# Definibilidad. Conjuntos aritméticos. Indecidibilidad.

---

Al comenzar el curso dijimos que la Teoría de la Computación surge de la necesidad de fijar y aclarar el significado de aquello que cabe entender por "tarea efectiva" o "algoritmo". La razón de esta necesidad se encuentra a su vez en la decidida voluntad de hacer uso de los recursos de la Lógica para fundamentar un cuerpo de conocimiento matemático aquejado de defectos e incoherencias debidos, según ciertas escuelas, a una desatención hacia su estructura formal. Por paradójico que parezca, las respuestas que la Teoría de la Computación ofrece a estas demandas se producen antes incluso de que ciertas cuestiones centrales para dicha disciplina hayan sido resueltas, y adoptan además, la forma de resultados de limitación de fuerte carga epistemológica. Me refiero, en concreto, a ese gran problema que el curso de los acontecimientos pospuso a la resolución de otros asuntos y que fue bautizado por Hilbert como *Problema de la Decisión* –Entscheidungsproblem-. En este capítulo veremos el modo en que Church y Turing proponen de manera casi simultánea una respuesta negativa a este problema, contribuyendo de forma decisiva a poner fin a la fascinación que los métodos de la naciente Lógica matemática había ejercido durante las primeras décadas del siglo xx.

De todos modos sería inadecuado concluir que los contenidos de un curso como éste se justifican por el interés de un último apartado como el que ahora se aborda, o lo que es lo mismo, por la utilidad de la Teoría de la Computación para la Lógica contemporánea. La historia real de la Teoría de la Computación recuerda en algo el descubrimiento de un nuevo Continente en la búsqueda de una nueva ruta hacia otro ya conocido. Del mismo modo que no pasó mucho tiempo hasta reconocer que la magnitud del descubrimiento real superaba con mucho la del que era pretendido originalmente, la

Teoría de la Computación pronto ganó en impulso y resultados a la Lógica dentro de la cual da sus primeros pasos.

Hemos dicho que la Matemática de comienzos de siglo busca resolver sus problemas de fundamentación sirviéndose para ello de los recursos de la Lógica, pero ¿qué recursos eran estos? La Lógica puede ser considerada sin asumir especiales compromisos como la ciencia dedicada al *estudio de la consecuencia en el dominio de los lenguajes formales*. Lo primero que procede es fijar un lenguaje suficientemente flexible como para *traducir* el tipo de razonamientos que, por ejemplo, hemos desarrollado en las demostraciones de los lemas y teoremas expuestos en este curso. Aunque ésta puede parecer en principio una tarea difícil de satisfacer, buena parte del éxito de la Lógica se basa, ya lo hemos visto, en la habilidad del lenguaje de la Lógica de Primer Orden para cumplir con este expediente. Será ese lenguaje, $L_C$ en símbolos, el que tengamos en mente a lo largo de este capítulo –cfr. cap. 2.1-.

En primer lugar se van a introducir, o simplemente recordar, algunas nociones fundamentales en el dominio de la Lógica formal. Una vez hecho esto se presentará una teoría formal considerada por muchos como la menor porción de conocimiento matemático que cabe considerar sin tratarse de un corte o amputación arbitraria. A continuación se dará entrada a la noción fundamental de *definibilidad.* Con su ayuda veremos una forma más general de alcanzar los resultados de limitación de Gödel y otro interesante teorema en esa misma dirección, el de *indefinibilidad del predicado verdad*. Finalmente dirigiremos nuestra atención al teorema de Church sobre indecidibilidad cerrando con ello, y a muy grandes trazos, los objetivos principales que nos habíamos propuesto en un principio.

Aunque muchas de estas definiciones ya han sido presentadas en el capítulo 2.1, tal vez convenga tenerlas todas juntas de una vez:

[1] *Teorías.* Un conjunto X constituye una *teoría* syss para toda fórmula A, sucede que $A \in X$ syss $X \mid A$.

## *Indecidibilidad*

Si los enunciados que forman una teoría X son expresables todos ellos en un lenguaje cuyas categorías son exactamente las que fija $L_C$, diremos que es una *teoría de primer orden*. Parece evidente que un lenguaje como $L_C$ sugiere la posibilidad de formar una teoría de primer orden que contenga exactamente aquellos enunciados que expresan verdades de la Aritmética asociadas a lo que hemos denominado su interpretación estándar. Ya sabemos que esto no es posible para teorías formales tan potentes como AP, pero, ¿existe alguna otra porción de esas verdades con suficiente sentido que sea expresable en términos de alguna teoría formal razonable?

