $X \in R$.

El sistema AP para la aritmética de los números naturales.

El lenguaje L_{AP} es muy reducido, sin símbolos de relación, sólo una constante ≪0≫ y tres símbolos de operación: ≪s≫ (sucesor), ≪+≫ (suma) y ≪·≫ (producto). Por comodidad, en vez de escribir $+(x, y)$ para la suma, escribiremos como es usual $x + y$, pudiéndose decir lo mismo para el producto (notación infija). El sistema de axiomas AP es el siguiente:

Axiomas para la igualdad	
$x = x$	(Identidad)
$x = y \to (A(x) \to A(y))$	(Axioma de Leibniz)
Axiomas aritméticos	
$\neg(sx = 0)$	(axiomas para el sucesor)
$sx = sy \to x = y$	
$x + 0 = x$	(axiomas para la suma)
$x + sy = s(x + y)$	
$x \cdot 0 = 0$	(axiomas para el producto)
$x \cdot sy = x \cdot y + x$	
$(A(0) \wedge \forall x(A(x) \to A(sx)) \to A(x)$	(axiomas de inducción)

Estos axiomas se utilizan como hipótesis en el cálculo de predicados para deducir los teoremas aritméticos. Aunque en L_{AP} no hay símbolos individuales para los números naturales, éstos se representan mediante las expresiones $s0$, $ss0$, $sss0$, etc. que por comodidad escribimos $\overline{1}$, $\overline{2}$, $\overline{3}$, etc.; asimismo, aunque el lenguaje no tiene un signo para la desigualdad, el predicado ≪$x < y$≫ se puede definir como sigue:

$$x < y \equiv_{def} \exists z(\neg(z = 0) \wedge x + z = y)$$

Pese a lo reducido de su lenguaje, el poder expresivo de AP es enorme, pudiéndose traducir y probar en él una multitud de proposiciones relativas a los números naturales, como por ejemplo, el teorema de Euclides sobre la existencia de una infinidad de números primos o el algoritmo de la división[18]. No obstante, y a pesar de lo satisfactorio que resulta el sistema, por el teorema de *Löwenheim-Skolem* sabemos de la existencia de una infinidad de modelos no estándar para AP.

[18]Del poder expresivo de AP hablaremos más tarde, cuando nos ocupemos de los teoremas de Gödel, que ponen un límite al poder de representación de este sistema y similares.

Representabilidad.

Si bien el lenguaje de AP carece notoriamente de signos de función, esta deficiencia no es una seria amenaza para su poder expresivo. En este sentido, en 1931 Gödel demostró un resultado (conocido como *lema de la correspondencia*) que pone en evidencia la relación existente entre el sistema AP y la aritmética recursiva: *todos los predicados y todas las funciones recursivas son representables en AP.*

Entre otras cosas, lo anterior significa que para toda relación recursiva $R(x_1, \ldots, x_n)$ existe en L_{AP} una fórmula $r(x_1, \ldots, x_n)$ con n variables libres tal que

$$\text{si } R(k_1, \ldots, k_n), \text{ entonces } AP \vdash r(\overline{k}_1, \ldots, \overline{k}_n), \text{ y}$$
$$\text{si no\_}R(k_1, \ldots, k_n), \text{ entonces } AP \vdash \neg r(\overline{k}_1, \ldots, \overline{k}_n)$$

de modo que en AP tenemos una representación exacta de las relaciones numéricas que se dan en el ámbito de la aritmética recursiva; en particular, la relación $y = f(x_1, \ldots, x_n)$ es representable cuando la función f es recursiva[19]. Este resultado es fundamental para la demostración de los teoremas de incompletud de Gödel que pronto veremos, y se puede parafrasear así: *el sistema AP contiene una formalización de la aritmética recursiva.*

Antes de finalizar queremos señalar que junto con la teoría axiomática de Zermelo Fraenkel (ZF), la aritmética de Peano se encuentra en la base de prácticamente toda la matemática moderna, habiendo sido estos dos sistemas los más estudiados por la lógica en el siglo XX[20]. Tras pasar una breve revista al programa de Hilbert volveremos a ocuparnos de AP, pues los teoremas de Gödel tratan básicamente de sus propiedades y las de sus extensiones.

5 El programa de Hilbert.

En la década de los años veinte el matemático alemán David Hilbert sugirió un camino para resolver el problema de los fundamentos de la matemática clásica, de cara a las dificultades planteadas por las paradojas y la crítica del intuicionismo. Su plan consistía en formalizar las

[19]La demostración de Gödel sólo comprende relaciones recursivas primitivas, mas es fácilmente extensible a todas las demás.

[20]En cuanto a ZF el lector encontrará la información correspondiente en el artículo sobre teoría de conjuntos en este mismo número de *Miscelánea Matemática*.

teorías matemáticas en el cálculo de predicados y probar ahí su consistencia (principalmente la aritmética de los números reales y la teoría de conjuntos). Obviamente, la formalización debería ser *completa*, en el sentido de que todo enunciado verdadero de la teoría se convirtiera en una fórmula demostrable en el sistema. Dado el carácter de la empresa, el cálculo de predicados se ofrecía como el instrumento idóneo, pues en él los modos de inferencia son algo explícito y susceptible de una investigación concreta (recordemos que probar la consistencia de un sistema axiomático es tanto como demostrar que de sus axiomas no es posible *deducir* contradicciones). Para sacar adelante su proyecto Hilbert creó una nueva teoría que denominó *metamatemática*, cuya función sería establecer la consistencia de los axiomas por medio de una investigación de índole combinatoria. A diferencia de la matemática formalizada, la metamatemática sólo recurriría a argumentos de corte intuitivo más estrictos incluso que los de Skolem, todos ellos referidos a los signos y combinaciones de signos del sistema, no a su significado[21]. Este proyecto se conoció como *programa de Hilbert*, y tenía como objetivo justificar el uso de las nociones y los métodos de la teoría cantoriana de conjuntos en la matemática, así como el uso de los métodos de prueba no constructivos que derivan de la aceptación indiscriminada del principio del tercero excluido y la teoría de la cuantificación[22].

Como un subproducto del programa, Hilbert esperaba resolver el más ambicioso *problema de la decisión*, consistente en hallar un algoritmo para responder mecánicamente a la pregunta de si una fórmula, escrita en los términos del lenguaje formal para la aritmética, se podía o no inferir de sus axiomas[23].

[21] Hilbert incluso llegó a bosquejar los métodos y procedimientos que él consideraba admisibles en una prueba de consistencia (él los llamó *finitistas*), aunque nunca los definió con precisión. Para una explicación más detallada de la naturaleza de los sistemas formales y de la metamatemática, véase Hilbert 1922 o Kleene 1974.

[22] La matemática clásica acepta de manera indiscriminada el *principio del tercero excluido*, con el cual se pueden demostrar enunciados existenciales de la forma $\exists xA(x)$ por reducción al absurdo, es decir, mostrando que su negación $\neg\exists xA(x)$ conduce a una contradicción. El problema con este tipo de demostraciones es que en ellas no se exhibe ningún objeto con la propiedad $A(x)$, sino que su existencia se afirma de manera indirecta. Tales métodos no son aceptables en la matemática finitista, donde, por ejemplo, para afirmar la existencia de una prueba lo que se tiene que hacer es exhibir dicha prueba o indicar cómo se le construye.

[23] Ya en 1900 Hilbert había expresado su confianza en que todo problema matemático se puede resolver: ≪La convicción en la resolubilidad de todo problema matemático es un poderoso incentivo para el trabajador. Oímos en nuestro interior la llamada perpetua: he ahí un problema. Busca sus solución. La puedes encontrar mediante la razón pura, pues en matemáticas no hay *ignorabimus* [ignoraremos]≫.

Estos dos problemas (el de la consistencia y el de la decisión) fueron un poderoso incentivo a las investigaciones en siglo XX. Para Hilbert, la solución favorable del problema de la consistencia daría fin al problema de los fundamentos, pues en su opinión la no contradicción es la única condición que podemos exigir a una teoría para que sea admisible en la matemática, al margen de que sea descriptiva de algún tipo de realidad, concuerde con los datos provenientes de la experiencia, o sea útil para las otras ciencias.

Alrededor de 1930 el programa parecía marchar con paso seguro hacia la consecución de sus metas: se contaba con más de un sistema formal para la matemática clásica (por ejemplo, *Principia Mathematica* de Russell y Whitehead, o la teoría axiomática ZF de Zermelo-Fraenkel) y sus seguidores trabajaban en la búsqueda de una prueba de consistencia para tales sistemas. Todo parecía ser cuestión de tiempo. Para facilitar la tarea, en un principio se intentó probar la consistencia de un sistema formal para la aritmética (básicamente el sistema AP) a fin de poner a prueba los medios elegidos, e incluso ya se contaba con una prueba de este tipo para algunos de sus fragmentos. Para entonces, Kurt Gödel era un estudiante de la Universidad de Viena que preparaba su disertación doctoral. Nadie imaginaba entonces que en breve este joven académico mostraría que los principales objetivos del programa nunca se lograrían.

6 Los teoremas de Gödel.

Cerramos el recuento de los logros alcanzados durante el primer tercio del siglo XX con los teoremas de Gödel. Estos resultados reúnen grandes atributos: profundidad, belleza, sobriedad e innovación; con ellos, Gödel establece hechos de limitación al método axiomático y circunscribe lo que se puede esperar de él, fijando así una base para la crítica filosófica.

Hasta 1930 los matemáticos creyeron posible formular un sistema de axiomas consistente en el que, al menos en principio, se pudiera demostrar la verdad o falsedad de todas las proposiciones matemáticas. A esto correspondían las ideas de consistencia y completud en el programa de Hilbert. Gödel demostró que dicha meta es inalcanzable y algo más: que las pruebas de consistencia suponen un creciente grado de complejidad.

Esto sucedió en el Segundo Congreso Internacional de Matemáticas, celebrado en París.

Estas conclusiones negativas representaron un enorme progreso tanto en la matemática como en la ciencia en general. Por decir lo menos, estos resultados significaron para la lógica un hallazgo tan importante como el de las geometrías no euclidianas para la ciencia del espacio.

Gödel dio a conocer sus teoremas en 1931, en un trabajo titulado ≪*Sobre proposiciones formalmente indecidibles de Principia Mathematica y sistemas afines I*≫[24], en el que puso en evidencia las enormes dificultades que habría que remontar para llevar a cabo la empresa hilbertiana, si es que esto era acaso posible. De entre las conclusiones que alcanza las más relevantes son las siguientes:

1) *Si escogemos un sistema bien definido de axiomas y reglas de inferencia en el que sólo sean derivables fórmulas aritméticas verdaderas, siempre habrá enunciados aritméticos de tipo elemental que son indecidibles para el sistema (es decir, fórmulas aritméticas A tales que ni A ni $\neg A$ son deducibles de los axiomas)*[25].

2) *No es posible demostrar la consistencia de los axiomas dentro del sistema mismo.*

En otras palabras, dado un sistema de axiomas matemáticos que contenga a la aritmética, siempre habrá enunciados que el sistema no puede *decidir*, es decir, enunciados cuya verdad o falsedad no se puede demostrar con base en los axiomas, siendo uno de ellos el que afirma la consistencia del sistema. La demostración que ofrece Gödel de estos hechos es constructiva, en el sentido de que en ella indica cómo obtener tales enunciados. La alternativa a esta situación es que el sistema sea inconsistente, en cuyo caso ya nada importa.

Los descubrimientos de Gödel significaron un duro revés a las pretensiones de Hilbert: por una parte, la idea de un sistema que incluyera toda la matemática no pasaba de ser una quimera, y por la otra, la posibilidad de una prueba elemental de consistencia parecía desvanecerse.

Veamos, con algunos cambios en la notación, la prueba heurística que ofrece Gödel del primer teorema sin ninguna pretensión de exactitud. El primer paso es asignar números a los símbolos, a las fórmulas

[24] *Principia Mathematica* es el título de un libro de Bertrand Russell y Alfred N. Whitehead, publicado entre 1910 y 1913 en dos tomos, en el que presentan un sistema axiomático para la matemática clásica con base en la teoría de tipos.

[25] Por ≪enunciados aritméticos de tipo elemental≫ entendemos fórmulas en las que sólo se hace referencia a las operaciones aritméticas de suma, producto y sucesor, y en las que la cuantificación sólo se realiza sobre variables numéricas.

y a las pruebas formales del sistema dado, digamos AP. Tras la asignación, las nociones y proposiciones metamatemáticas se convierten en conceptos y enunciados aritméticos acerca de números y sucesiones de números naturales, mismos que podemos expresar en el sistema. La existencia de proposiciones indecidibles se prueba mediante una aplicación del método diagonal de Cantor como sigue.

Enumérense las fórmulas con una variable libre (por ejemplo, respecto sus números de Gödel), formando una sucesión $A_1(x), A_2(x), \ldots, A_n(x), \ldots$ y sea $G(m)$ el enunciado metamatemático que afirma que $A_m(\overline{m})$ no es derivable en AP. Podemos probar (de facto, gran parte del trabajo de Gödel consiste en demostrar este hecho) que una de las fórmulas $A_n(x)$ define en el lenguaje de AP esta propiedad, digamos la fórmula $A_k(x)$ (donde k es un número entero que podemos calcular). Nótese que al sustituir $\overline{k}$ en vez de x la fórmula resultante $A_k(\overline{k})$ afirma, bajo su significado intuitivo, lo mismo que $G(k)$, es decir, que la fórmula $A_k(\overline{k})$ no es derivable en AP. En otras palabras, $A_k(\overline{k})$ *afirma* su propia inderivabilidad en AP. Si $A_k(\overline{k})$ fuera derivable en AP, entonces bajo su significado intuitivo sería verdadera y $A_k(\overline{k})$ no sería derivable en AP, lo cual sería absurdo, de donde resulta que $A_k(\overline{k})$ no es derivable en AP; mas de este último hecho se sigue que la fórmula en cuestión es verdadera, pues eso es precisamente lo que ella afirma.

A su vez, si $\neg A_k(\overline{k})$ fuera derivable en AP, entonces $A_k(\overline{k})$ sería falsa bajo su significado intuitivo y por tanto derivable en el sistema, por lo que éste no cumpliría la condición de sólo probar enunciados verdaderos. Como por hipótesis esto último no sucede, la fórmula $\neg A_k(\overline{k})$ tampoco es derivable en AP. La conclusión es que ninguna de la fórmulas $A_k(\overline{k})$ y $\neg A_k(\overline{k})$ es derivable en el sistema.

Este razonamiento muestra una interesante analogía con las paradojas de Richard y del mentiroso. La aplicación del método diagonal de Cantor salta a la vista en la construcción de la fórmula $A_k(\overline{k})$, donde el argumento toma como valor el índice de la fórmula.

La numeración de Gödel.

El método de asignación de números ideado por Gödel tiene suficiente importancia como para dedicarle algunas líneas. Tras su introducción, éste fue utilizado con éxito en muchas otras investigaciones lógicas, sobre todo en aquellas tendientes a fijar el alcance y poder expresivo de las teorías matemáticas.

Aunque la idea de codificar las "cosas" en los números ya se conocía desde la introducción del método de las coordenadas en el siglo XVII, fue Gödel quien introdujo esta práctica en la lógica matemática. El resultado fue que el discurso metamatemático acerca del sistema se transformó en un discurso aritmético, pudiéndose llevar de este modo al interior del sistema axiomático. Con su proceder pareciera suscribir la regla de que las respuestas a los grandes problemas suelen resultar de ideas muy simples.

En el caso del sistema AP la codificación comienza cuando a cada símbolo le asignamos un número. Una manera de hacerlo es la siguiente[26]:

0	$=$	s	$+$	$\cdot$	$\neg$	$\vee$	$\forall$	$\exists$	$($	$)$	x	y	z	x_1	y_1	$\dots$
1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	$\dots$

Llamemos h a esta correspondencia. Con ella, a cada fórmula corresponde una sucesión de enteros. Por ejemplo:

$$\overbrace{\neg(sx = 0)}^{\text{fórmula}} \mapsto \overbrace{11, 19, 5, 23, 3, 1, 21}^{\text{sucesión correspondiente}}$$

Ahora bien, para todo fin práctico, a cada sucesión de símbolos conviene asignarle, en vez de una sucesiones de números, un único número entero. Esto se puede hacer como sigue. Si $E = s_1 s_2 \dots s_m$ es una sucesión finita de símbolos de L_{AP}, el *número de Gödel* de E es el número $g(E) = 2^{h(s_1)} 3^{h(s_2)} \dots p_m^{h(sm)}$ donde $2, 3, \dots, p_m$ son los primeros m números primos dispuestos en orden creciente. Conforme al teorema fundamental de la aritmética (según el cual cada número natural se puede descomponer en forma única como un producto de números primos si ignoramos el orden), la función g asigna a cada expresión de L_{AP} un número distinto. Además, dado el número $g(E)$, es fácil reconstruir la expresión E a partir de él.