De lo que se trata es de proceder de forma tentativa construyendo ciertas aproximaciones relevantes desde un punto de vista matemático. Para ello intentaremos dotarnos de una colección de axiomas específicos sobre los cuales generar una relación de consecuencia que conduzca a teorías notables por su contenido aritmético. El siguiente sistema fue popularizado por Tarski, Mostowski y Robinson y será nuestro punto de partida en lo que sigue:

[2] *Aritmética mínimal* Q (Tarski, Mostowski, Robinson):

Ax.1. $\forall xy(x'=y' \rightarrow x=y)$

Ax.2. $\forall x\neg(x'=0)$

Ax.3. $\forall x(\neg(x=0 \rightarrow \neg\exists y(x=y'))$

Ax.4. $\forall x(x+0=x)$

Ax.5. $\forall x\forall y[(x+y')=(x+y)']$

Ax.6. $\forall y(yx0=0)$

Ax.7. $\forall y\forall z[(yxz')=(yxz)+y]$.

Antes de proseguir será bueno recordar algunas propiedades más acerca de teorías:

[3] *Teorías: propiedades*

i. $\Gamma$ es *axiomatizable* si existe un subconjunto de $\Gamma$ del cual resulta $\Gamma$ como su clausura deductiva.

ii. $\Gamma$ es *finitamente axiomatizable* si su conjunto de axiomas es finito.

iii. $\Gamma$ es *consistente* si no es capaz de derivar una fórmula y su negación.

iv. $\Gamma$ es *completa* dada una interpretación o modelo estándar si contiene todas las verdades relativamente a esa interpretación o modelo.

v. $\Gamma$ es *decidible* si su función característica es recursiva.

Esta presentación del sistema Q hace de él una teoría finitamente axiomatizable de la cual ignoramos el resto de sus propiedades, aunque podamos suponer –y demostrar- con cierta inmediatez que al menos es consistente. A continuación vamos a considerar, siquiera de forma ideal, una teoría que integrada por todas las verdades de la aritmética expresables en el lenguaje $L_C$ bajo el modelo estándar –en el que los símbolos artiméticos empleados tienen su significado habitual, y el dominio está formado por los números naturales (los auténticos enteros)-. Es evidente que esta teoría, a la que denominamos Th(ù), es completa *por definición* en el sentido de [3.iv] aunque ignoremos el resto de su conducta. Sería realmente afortunado comprobar que ù no es nada distinto de *Q*, o lo que es lo mismo, que el cuerpo de verdades aritméticas expresables en $L_C$ constituye una teoría deductiva finitamente axiomatizable. A lo largo de este capítulo tendremos ocasión de comprobar que ù no es finitamente axiomatizable, ni aún axiomatizable, con lo que tampoco constituye propiamente una teoría al menos en

el sentido que aquí se le atribuye al término. Otra forma de resumir este resultado consiste en afirmar la inexistencia de una teoría a la vez consistente, completa y axiomatizable de la Aritmética. Esta limitación de nuestra capacidad deductiva, apartada en apariencia de los contenidos de este curso, es el resultado de una interesante observación: *Q* constituye justamente la versión más elemental de las teorías axiomatizables atenidas al modelo estándar de la Aritmética que es a la vez capaz de representar en su interior un fragmento relevante de las funciones computables, a saber, el formado por las funciones recursivas totalmente definidas con rango y dominio sobre los naturales.

El estudio de la capacidad de una teoría formalizada de la Aritmética para capturar fragmentos relevantes de la clase de los procedimientos llamados efectivos, no es una cuestión puramente estética. Si resultase posible demostrar que *Q*, por ejemplo, contiene esa porción de conocimiento matemático entonces cabría discutir un hecho de importancia trascendental como es el siguiente: ¿son los procedimientos de prueba de *Q* procedimientos efectivos definibles en *Q*? Si es así, nuestra teoría axiomática procederá como una teoría deductiva a la hora de establecer sus teoremas, dicho de otra forma, habremos mostrado que una teoría axiomática de la Aritmética tiene el efecto de reducir la investigación en teoría elemental de números a un ejercicio deductivo puramente formal.

Ya sabemos que el final de esta apasionada historia lo pone Gödel al proponer la primera aproximación a lo que es el contenido de la clase de procedimientos efectivos, la clase de las funciones recursivas primitivas, y demostrar su representabilidad en *AP*. El tiempo ha permitido comprobar que la capacidad de un lenguaje formal para representar funciones o propiedades predicables de números tiene un interés intrínseco al suministrar una medida de la complejidad de aquellas propiedades o funciones. La capacidad para representar un fragmento de las funciones recursivas en *Q* -*AP*- es así una instancia de un fenómeno mucho más general conocido bajo el nombre de *definibilidad*.

[4] *Definibilidad*

Dada una teoría T,

i. La función n-aria $f(x_1,...x_n)$ es *definible en T* si existe una fórmula $A(x_1,...x_n,y)$ tal que para cualesquiera naturales $k_1,... k_n, j$ si $f(k_1,...k_n)=j$ entonces $|_T \forall y(A(k_1,...k_n,y)\leftrightarrow y=j)$

ii. El conjunto $\Delta$ es definible en T si existe una fórmula A(x) tal que para cualquier número natural *k*: a) si $k\in\Delta$ entonces $|_T A(k)$ y b) si $k\notin\Delta$ entonces $|_T \neg A(k)$.

La definibilidad aplicada a subconjuntos de ù constituye la acepción más amplia del término al permitir extender su aplicación a relaciones sobre $ù^n$ -considerando el conjunto de las tuplas que las satisfacen- y de ahí de nuevo a funciones. Sea como fuere, la noción introducida ahora permite una nueva medida de la complejidad de una relación o función derivada del estudio de la fórmula que define dicha función o relación en una teoría T. Apreciaremos la importancia de estos comentarios al ver de qué forma el lenguaje de primer orden en que se expresa una teoría de suficiente potencia permite generar una jerarquía de grados de complejidad útil para el estudio de los objetos matemáticos definibles en dicha teoría. Pero antes de eso necesitamos fijar una especie de *hito* que permita asentar esa jerarquía sobre una base firme, dicho de otro modo, necesitamos determinar una clase significativa de relaciones o funciones definibles sobre la que operar a continuación. Este resultado, nos devuelve a los teoremas de Gödel que fueron objeto de discusión en el capítulo 1.2:

[5] Teorema: La clase de las funciones recursivas totalmente definidas con rango y dominio en ù es definible en *Q*.

Es evidente que el resultado anterior se predica inmediatamente de la relaciones recursivas $R^i_j$ y de cualesquiera subconjuntos en ù utilizando para ello la conexión existente entre estas entidades y las funciones recursivas. Observamos entonces que la clase formada por las relaciones recursivas (conjuntos recursivos) resulta definible en *Q* fijando de este modo la mínima conexión entre complejidad y lenguaje que anunciábamos líneas atrás. Sea $\Pi_0$ la clase de todas las relaciones recursivas. Si definimos ahora:

[6] *Jerarquía aritmética*:

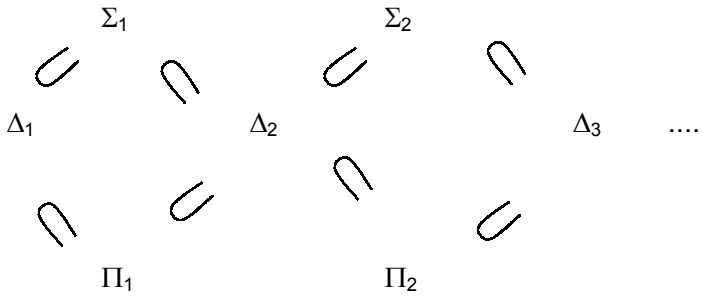
i. $\Sigma_{n+1}=\exists xA$, donde A es una relación $\Pi_n$

ii. $\Pi_n$= complementario de $\Sigma_n$

iii. $\Delta_n=\Sigma_n 1 \Pi_n$,

obtenemos una expresión de la complejidad de relaciones, funciones y conjuntos apoyada en la capacidad expresiva de un lenguaje como $L_C$. Un resultado que no vamos a comentar ahora permite establecer el siguiente cuadro:

[7]