Repitiendo el procedimiento anterior podemos asignar a cada sucesión finita de fórmulas (en general, de expresiones) $S = E_1, E_2, \dots, E_n$ de L_{AP} un único *número de secuencia* $\gamma(S)$. Si $g_1, \dots, g_n$ son los números de Gödel de las expresiones $E_1, \dots, E_n$, entonces el número de secuencia de S es

$$\gamma(S) = 2^{g_1} 3^{g_2} \dots p_n^{g_n}$$

[26]Recordemos que el lenguaje L_{AP} para la aritmética de Peano consiste de los siguientes símbolos: *variables* $x, y, z, x_1, y_1, z_1, \dots$; *conectivos* $\neg$ y $\vee$; *cuantificadores* $\forall$ y $\exists$; *igualdad* $=$; *una constante* 0, *símbolos para función* s (de grado 1), $+$ y $\cdot$ (de grado 2) y *paréntesis*) y (.

Este modo de proceder es aplicable a un amplia gama de lenguajes, no sólo a aquellos relacionados con la lógica, y ha sido utilizado ampliamente en otros dominios, como, por ejemplo, las investigaciones en torno a las máquinas de Turing y la teoría de algoritmos.

La prueba de Gödel.

En el caso del sistema AP el método recién descrito permite asignar a cada fórmula y a cada prueba un único número natural de modo que las reglas sintácticas que describen la estructura del sistema (v. gr., aquellas que especifican cuáles expresiones son fórmulas y axiomas, cómo se lleva cabo la inferencia lógica, qué es una prueba, etc.) se convierten en operaciones y relaciones aritméticas entre números naturales[27]. ¿Se pueden expresar estas propiedades en AP? Gödel dedicó gran parte de su trabajo a mostrar que sí, valiéndose para ello de la aritmética recursiva. Metódicamente, investigó una sucesión de 45 funciones y relaciones recursivas primitivas, hasta probar que la relación $\ll x$ es el número de secuencia de una prueba y z es el número de Gödel de la fórmula que se prueba con $x\gg$[28] es recursiva, y por tanto representable en AR (*v.* §4).

Con esto Gödel dispuso de los medios suficientes para demostrar el primero de sus teoremas. Para ello definió un predicado $P(x, y)$ con la siguiente propiedad: dados dos números h y k, $P(h, k)$ es verdadero si y sólo si k es el número de Gödel de una fórmula $A(x)$ (cuya única variable libre es x) y h es el número de secuencia de una prueba de $A(\overline{k})$. Gödel demostró que este predicado es recursivo primitivo y por tanto representable en AP mediante una fórmula $p(x, z)$.

Consideremos la fórmula $\neg\exists\, xp(x, z)$ con número de Gödel g, y sustituyamos $\overline{g}$ en vez de la variable libre z, para obtener el *enunciado* de Gödel $G \equiv_{def} \neg\exists\, xp(x, \overline{g})$[29]. El primer teorema de incompletud de GÖdel establece lo siguiente:

[27]Debido a ello, al método se le conoce como *aritmetización de la sintaxis*. Por ejemplo, la propiedad ≪el símbolo v es una variable≫ la podemos expresar, conforme a la correspondencia h, diciendo que $\ll v$ es un número de la forma $2n + 1$, con $n \geq 11 \gg$, y esta última propiedad sólo alude a nociones numéricas.

[28]Esta relación la denotamos con $PR(x, y)$ y nos habremos de referir a ella más adelante.

[29]Un cuidadoso examen de G nos hará ver que se trata de un enunciado autorreferente, en el sentido de que en su lectura metamatemática afirma ser inderivable en AP, al "decir": *en AP no hay una prueba de la fórmula que resulta al sustituir en la fórmula g el numeral $\overline{g}$ en vez de la variable libre z.* Al realizar las operaciones indicadas en G, resulta que la fórmula en cuestión es ella misma.

1) Si AP es consistente, entonces G no es un teorema de AP.

2) Si AP es ω-consistente, entonces $\neg G$ no es un teorema de AP[30].

La demostración procede por contraposición en un caso y por reducción al absurdo en el otro, y tiene como base la representabilidad de la aritmética recursiva en AP. En efecto, supongamos que AP es consistente y que G sí es derivable. En tal caso hay una prueba de la fórmula g, digamos con número de secuencia h. Por tanto, $P(h, g)$ es verdadero y la fórmula $p(\overline{h}, \overline{g})$ es derivable en AP. Mas de lo anterior se sigue que $\neg G \equiv \exists\, xp(x, \overline{g})$ es un teorema de AP, por lo que el sistema es inconsistente.

Por tanto si el sistema es consistente, el enunciado G no es derivable en AP. En tal caso los enunciados aritméticos no_$P(0, g)$, no_$P(1, g)$, no_$P(2, g)$, etc. son todos verdaderos, pues ningún número natural es el número de secuencia de una prueba de la fórmula G. De esto último se sigue que todas las fórmulas $\neg p(\overline{0}, \overline{g})$, $\neg p(\overline{1}, \overline{g})$, $\neg p(\overline{2}, \overline{g})$, etc. son derivables en AP. Obligado por la forma del argumento, Gödel debió asumir en este punto la ω-consistencia del sistema: si $\neg G \equiv \exists\, xp(x, \overline{g})$ fuera un teorema de AP, el sistema sería ω-inconsistente[31].

En el mismo artículo Gödel reveló un sorprendente resultado que, curiosamente, jamás demostró. Sea $pr(x, y)$ la fórmula de L_{AP} que representa al predicado de prueba $PR(x, y)$, y sea form(x) la fórmula correspondiente a la propiedad $\ll x$ es el número de Gödel de una fórmula$\gg$. En su lectura metamatemática, el enunciado $\exists\, y[\text{form}(y) \wedge \forall\, x \neg pr(x, y)]$ afirma la existencia de una fórmula que no es derivable en AP, lo cual equivale a decir que AP es consistente (en una teoría inconsistente todas las fórmulas son derivables). Si escribimos cons$_{AP}$ como una abreviatura de este enunciado, el segundo teorema de incompletud de Gödel establece lo siguiente: *el enunciado* cons$_{AP}$ *no es derivable en* AP.

De lo anterior se sigue que en caso de que AP sea consistente, ninguna prueba de su consistencia se puede formalizar en él, pues ello equivaldría a demostrar el enunciado cons$_{AP}$. En particular, este resultado hace prácticamente imposible una prueba de consistencia finitista para la matemática clásica como la soñada por Hilbert, y echa por tierra su programa.

[30] La ω-consistencia es una condición más poderosa que la consistencia simple y se puede definir así: el sistema AP es ω-consistente si no hay una fórmula $A(x)$ tal que $\neg A(\overline{m})$ es derivable para todo $m \in N$ y $\exists\, xA(x)$ también.

[31] Al respecto, en 1936 Barkley Rosser expuso un teorema similar al de Gödel en el que sólo supone la consistencia del sistema, evitando con ello la más poderosa hipótesis de ω-consistencia.

Gödel completó su artículo mostrando que las limitaciones señaladas se cumplen para todo sistema que satisfaga un mínimo de condiciones, como son: i) que el conjunto de axiomas y reglas de inferencia sea definible recursivamente, ii) que toda relación recursiva sea definible en el sistema, y iii) que el sistema sea ω-consistente (condición que ahora podemos cambiar en favor de la consistencia simple).

Consecuencias para el programa.

Los teoremas de Gödel señalaron el fin de la euforia formalista, que había dominado a la lógica el decenio anterior con el programa de Hilbert. Esta corriente sólo admitía el proceder axiomático como modo de reconstrucción de las teorías matemáticas. Al respecto, sostenía que toda teoría se debía exponer con base en sistemas de símbolos carentes de contenido, con apego a estrictas reglas sintácticas de construcción y evitando a toda costa nociones semánticas como las de ≪verdad≫ y ≪satisfacción≫, consideradas como carentes de significado. De hecho, para los seguidores de esta tendencia la noción de prueba formal era el sustituto constructivista de la noción de verdad, la cual quedaba relegada a un segundo plano. Tal como el mismo Gödel lo dijera, una de sus motivaciones al explorar los alcances de las teorías axiomáticas fue enfrentar esta tradición, que con tanta vehemencia se oponía a su punto de vista realista[32].

En cuanto a la consistencia, éste siguió como un problema abierto para las distintas teorías matemáticas (teoría de los números, análisis matemático) y sus fragmentos. Al respecto, la actividad fue muy intensa, y sirvió como un estímulo para el desarrollo de la teoría de la demostración. En cuanto a la consistencia de AP, en 1936 Gerhard Gentzen ofreció una prueba de la misma con base en un argumento inductivo que penetra en la segunda clase de los números ordinales de Cantor, en el que quizá sea el caso más sonado en esta área[33].