Es evidente que el ascenso por la jerarquía determina mayores grados de complejidad en las fórmulas que definen una relación o conjunto, y por tanto, un mayor alejamiento de las técnicas recursivas de representación. Obsérvese que la jerarquía aritmética permite establecer, mediante el uso de técnicas elementales para teorías de primer orden, que una relación o conjunto es $\Sigma_{n+1}$ syss existe una fórmula con *n* cuantores alternados, el primero de los cuales es existencial, y tal que define dicha relación en *Q*. La definición de $\Pi_{n+1}$ permite afirmar lo mismo para una fórmula con *n* cuantores alternados el primero de los cuales es esta vez universal. Esta observación da lugar, por ejemplo, a que la clase de las relaciones recursivamente enumerables -r.e.- sea precisamente la clase de relaciones $\Sigma_1$. Por la definición [6] resulta entonces que la clase $\Delta_1$ es la clase de las relaciones r.e con complementos expresables también por medio de fórmulas en $\Delta_1$, o lo que es lo mismo, con complementos r.e. Esta observación hace de $\Delta_1$ la clase de las relaciones recursivas.

En lo que sigue utilizaremos mucho más el teorema [5] y sus consecuencias que la jerarquía a que da lugar. En cualquier caso, iniciamos la parte final de este apartado estudiando una cuestión fácilmente expresable ahora en términos de la jerarquía aritmética.

La relación de prueba que se define entre un conjunto finito de fórmulas X, y otra fórmula A a partir de un sistema como el que da lugar a *Q* puede ser expresada ahora como una relación representable como $R_{Prov}(X,A)$. Evidentemente, $R_{Prov}(X,A)$ no es una relación definible en el modelo estándar de *Q* por la sencilla razón de que sus argumentos son fórmulas y no números naturales. No obstante el potencial analítico de *Q*, puesto de manifiesto a través de la noción de definibilidad, parece sugerir la conveniencia de superar ese obstáculo intentado verter $R_{Prov}(X,A)$ sobre alguna relación expresable en el lenguaje de *Q*. Bastará para ello conseguir asociar a cada enunciado de $L_C$ un entero positivo que actúe como su código para comprobar después si existe alguna relación en el lenguaje de *Q* establecida entre códigos de fórmulas que *defina* $R_{Prov}(X,A)$. Esto da lugar a:

[8] Teorema: La relación $Prov_Q([A],[B])$ establecida entre los códigos de sendas fórmulas A,B en $L_C$ define recursivamente la relación $A|_CB$ - análogamente $R_{Prov}(\{A\},B)$.

Este resultado fue establecido por primera vez por Gödel para *AP* operando sobre la clase de funciones recursivas primitivas. $Prov_{AP}$ resultaba así una relación recursiva primitiva y definible por tanto en *AP*.

Una vez alcanzado este punto observamos que la noción que mejor caracteriza una teoría axiomática, la que se expresa en el predicado de prueba $|_QB$ que hace de B un teorema de *Q*, queda bajo el potencial analítico brindado por la definibilidad de ciertas relaciones metateóricas como $Prov_Q$. La teorematicidad en *Q* puede expresarse definicionalmente del siguiente modo:

[9] $Pr_Q([B])=_{def}\exists yProv_Q(y,[B])$,

El predicado $Pr_Q([B])$ afirma entonces que la fórmula cuyo código figura como argumento es tal que existe un código asociado a una cadena de fórmulas -expresable como su conjunción- que constituye una demostración en *Q* de la fórmula cuyo código es [B]. Nótese que nos hemos limitado a analizar el aspecto de la fórmula que permite expresar el predicado de prueba de *Q* sin presumir si dicha expresión *define*, en el sentido que aquí se le ha atribuido al término, dicho predicado en *Q*. Si así fuera, el predicado $Pr_Q$ pasaría a formar parte, en virtud tan sólo del teorema 8, de la clase de relaciones $\Sigma_1$-definibles. Una vez ahí aún sería posible progresar en precisión considerando si el complemento de dicha clase, el formado por enunciados de $L_C$ que no son teoremas de *Q*, posee una definición $\Sigma_1$. En caso afirmativo, habríamos llegado a comprobar el carácter $\Delta_1$ de $Pr_Q$ haciendo de él un predicado recursivo. Este par de

conjeturas demuestran que el análisis de la proximidad que exhibe la noción de prueba de *Q* a la clase de procedimientos recursivos se transforma, gracias a la potencia expresiva de *Q*, en el estudio de la definibilidad del predicado $Pr_Q$ asociado inicialmente a una expresión del tipo $\Sigma_1$. Un análisis algo más detallado de las consecuencias de operar con una teoría capaz de codificar su propia sintaxis demuestra que la cantidad de *autorreferencia* que de ello se obtiene impide definir $Pr_Q$ en *Q* haciendo extensiva además esa limitación a cualquier extensión consistente de dicho fragmento de la Aritmética.