A fin de cuentas, el legado de Gödel en este dominio comprende dos aspectos: por una parte, una nueva visión de la matemática en la

[32]Es decir, al punto de vista según el cual hay una realidad conceptual objetiva que es la que determina la verdad de los enunciados matemáticos, siendo la demostración un procedimiento mediante el cual se reproducen los vínculos entre tales conceptos en el plano simbólico.

[33]Respecto al problema de la consistencia, el lector encontrará un artículo dedicado al tema en el número 29 de *Miscelánea Matemática*, por lo que aquí no lo tocaremos más. V., [Torres, 1999].

que ésta aparece como una ciencia por siempre inconclusa e incapaz de asegurar su propio funcionamiento consistente; por la otra, una riqueza de métodos de investigación muy sugerentes, que pronto fueron puestos en práctica en conexión con otros problemas. La importancia de su obra se puede entonces valorar de dos maneras: por su significación y por el caudal de resultados inspirados en ella.

Indefinibilidad del concepto de verdad.

Si bien en su primer teorema de incompletud Gödel no alude a la noción de verdad (eso lo hace en la prueba heurística), éste se encuentra directamente relacionado con ella y con algo más: con la imposibilidad de definir la noción de verdad en una teoría para la aritmética[34]. De este modo el problema de la verdad volvió al escenario de la investigación lógica y abrió la puerta al estudio de las propiedades semánticas de la teorías matemáticas. Este retorno a la semántica resultó sumamente exitoso, al grado de que en la segunda mitad del siglo XX el desarrollo de la teoría de modelos fue uno de lo hechos más destacados de la lógica matemática[35].

El primero en abordar abiertamente el problema de la verdad en relación a los lenguajes formalizados fue Alfred Tarski en 1933. Recordemos la definición de *satisfacción* para fórmulas de un lenguaje de primer orden que vimos en la parte correspondiente a la lógica de predicados en el apartado §1. Si bien ésta se expuso en el lenguaje de la teoría intuitiva de conjuntos, la definición es expresable en un lenguaje L suficientemente rico por medio de la aritmetización. Lo que Tarski demostró es que si el concepto de ≪fórmula verdadera de L≫ es expresable en L, entonces en L podemos derivar contradicciones análogas

[34]De hecho, Gödel descubrió el teorema al investigar si la noción de verdad se podía identificar con la de demostrabilidad. No obstante, en la prueba del teorema evitó de propósito la noción de verdad, al parecer intimidado por el espíritu de su tiempo, y la sustituyó con la noción sintáctica de consistencia, a fin de evitar de este modo toda reacción adversa (algo que marcha acorde con su habitual cautela). En un párrafo tachado de una carta que jamás envió a un joven estudiante de nombre Yossef Balas, escrita en 1970, Gödel dice a propósito de sus teoremas de completud e incompletud: ≪A consecuencia de los prejuicios filosóficos de nuestro tiempo [...] el concepto de verdad matemática como contrapuesto al de demostrabilidad era visto con gran recelo y ampliamente rechazado como carente de sentido≫. Enfrentar tal tradición fue algo que Gödel decidió no hacer, al menos de manera frontal.

[35]Otra consecuencia de la crisis desencadena por Gödel fue que la axiomatización debió ser revalorada como lo que es, un instrumento eficaz al momento de sistematizar las teorías deductivas, y no el ser absoluto de las matemáticas: la matemática no es la ciencia de los métodos formales.

a las denominadas paradojas semánticas. Para ser más precisos, Tarski demostró lo siguiente: *si L es un lenguaje en el que todas las relaciones y funciones recursivas son expresables, entonces el conjunto $V = \{x \mid x$ es el número de Gödel de un enunciado aritmético verdadero$\}$ no es definible en L.*

Consideremos el caso específico del lenguaje L_{AP}. Conforme al teorema de Tarski, no hay en este lenguaje ningún predicado $v(x)$ con la propiedad de que $v(\overline{k})$ es verdadero en N si y sólo si k es el número de Gödel de un enunciado verdadero en N. Al igual que el primer teorema de incompletud de Gödel, la demostración de este hecho hace uso de la codificación del lenguaje L_{AP} en la aritmética recursiva, y de la representación de ésta en L_{AP}.

El resultado se obtiene al suponer que existe una expresión $v(x)$ en L_{AP} con el significado ≪x es verdadero≫. En tal caso se puede construir una fórmula $\omega(x)$ que define la siguiente propiedad: ≪la fórmula $A_m(\overline{m})$ no es verdadera≫, donde $A_1(x), A_2(x), \ldots, A_n(x)$, ... es una enumeración de las fórmulas con una variable libre de L_{AP} (digamos, respecto a sus números de Gödel). Intuitivamente, $\omega(x)$ significa: ≪la fórmula que resulta de sustituir en $A_m(x)$ el numeral $\overline{m}$ en vez de x, es falsa≫. Dado que esta última fórmula tiene una sola variable libre, debe figurar en la lista, digamos en el lugar h (es decir, $\omega(x)$ es $A_h(x)$). En tal caso la fórmula $\omega(\overline{h})$ significa ≪yo no soy verdadera≫. De hecho, este enunciado es verdadero si y sólo si es falso, lo cual prueba su inexistencia. Por tanto, el predicado ≪x es el número de Gödel de una fórmula de L_{AP} verdadera en N≫ no es expresable en L_{AP}.

Este argumento se relaciona directamente con una antinomia conocida en la antigüedad bajo el nombre de *paradoja del embustero* que citara Cicerón (106-43 a. C): ≪Si tú dices que mientes, o dices la verdad y entonces mientes, o mientes y entonces dices la verdad≫, la cual falta al principio de no contradicción (el enunciado es verdadero y falso a la vez).

Como se ve, frente a la idea de que las paradojas semánticas son meras curiosidades carentes de interés real, Tarski descubrió que hay cosas muy importantes que debemos aprender de ellas, y con su ayuda demostró que no podemos tener una noción de verdad para los enunciados de un sistema lógico sin tener que salir de él, de modo que sólo es posible definir esta noción en un metalenguaje que lo tenga como su objeto de estudio[36].

---

[36]Por ejemplo, el hecho de que el correcto uso de la lengua española nos lleva a flagrantes contradicciones es una prueba de que los lenguajes naturales no pueden

7 Algoritmos y máquinas de Turing.

La noción de algoritmo y la tesis de Church.

La década de los años treinta se distinguió por un viraje en la investigaciones lógicas. Los matemáticos, convencidos del poder de los métodos recursivos utilizados por Gödel, dirigieron su atención hacia las nociones de *calculabilidad* y de *procedimiento efectivo* o *algoritmo*[37]. Como resultado, varias caracterizaciones fueron propuestas, entre las que podemos mencionar: los sistemas canónicos de Post, el cálculo ecuacional de Gödel y Herbrand, el cálculo de conversión λ de Church, las cadenas de Markov, las funciones Turing-calculables y, por supuesto, las funciones recursivas. En este trabajo sólo trataremos con las dos últimas.

Hacia 1936 Stephen C. Kleene descubrió un hecho sorprendente: que todas la definiciones propuestas de la noción de *función calculable* eran equivalentes entre sí, en el sentido de que si una función pertenecía a una de tales categorías, también pertenecía a las otras. Por ejemplo, demostró que toda función recursiva es λ-definible (es decir, definible en el cálculo de la conversión λ de Church), y viceversa. El hecho de que éstas y otras ideas igualmente plausibles de la calculabilidad conducían a la misma clase de funciones llevó a Alonso Church a proponer en 1936 la tesis que ahora lleva su nombre, según la cual una *función es efectivamente* calculable (en el sentido intuitivo del término) si y sólo si es recursiva. Como ya lo hemos dicho, se trata de una aseveración que no es susceptible de prueba, pues en ella se equipara una noción intuitiva (la de función calculable) con una noción formal (la de función recursiva). Sin embargo, y a pesar de lo anterior, la tesis goza de una amplia aceptación, en parte porque todas las funciones calculables conocidas a la fecha son recursivas, y en parte porque todos los estudios realizados en torno a la noción de *calculabilidad efectiva* han llevado a lo mismo. Al respecto, Post se refirió a la tesis de Church como algo que no es ni definición ni axioma, sino una ley, un descubrimiento fundamental

---

expresar su semántica completamente.

[37] Con el advenimiento de las máquinas computadoras la noción de algoritmo se ha convertido en algo común. En general, por *algoritmo* se entiende un procedimiento de cómputo que toma un *valor* (o conjunto de valores) como *datos de entrada* y produce un *valor* (o conjunto de valores) como *resultado*. Una condición *sine qua non* es que el algoritmo no requiera en su ejecución de ningún pensamiento creativo, y que en principio sea posible construir un programa por medio del cual una computadora digital sea capaz de realizar las operaciones por él indicadas.

relativo al poder matematizante del *Homo Sapiens* en necesidad de una continua verificación.

Máquinas de Turing.

Íntimamente relacionada con la noción de calculabilidad se encuentra la noción de *algoritmo*, pues se considera que todo los que es calculable lo es a través de un algoritmo. Al respecto, una cuestión fundamental es la siguiente: ¿qué podemos y qué no podemos resolver por medio de algoritmos?

A fin de responder a esta pregunta, en 1936 Alan M. Turing propuso entender por *algoritmo* algo que una *máquina* puede ejecutar, es decir, algo que pueden realizar hipotéticos mecanismos muy simples conocidos como *máquinas de Turing o máquinas de cómputo automáticas*. Desde este punto de vista, especificar un algoritmo es lo mismo que describir un proceso de modo que éste puede ser seguido o imitado por una máquina, y una función se considera *efectivamente calculable* si en principio es posible construir una máquina que la calcule en todas sus instancias. Con tal propuesta, Turing tendió un puente entre ciertos problemas de lógica y el estudio teórico de los algoritmos y las máquinas de cómputo automáticas[38].

Descripción general de las máquinas de Turing.

Imaginemos un dispositivo al que se puede alimentar con una cinta infinita. La cinta se divide en celdas, cada una de las cuales o tiene impreso el símbolo | (trazo vertical) o se encuentra en blanco (lo cual a veces se expresa diciendo que tiene *impreso* el símbolo vacío, que denotamos con $*$). En cada momento de operación una y sólo una celda se encuentra en inspección por una cabeza lectora/escritora que se comunica con un mecanismo de control. Dicho mecanismo contiene una lista de instrucciones (o estados) $q_0, q_1, q_2, \ldots, q_n$ cada uno de los cuales prescribe dos cursos de acción, uno sobre lo que se ha de hacer si en la celda bajo inspección se encuentra impreso el símbolo $*$ y otro

[38]Se puede considerar que las computadoras electrónicas son máquinas de Turing. Si acaso, la única diferencia entre unas y otras es que a las máquinas de Turing se les otorga una memoria ilimitada, dado que pueden leer y escribir en una cinta de longitud infinita. Como las computadoras reales no tienen límites teóricos (sólo prácticos) para la extensión de la memoria disponible, se les atribuye una potencia comparable a la de las máquinas de Turing.

similar para el símbolo |. En todos los casos la acción prescrita se limita a las siguientes operaciones:

1) escribir en la celda alguno de los símbolos | o $*$, borrando primero lo que ahí hubiera.

2) desplazar la cinta una celda hacia la derecha (D), una celda hacia la izquierda (I) o detener el funcionamiento de la máquina (P).

3) especificar la siguiente instrucción q_i.

Por tanto, la lista de instrucciones determina una función de transición que, dada la instrucción en curso y el símbolo inspeccionado, prescribe tres cursos de acción: escribir, mover y cambiar de instrucción. Por tanto, una *máquina de Turing* se puede definir formalmente como una función M cuyo domino es el conjunto $\{q_0, q_1, \ldots, q_n\} \times \{|, *\}$ y cuyo codominio es el conjunto $\{|, *\} \times \{I, D, P\} \times \{q_0, q_1, \ldots, q_n\}$. La función M determina de manera absoluta el funcionamiento de la máquina y se puede definir mediante una tabla con un número finito de entradas.

Para representar números en la cinta acordamos lo siguiente: una cadena de $k+1$ trazos verticales | limitada a la izquierda y derecha por el símbolo $*$ representa al número k (la presencia del trazo adicional es para distinguir al número 0 de la expresión vacía, pues según lo convenido el 0 se denota con $\square | \square$). Denotamos con $\overline{k}$ esta cadena de $k+1$ trazos y la llamamos *numeral* de k.

En este contexto decimos que una función aritmética f de grado n es *Turing-calculable* si existe una máquina de Turing M tal que siempre que ésta inicia su funcionamiento en la instrucción q_0 (estado *inicial*) estando bajo inspección el primer símbolo de la expresión $\overline{k_1} \, \square \overline{k_2} \, \square \ldots \overline{k_n}$, entonces

a) si f está definida en $(k_1, k_2, \ldots, k_n)$, M se detiene estando bajo inspección algún trazo del numeral $\overline{f(k_1, k_2, \ldots, k_n)}$, y

b) si f no está definida en $(k_1, k_2, \ldots, k_n)$, M jamás se detiene, o lo hace en una celda en blanco.

Aunque la descripción de las máquinas de Turing es muy simple, son muchas y muy complejas las tareas que éstas pueden realizar, al grado de que en un famoso artículo Turing llegó a la conclusión de que no hay una diferencia esencial entre una mente y una máquina (lo cual sigue siendo un tema polémico).

Problemas irresolubles.

Pese a su capacidad para llevar a cabo cualquier tarea de cómputo concebible, hay límites al poder de las máquinas de Turing, problemas que no pueden resolver. Para establecer tales límites los investigadores recurrieron a un método de codificación similar al de Gödel, asignando a cada máquina de Turing un número, al igual que a cada configuración de la cinta con que ésta se alimenta (es decir, a la información impresa en la cinta al momento de poner en funcionamiento la máquina, la cual se supone que sólo contiene un número finito de trazos). Sin entrar en detalles sobre cómo se lleva a cabo la codificación, supondremos a la mano una de ellas y algo más: que hay máquinas de Turing que pueden llevar a cabo la codificación y la decodificación.

Un problema que no se puede resolver con una máquina de Turing es el siguiente, denominado *problema de la parada* (Turing, 1936): *dado el número* m *de una máquina de Turing M y el número c de una cinta C, construir una máquina de Turing M_p que determine si M se detendrá al ser alimentada con* c (es decir, que al poner la máquina M_p en funcionamiento estando bajo inspección el primer símbolo de la expresión $\overline{m}\,\Box\overline{c}$, ésta calculará el valor $\overline{0}$ si y sólo si el cálculo realizado por M terminará en algún momento).

La solución negativa de este problema guarda un estrecho vínculo con otro problema resuelto por Kleene en 1936: el de exhibir una función aritmética que no es calculable mediante una máquina de Turing.

Sea f la siguiente función de dos argumentos:

1) si e es el número de código de una máquina M y ésta calcula un valor al ser aplicada a un número x, entonces $f_e(x)$ es el valor que la máquina M calcula para x.

2) Si e no es el número de código de una máquina, o si la máquina M con número de código e no calcula nada para x, entonces $f_e(x)$ no está definido.

Con base en f y el procedimiento diagonal de Cantor podemos definir una función g que no es Turing-calculable como sigue:

1) si $f_x(x)$ está definido, entonces $g(x) = f_x(x) + 1$

2) si $f_x(x)$ no está definido, entonces $g(x) = 0$.

La función g no es Turing-calculable, pues si una máquina M con código p la calculara, el valor calculado por M para p sería $f_p(p) + 1$, y no $f_p(p)$, como lo debería hacer M. Obviamente, la contradicción resulta de suponer que g es calculable.

De lo anterior se sigue que la cuestión de saber si $f_x(x)$ es un valor definido no es decidible, pues si lo fuera la función g se podría calcular como sigue: primero se determinaría si $f_x(x)$ está definido. Si no lo estuviera, entonces $g(x)$ sería 0; en cambio, si lo estuviera, el valor $f_x(x)$ se calcularía imitando el comportamiento de la máquina M_x aplicada al argumento x, y $g(x)$ se obtendría añadiendo 1 a dicho valor. Esto prueba la existencia de cuestiones elementales para las que no hay un procedimiento de decisión.

A este resultado se le conoce como *teorema de irresolubilidad del problema de la parada*, pues equivale a decir que no hay un procedimiento general para decidir si una máquina M se detendrá al darle como argumento un número arbitrario x (es decir, un procedimiento para saber si M terminará por calcular un valor para x). De este resultado se sigue la irresolubilidad de muchos otros problemas. Por ejemplo, con base en él Post respondió negativamente a la siguiente cuestión, conocida como *problema de Thue para semigrupos*: dado un alfabeto A y un conjunto de reglas de sustitución de expresiones para dicho alfabeto, ¿se puede hallar un algoritmo que responda a la pregunta sobre si dos palabras cualesquiera del alfabeto son equivalentes entre sí, es decir, si se puede convertir una en la otra aplicando las reglas?