[9] Sea sust([B(x)],[t]) la función que caracterizada por satisfacer la ecuación sust([B(x)],[t])=[B(t)].

Esta función arroja como valor el código de la fórmula que resulta al substituir en B(x) su única variable libre *x* por el término *t*. Asumimos sin demostración que sust(x,y) es definible en *Q* y que es, además, una función recursiva -recursiva primitiva. Mediante su concurso procedemos a introducir un resultado que desempeña en el contexto de los fragmentos de la Aritmética el mismo papel que el Teorema de recursión desempeña en el dominio de las funciones computables: controla la conducta de la autorreferencia inducida por la codificación que *Q* efectúa de su sintaxis.

[10] Lema de Diagonalización: Sea S(x) un predicado expresable en el lenguaje de *Q* con *x* como única variable libre. Es posible construir entonces una fórmula $\beta$ en ese mismo lenguaje tal que:

$\vdash_T B \leftrightarrow S([B])$, donde *T* es cualquier extensión consistente de *Q*.

Esquema de la demostración: En primer lugar tomamos el predicado S(x) para definir $U(x)=_{def}S(sust(x,x))$. Este nuevo predicado recibe el nombre de *diagonalización* de S(x). Puesto que U(x) es expresable en $L_C$, podemos conjeturar la existencia de un entero positivo *k* que codifica dicho predicado de tal modo que k=[U(x)]. Definimos B como U(k) y procedemos ahora a construir la afirmación introducida en el enunciado del lema.

$|_T B \leftrightarrow U(k)$, por la definición de B

$|_T B \leftrightarrow S(sust(k,k))$, por la definición de U(x) y haciendo x=k

$|_T B \leftrightarrow S(sust([U(x)],k))$, por la elección de *k*.

$|_T B \leftrightarrow S([U(k)])$, por la definición de sust(x,y)

$|_T B \leftrightarrow S([B])$, por la elección de B.

Puede ser un ejercicio interesante para el lector que no renuncia a los detalles analizar las similitudes entre esta demostración y la que lleva a establecer el Teorema de recursión. En particular, resulta especialmente revelador comprobar la forma en que ciertas funciones actúan como generadores de autorreferencia en el seno de funciones o relaciones arbitrarias. En el caso del Lema de diagonalización parece evidente que la función relevante es sust(x,y) mientras que en el caso del Teorema de recursión la responsable era la función s(x,y) cuya existencia determina el Teorema de los parámetros.

Al igual que se hiciera con las entidades cuya existencia quedaba demostrada por el Teorema de la Recursión, denominaremos *punto fijo* a aquella fórmula cuya existencia acabamos de demostrar para predicados arbitrarios en teorías del tipo indicado. El resultado de limitación mencionado líneas atrás a propósito del predicado $Pr_Q$ surge, precisamente, del estudio de un punto fijo basado en dicho predicado. Estudiaremos el problema de la definibilidad del predicado $Pr_T$ en términos de la definibilidad del conjunto numérico que constituye su extensión, esto es, a través de la definibilidad del conjunto de enteros positivos que son códigos de teoremas de *T*.

[11] Teorema: El predicado $Pr_T$, donde *T* es cualquier extensión consistente de *Q*, no es definible en *T*.

Esquema de la demostración: Supondremos que $Pr_T$ es definible en *T* para localizar una contradicción. Si $Pr_T$ es definible syss lo es el conjunto $\{k/Pr_T(k)\}$, lo que permite utilizar los términos de la definición [4.ii]. Haciendo uso del Lema de Diagonalización podemos asegurar la existencia de un punto fijo *g*, cuya fórmula característica es: $\vdash_T g \leftrightarrow \neg Pr_T([g])$. Desde el punto de vista de *T*, sólo pueden suceder dos cosas dado *g*, que $g \in Pr_T$ o que $g \notin Pr_T$. Supongamos que $g \in Pr_T$, esto es, que $\vdash_T g$. Puesto que hemos asumido que $Pr_T$ es definible en *T*, $\vdash_T Pr_T([g])$, de donde por su definición y lógica elemental se tiene que $\vdash_T \neg g$, resultando *T* inconsistente contrariamente a lo que se había establecido. Por tanto, debemos concluir que $g \notin Pr_T$. Pero en tal caso y puesto que asumimos la definibilidad de $Pr_T$, $\vdash_T \neg Pr_T([g])$. Por lógica elemental y la definición de *g* se tiene entonces que $\vdash_T g$, de donde resulta que $g \in Pr_T$. De esta contradicción se sigue, pues, que $Pr_T$ no es definible en *T*.