Máquinas universales.

En el penúltimo párrafo indicamos la posibilidad de imitar el comportamiento de cualquier máquina de Turing. Esto tiene como base la idea de que los seres humanos en principio podemos hacer cualquier cosa que pueda hacer una de tales máquinas, que en cierto sentido somos *máquinas universales*. En este sentido, lo que Turing hizo fue demostrar la existencia de máquinas con tal poder de imitación.

Una *máquina universal* es una máquina de Turing U que realiza la siguiente tarea: si e es el número de código de una máquina de Turing M que calcula un valor $f_e(k)$ para un número natural k, entonces la máquina U calcula el mismo valor al ser aplicada a la expresión $\overline{e}\,\square\overline{k}$ (nótese que uno de estos parámetros es el código de una máquina), o de lo contrario no calcula nada (no se detiene, o se detiene en un cuadro en blanco). Con base en la codificación, Turing demostró en 1936 la existencia de máquinas con esta habilidad: la de imitar el comportamiento de todos los demás dispositivos de cómputo automáticos[39].

[39]El concepto de *máquina de Turing universal* está relacionado con la idea de *computadora digital programable*, donde el número e corresponde al programa que

8 El problema de la decisión.

En 1933 Church demostró un resultado que se inspira en el método de aritmetización de Gödel y el procedimiento diagonal de Cantor; en él, establece la inexistencia de un procedimiento de decisión para la aritmética de Peano: *el sistema AP es indecidible, es decir, el conjunto* $T_{AP} = \{x \mid x$ *es el número de Gödel de un teorema de* $AP\}$ *no es recursivo.*

La forma en que se enuncia el teorema presupone la tesis de Church, según la cual una función aritmética es calculable si y sólo si es recursiva[40]. En el mismo trabajo Church extrajo una consecuencia quizá inesperada para algunos, y que marca una diferencia fundamental entre el cálculo de proposiciones y el cálculo de predicados: *El sistema HA es indecidible, es decir, el conjunto* $T_{HA} = \{x \mid x$ *es el número de Gödel de un teorema de* $AP\}$ *no es recursivo.*

Una consecuencia de este resultado es que no podemos idear un algoritmo para decidir si una fórmula es válida o no (esto a consecuencia del teorema de completud de Gödel), ni disponer de un procedimiento general que nos permita decidir si una fórmula A es consecuencia lógica de un conjunto de enunciados Γ. Con ello, la posibilidad de resolver favorablemente el problema de la decisión planteado por Hilbert, de vital importancia para su programa, se vino a tierra[41]. Años más tarde Alan Turing llegaría a las mismas conclusiones, esta vez por el rumbo del problema de la parada visto en la sección anterior.

---

la máquina va a ejecutar, y el número k a los datos de entrada. La máquina universal en sí corresponde a un programa que imita la acción de otras máquinas (o programas) leyendo su código. El programa residente en U es el equivalente al sistema operativo residente en algunas computadoras electrónicas que les permite correr otros programas, siendo por ello el análogo de las máquinas universales.

[40]Al respecto cabe señalar que de ser cierta la tesis de Church, la falta de un procedimiento de decisión para la aritmética no se debería a la falta de ingenio o imaginación, sino a que simplemente no habría ninguno, situación análoga a la que se presenta respecto al quinto postulado de Euclides, que no se puede derivar de los cuatro primeros postulados no por falta de talento, sino porque tal demostración es imposible.

[41]El problema lo podemos expresar mediante la siguiente pregunta ≪¿es tal o cuál proposición demostrable en una teoría que tiene tales o cuales axiomas?≫, y fue considerado por Hilbert como ≪el problema fundamental de la lógica matemática≫, y por Jacques Herbrand como ≪el problema más general de las matemáticas≫. De hecho, este problema ya había sido mencionado por Ernst Schröder en 1895, pero fue Hilbert quien en 1917, en un memorable escrito cuyas raíces se remontan a su intervención en el Congreso Internacional de Matemáticas de 1900, lo elevó a tan alto rango, y soñó con un procedimiento de decisión universal para resolver todos los problemas matemáticos.

Tales resultados atrajeron rápidamente la atención sobre esta clase de problemas, que ahora podían ser examinados con base en las nuevas técnicas de investigación. Así, una de las tareas de la lógica matemática en el siglo XX fue la búsqueda de métodos de decisión para grandes clases de problemas, o pruebas de su inexistencia.

Algunos resultados en una y otra dirección son los siguientes:

- la teoría elemental de grupos es indecidible.
- la teoría elemental de campos es indecidible.
- la teoría elemental de los grupos abelianos es decidible.
- la teoría elemental del campo de los números reales es decidible.
- la geometría elemental es decidible.
- el álgebra de Boole es decidible.
- el conjunto de fórmulas demostrables en el cálculo de predicados que sólo contienen predicados monádicos (de un sólo argumento) es decidible.
- el conjunto de fórmulas demostrables en el cálculo de predicados que sólo contienen un tipo de cuantificador es decidible.
- el conjunto de fórmulas prenex demostrables en el cálculo de predicados en las que todos los cuantificadores universales preceden a los cuantificadores existenciales es decidible[42].

En relación a las teorías axiomáticas, podemos decir que en general los resultados obtenidos han sido negativos, habiéndose visto que toda teoría suficientemente expresiva como para contener a la aritmética recursiva es indecidible. Este reconocimiento de las limitaciones y del alcance del método axiomático fue uno de los más importantes frutos de las investigaciones en torno al fundamento de las matemáticas en el siglo XX.

[42]Las fórmulas *prenex* son de la forma $Q_1x_1 \ldots Q_nx_nA$, donde cada Q_i es alguno de los cuantificadores $\forall$ o $\exists$ y A no tiene cuantificadores (a esta última se le llama *matriz* de la fórmula). Ya para los años veinte se sabía que toda fórmula en la lógica de predicados es equivalente a una fórmula prenex.

Enumerabilidad recursiva.

Una noción que pronto mostró su fecundidad en el estudio de problemas de decisión fue *la enumerabilidad recursiva*, la cual se refiere a conjuntos de números. En general se dice que un conjunto A de números naturales es *recursivamente enumerable* (RE) cuando es la imagen de una función recursiva f, en cuyo caso la sucesión $f(0), f(1), f(2), \ldots$ se dice que es una enumeración recursiva de A[43]. Esta noción corresponde a la idea intuitiva de una lista con todos los elementos de A (quizá con repeticiones) generada mediante un algoritmo. Por ejemplo, el conjunto de números pares es RE, pues es la imagen de la función $f(x) = 2x$. Un ejemplo menos simple es el de los números de Gödel de las fórmulas demostrables en AP. Para generar la lista, basta recorrer el conjunto de números naturales en orden creciente y separar aquellos que son números de secuencia de una prueba; en cada uno de ellos, el número del teorema correspondiente aparecerá como exponente del mayor factor primo del número, y ya está. Un ejemplo de conjunto que no es RE es el conjunto T_{AP} de números de Gödel de fórmulas de L_{AP} que no son teorema de AP.

El primer matemático en examinar la enumerabilidad recursiva fue Kleene en 1936 en un trabajo ahora clásico del tema. Después, en 1944 Post extendió los métodos de análisis de modo que para tratar con estos conjuntos no era necesario aludir al concepto de función calculable. Estos dos trabajos abrieron una nueva era de investigación en la lógica matemática cuyos efectos aun se sienten hoy en día en áreas como la teoría de los sistemas formales y la teoría matemática de la computación.

Post demostró que *todo conjunto recursivo es recursivamente enumerable*, pero que lo recíproco no siempre sucede. Por ejemplo, el conjunto de números de Gödel de fórmulas demostrables en AP no es recursivo, aunque es RE. Este descubrimiento tuvo importantes consecuencias e indujo una jerarquía creciente de clases de conjuntos de números naturales: los conjuntos recursivos primitivos, los conjuntos recursivos y los conjuntos recursivamente enumerables. Post también demostró el siguiente teorema: *un conjunto de números naturales es recursivo si y sólo si él y su complemento son recursivamente enumerables.* La importancia de este resultado es que permitió establecer un puente entre el problema de la decisión y la enumerabilidad recursiva:

[43]Una segunda caracterización de esta noción es la siguiente: un conjunto A es recursivamente enumerable sii hay un predicado decidible $R(x,y)$ tal que $x \in A$ si y sólo si $\exists y R(x,y)$.

el problema de la decisión de un conjunto RE tiene solución recursiva si y sólo si su complemento es RE. Como veremos, de aquí deriva la prueba de que el conjunto T_{AP} recién mencionado no es RE.

Dos ejemplos.

Hasta aquí sólo hemos evocado algunos resultados básicos de la teoría de las funciones recursivas. Para finalizar esta sección queremos referir una aplicación al problema de la enumerabilidad recursiva y un refinamiento del primer teorema de incompletud de Gödel.

No enumerabilidad recursiva de K^c.

Con base en el método de codificación de máquinas de Turing, Kleene mostró cómo codificar en los números naturales no sólo su estructura, sino la sucesión de operaciones que éstas realizan sobre una cinta predeterminada. Así, algunos números naturales z son una especie de "expediente" en el que se encuentra registrada la historia de todos los cálculos realizados por una máquina M desde que inició su operación en el estado q_0 hasta que se detuvo. Kleene llevó a cabo la codificación de modo tal que el predicado $T(e, k_1, k_2, \ldots, k_n, z)$, que es verdadero cuando e es el código de una máquina M y z es el valor calculado por M teniendo como dato de entrada la expresión $\overline{k}_1 \,\square \overline{k}_2 \,\square \ldots \,\square \overline{k}_n$, es recursivo primitivo. Ahora bien, en la sección titulada "problemas irresolubles" vimos que el conjunto $K = \{x \mid f_x(x) \text{ está definido}\}$ no es recursivo (la cuestión no es decidible). No obstante, K es recursivamente enumerable, pues $x \in K$ si y sólo si $\exists\, zT(x, x, z)$. Por tanto, concluimos que K^c no es RE, pues si lo fuera el problema de la decisión de K tendría solución recursiva.

Un refinamiento de los teoremas de Gödel.

A lo largo del siglo XX los teoremas de Gödel fueron refinados, modificados y generalizados. Una versión especialmente elegante, debida a V. A. Uspenskii y dada a conocer en 1953, incorpora el concepto de *conjuntos no separables*, introducido por Kleene en 1950.

Sean X y Z dos conjunto de números naturales recursivamente enumerables y ajenos entre sí. Decimos que X y Z son *recursivamente separables*, si existe un conjunto recursivo A tal que $X \subset A$ y $Z \subset A^c$. En el caso contrario decimos que X y Z no son recursivamente separables. Para asegurar la existencia de proposiciones indecidibles en AP y todas sus extensiones consistentes, Uspenskii demostró que los conjuntos $T_{AP} = \{x \mid x$ es el número de Gödel de un teorema de $AP\}$ y $R_{AP} = \{x \mid x$ es el número de Gödel de una fórmula refutable en $AP\}$[44] no son recursivamente separables, de donde se sigue que ninguna extensión consistente de AP puede ser completa.

En efecto, si hubiera tal extensión, digamos B, entonces $T_B \cup R_B$ sería igual al conjunto $\{x \mid x$ es el número de Gödel de un enunciado$\}$, y los conjuntos T_B y R_B serían recursivos. Por tanto, habría un conjunto recursivo A, a saber T_B, que separaría a T_{AP} y R_{AP}, lo cual contradiría el hecho de que estos conjuntos no son recursivamente separables. Por tanto, ninguna extensión consistente de AP es completa.

Asimismo, el sistema AP no es decidible, pues si lo fuera el conjunto T_{AP} sería recursivo y por tanto un separador de él y de R_{AP}. De este modo, la incompletud y la indecidibilidad de AP son una consecuencia del hecho de que T_{AP} y R_{AP} no son recursivamente separables.

9 El décimo problema de Hilbert.

En el Congreso Internacional de Matemáticas celebrado en París en 1900, Hilbert presentó una lista de 23 problemas cuya solución, pensaba, estimularía el avance de las matemáticas en el siglo XX. Algunos de estos problemas tenían que ver con la lógica y el fundamento de las matemáticas, y al respecto no se equivocó: ciertamente, fueron un poderoso estímulo para el desarrollo de esta disciplina[45]. El décimo de ellos se refiere a las ecuaciones diofánticas, y es el tema de esta sección[46].

Una ecuación diofántica es simplemente una ecuación de la forma $p(x_1, \dots, x_m) = 0$, donde $p(x_1, \dots, x_m)$ es un polinomio con coeficientes enteros. Por ejemplo, $x^3 - 2xyz + 3 = 0$ es una ecuación de este tipo.

El problema en cuestión es el siguiente: dada una ecuación diofántica con cualquier número de incógnitas, *diseñar un proceso acorde con el cual se pueda determinar mediante un número finito de operaciones si la ecuación tiene soluciones enteras* (donde por ≪*un proceso*≫ debe-

[44] *Refutable*: que su negación es demostrable.

[45] Los dos primeros son: el relativo al problema del continuo de Cantor (hipótesis del continuo) que dio lugar a innumerables investigaciones en la teoría de conjuntos, y el relativo a la compatibilidad de los axiomas aritméticos, que estimuló el desarrollo de la teoría de la demostración y dio lugar a los teoremas de Gödel.

[46] Las ecuaciones se llaman *diofánticas* en honor a Diofanto de Alejandría, quien escribió un libro sobre el tema en siglo III de nuestra era.

mos entender ≪un *algoritmo*≫). Algo esencial al problema es que las soluciones sean en números enteros, no aceptándose ni siquiera fracciones, ya no digamos números irracionales o imaginarios.

El problema fue ampliamente investigado en el siglo XX, y detrás de su solución se encuentra una amplia gama de matemáticos, entre los que podemos mencionar a Gödel, Turing, Church, Post, Kleene y, en la segunda mitad del siglo, a Martin Davis, Julia Robinson, Hilary Putnam y Yuri Matijacevic, quien finalmente lo resolvió en 1970.

La respuesta de Matijacevic es igualmente simple: *no existe tal algoritmo; el problema es indecidible.* Lo sorprendente de la solución es que nos da una mejor comprensión de las propiedades de los números enteros.

Un algoritmo como el buscado por Hilbert tomaría como datos de entrada los coeficientes de una ecuación diofántica. Como respuesta, produciría un ≪1≫ si la ecuación tiene soluciones enteras y un ≪0≫ si no (1 = sí, 0 = no). En tal caso, y con apego a la tesis de Church, se podría construir una máquina de Turing M_H que decidiría la cuestión. [Lo que sí es posible es construir una máquina de Turing M que responde con un ≪1≫ cuando una ecuación diofántica tiene solución, pero que no se detiene cuando no la tiene. El dispositivo no es muy complicado: lo único que hace es verificar una tras otra todas las sucesiones $k_1, \ldots, k_m$ de números enteros hasta encontrar una que sea solución, en cuyo caso la máquina se detiene estando bajo inspección el primer símbolo de la expresión $*\overline{1}*$. Esto es posible gracias al método de numeración de Gödel. Sin embargo, cuando la ecuación no tiene solución, la búsqueda continúa indefinidamente, y la máquina jamás se detendrá. Por ejemplo, tal cosa sucedería con la ecuación $x^2+1 = 0$. No obstante, la existencia de esta máquina lo único que demuestra es que el conjunto de ecuaciones diofánticas que tienen al menos una solución entera es RE.]

En la solución del problema Matijacevic hizo intervenir al conjunto K de la sección anterior (v. el apartado sobre la *no enumerabilidad recursiva de K^c*). La relación de este conjunto con el problema que nos ocupa es simple: en 1970 Matijacevic demostró que *todo conjunto RE tiene una ecuación diofántica correspondiente*, es decir, demostró que si A es un conjunto RE, entonces existe un polinomio con coeficientes enteros $P_A(x, y_1, \ldots, y_m)$ tal que para todo n, $n \in A$ si y sólo si la ecuación $P_A(n, y_1, \ldots, y_m) = 0$ tiene una solución. Con base en este resultado pronto llegó a la conclusión de que no puede haber un algoritmo como el buscado por Hilbert, es decir que la máquina M_H no existe.

En efecto, consideremos el polinomio $P_K(x, y_1, \ldots, y_m)$ correspondiente al conjunto K. Si tal algoritmo (máquina) existiera, la pertenencia de un número n a K la podríamos determinar viendo si la ecuación $P_K(n, y_1, \ldots, y_m) = 0$ tiene un solución, y el conjunto K sería recursivo. Mas en la sección encabezada como "problemas irresolubles" vimos que K no es recursivo, de donde se sigue que el décimo problema de Hilbert es irresoluble.

10 La teoría de modelos.

Si bien los trabajos de Löwenheim, Skolem, Tarski, Gödel y Maltzev mencionados en los apartados §1, §2 y §6 fueron los primeros esfuerzos en la teoría de modelos, esta disciplina no se desarrolló como rama separada de la lógica matemática sino hasta después de la segunda guerra mundial, sobre todo a partir de los trabajos de Leon Henkin, Abraham Robinson y Tarski en los años cuarenta y cincuenta.

Grosso modo, la teoría de modelos se puede definir como la rama de la lógica matemática que se ocupa de la relación entre los lenguajes formales (esencialmente la lógica de predicados) y sus interpretaciones. En su aspecto interno, el trabajo en esta teoría se concentró durante la segunda mitad del siglo XX en el desarrollo de métodos para construir modelos, entre los que destacan el *método de las constantes* (que incluye al teorema de finitud), las *funciones de Skolem, los ultraproductos y los modelos especiales.* Si bien todos estos métodos son muy simples en sí, en la práctica se les supo combinar de manera sutil hasta alcanzar resultados nada triviales. A su vez, en su aspecto externo, la teoría se orientó hacia la obtención de resultados en distintas ramas de la matemática, especialmente en el álgebra y el análisis. En este sentido, un dominio de especial significación fue la teoría de conjuntos, donde la construcción de modelos fue la clave en la demostración de la consistencia y la independencia de la hipótesis de continuo y el axioma de elección por parte de Gödel y Paul J. Cohen, tema sobre el que nada habremos de añadir en virtud de que en este mismo número de *Miscelánea Matemática* hay un trabajo dedicado a él.

Para finalizar queremos llamar la atención sobre un ejemplo que ilustra muy bien los alcances de esta teoría. Se trata de un modelo descubierto por Abraham Robinson para la teoría de los números reales en el que, además de los números habituales, se cuenta con números infinitesimales. Estos números, ya presentes en la obra de Cavalieri, Newton, Leibniz y Euler, fueron eliminados en el siglo XIX en favor de la noción de límite a causa de las dificultades para describirlos o justificarlos. Con su trabajo, Robinson mostró que una teoría que sólo contemple números reales es tan consistente como una que además supone la existencia de otros números que, comparados con éstos, lucen infinitesimales.

Hay dos maneras de llegar a esta teoría. La primera consiste en llevar a cabo una construcción algebraica con base en un ultraproducto; la segunda, en una aplicación del teorema de finitud ya mencionado en la sección §2.

Cada modelo de la teoría de Robinson es un campo no arquimideano R^* que extiende de manera elemental al campo R de los números reales, en el sentido de que todos los enunciados de L_R (el lenguaje correspondiente a R en la lógica de predicados) verdaderos en R también son verdaderos en relación a R^* (ambos modelos realizan los mismos enunciados de L_R). No obstante, el campo R^* contiene, además de los números estándar R, elementos infinitamente pequeños, es decir, un subconjunto $I \subset R^*$ tal que $0 < i < 1/n$ para todo $n \in N$ (siendo el inverso i^{-1} de cada uno de estos números un elemento infinitamente grande). En este contexto se cuenta con un criterio de proximidad absoluto: dos números x e y son *próximos* entre sí cuando $x - y \in I$. Así, por ejemplo, es posible hacer un lado la teoría de límites y decir que una función es continua en x si $f(x+i) - f(x)$ es infinitesimal para cada número infinitesimal i, o entender la integral como una suma infinita. A su vez, la derivada de una función f en x es un número d tal que la diferencia

$$\frac{f(x+i) - f(x)}{i} - d$$

es infinitamente pequeña para cada infinitesimal i. De esta manera Robinson obtuvo una teoría enteramente rigurosa que produce los mismos resultados que el análisis clásico, y que tiene la ventaja de poder hacer uso de los números infinitesimales. Como prueba del alcance de la nueva teoría, él y otros demostraron diversos resultados que no se habían podido probar con los métodos tradicionales (básicamente la teoría de límites) en áreas como la topología y el análisis funcional. De este modo, los números infinitesimales fueron rescatados del descrédito en que habían caído.

11 Comentario final.

Para la lógica, el siglo XX significó un periodo de renovación. Integrada al fin a la matemática, a cambio la recompensó con un conocimiento más profundo de su naturaleza y de las complejidades que se ocultan detrás de ella. Ahora sabemos, con la exactitud de un teorema matemático, de las limitaciones del método axiomático, y que la matemática no es el edificio sólido y completo que Hilbert alguna vez imaginó. También sabemos que vastos dominios de esta disciplina no son mecanizables, y que estarán por siempre abiertos a nuevos métodos y procedimientos de demostración. Así, tras los hechos limitativos, muchos de los cuales pueblan estas páginas, podemos decir con toda certeza que el *pensamiento matemático es, y debe ser, esencialmente creativo*, como dijera Emil Post hace ya algún tiempo. Esta es, quizá, la principal enseñanza que nos dejó la lógica matemática en el siglo XX.

Referencias

Bochenski, Inocenty M.,
1955 *Formale Logik*, Friburgo-Munich, K. Alber, 1955.

Davis, Martin, (editor)
1964 *The Undecidable*, Nueva York, Raven Press, 1964.

Dedekind, Richard,
1888 *Essays on the Theory of Numbers*, Nueva York, Dover Publications, 1963.

DeLong, Howard,
1971 *A Prifile of Mathematical Logic*, Reading, Massachusetts, Addison -Wesley, 1971.

Dewdney, A. K.,
1989 *The Turing Omnibus*, Nueva York, Computer Science Press, 1989.

Feys, R., y Fitch, F. B.,
1980 *Los símbolos de la lógica matemática*, Madrid, Paraninfo S. A., 1980.

Gödel, Kurt,
1931 ≪On Formally undecidable propositions of Principia Mathematica and related systems I≫, en van Heijenoort 1967, pp. 82–108

1986 *Collected Works*, vol. I: publicaciones 1929–1936, (ed. por Solomon Feferman, John W. Dawson, Jr., Stephen C. Kleene, Gregory H. Moore, Robert M. Solovay y Jean van Heijenoort), Nueva York y Oxford, Oxford University Press.

1990 *Collected Works*, vol. II: publicaciones 1938-1947, (ed. por Solomon Feferman, John W. Dawson, Jr., Stephen C. Kleene, Gregory H. Moore, Robert M. Solovay y Jean van Heijenoort), Nueva York y Oxford, Oxford University Press.

Goodstein, R. L.,
1971 *Developement of Mathematical Logic*, Glasgow, Springer-Verlag, 1971.

Heijenoort, Jean van, (editor)
1967 *From Fregeto Gödel*, Cambridge, Massachusetts, Harvard University Press, 1967.

Hilbert, David,
1900 ≪Mathematical Problems≫, en *Mathematical Developments Arising From Hilbert Problems*, American Mathematical Society, Vol. 28 parte 1.

(1993) *Fundamentos de las matemáticas* (recopilación), Colección MATHEMA, Facultad de Ciencias, UNAM, 1993.

Hilbert, David, y Ackermann, Wilhelm,
1928 *Principles of Mathematical Logic*, Nueva York, Chelsea Publishing Company, 1950.

Kleene, Stephen C.,
1952 *Introduction to Metamathematics*, Princeton, Nueva Jersey, D. Van Nostrand Company, Inc., 1952.

Kline, Morris,
1994 *El pensamiento matemático de la antigüedad a nuestros días*, Madrid, Alianza Editorial, vol III, AU 729, 1994.

Kneale, Martha y William,
1972 *El desarrollo de la lógica*, Madrid, Editorial Tecnos S. A., 1972.

Mendelson, Elliot,
1964 *Introduction to Mathematical Logic*, Nueva York, Van Nostrand Reinhold Company, 1964.

Nagel, Ernest y Newman, James, R.,
1959 *La prueba de Gödel*, México, Cuadernos del Centro de Estudios Filosóficos, UNAM, 1959.

Rogers Jr., Hartley,
1967 *Theory of Recursive Functions and Effective Computability*, Nueva York, McGraw-Hill, 1967.

Russell, Bertrand y Whitehead, Alfred,
1910 *Principia Mathematica (To *56)*, Londres, Cambridge at the University Press, 4ª ed. 1967.

Torres, Carlos,
1989 ≪La filosofía y el programa de Hilbert≫, MATHESIS, Vol. V, N° 1, pp. 33–56.

1999 ≪El segundo problema de Hilbert sobre la compatibilidad de los axiomas de la aritmética≫, *Miscelánea Matemática*, N° 29, pp. 73–97, diciembre de 1999.

Wang, Hao,
1993 *Popular Lectures on Mathematical Logic*, Nueva York, Dover Publications, Inc., 1993.