Este resultado, generado a partir de un enunciado autorreferencial conocido por extensión como *punto fijo de Gödel* viene a ofrecer algo similar a lo que sería un centro de gravedad sobre el cual giran unos cuantos resultados de trascendental importancia. A ellos se dedica las siguientes líneas.

La principal virtud del teorema 11, en comparación por ejemplo con su inmediato antecesor, el Primer Teorema de Incompletitud de Gödel, reside en la economía de medios y en el mayor rigor concedido al análisis de sus condiciones de contorno. Tal vez por ello es frecuente confundir ambos resultados haciendo pasar el Teorema 11 por una versión remozada del citado Teorema de Gödel. En resumen, hemos podido comprobar

de qué modo la existencia de teorías axiomáticas de fragmentos relevantes de la Aritmética no mejora en mucho la situación que dio lugar a su búsqueda y análisis. Teorías incluso tan débiles como *Q* demuestran que el predicado de prueba asociado a su presentación axiomática queda más allá del alcance de la colección de procedimientos efectivos -recursivos- que presuntamente caracterizan el núcleo más firme de nuestro conocimiento matemático: el conocimiento constructivo. La claridad e inmediatez de este resultado quedan a la vista de forma inmejorable en el Teorema 11 al ofrecer el mejor equilibrio posible entre las diversas propiedades a exigir en cualquier teoría matemática: *Q* es la más elemental de las teorías consistentes de la Aritmética que puede ser representada como una teoría finitamente axiomatizable y cuya potencia expresiva es suficiente para capturar el dominio más representativo de las funciones, relaciones y conjuntos recursivos. Que dicha potencia resulte suficiente para permitir codificar la sintaxis de una teoría tal, generando así dosis relevantes de conducta autorreferencial es, posiblemente, uno de los goznes sobre los cuales pivota la estructura más íntima de nuestro ingenio matemático.

Compete ahora mostrar de qué modo el contenido del Teorema 11 afecta a otras teorías y nociones en su entorno. Para ello resultará útil disponer del siguiente resultado:

[12] Lema*:* Sea *T* una extensión consistente de *Q*. *T* no es decidible.

Esquema de la demostración: Basta observar que en caso de ser *T* decidible la función característica asociada al conjunto de enteros positivos que codifican teoremas de *T* sería recursiva y por tanto definible en *T*. Pero eso es tanto como afirmar que $Pr_T$ es recursivo lo cual contradice el Teorema [11]

Una consecuencia previsible a partir del tratamiento que se ha concedido a todo lo dicho acerca de *Q* es su efecto inmediato sobre extensiones consistentes de dicho fragmento de la Aritmética. Mucho menos evidente es el tipo de influencia que eso mismo

pueda tener sobre sistemas substancialmente más débiles que *Q*, influencias, claro está, que vayan más allá de una mera decepción general acerca de las virtudes de los sistemas axiomáticos. Este comentario permite rastrear el impacto del Teorema 11 en dos direcciones, una *descendente*, en la que el sujeto de análisis son sistemas o teorías más débiles que *Q*, y otra *ascendente* en el que el sujeto son sus extensiones, con la vista puesta finalmente en algo tan general como el conjunto de todas las verdades de la Aritmética. Comentaremos algún ejemplo destacado en cada una de estas direcciones.

En sentido descendente lo más débil que encontramos bajo la corteza de un fragmento de primer orden de la Aritmética es, cómo no, la propia Lógica de Primer Orden -LPO en siglas. A diferencia de lo que sucede con *Q*, LPO carece de un modelo estándar asociado a sus símbolos no-lógicos. Esto hace que sea posible obtener una teoría para cada interpretación admisible de sus signos no-lógicos y que, en definitiva, nos veamos obligados a considerar una menor teoría de entre ellas, su intersección, como aquella asociada a LPO por excelencia. Esta mayor generalidad hace que algunos términos varíen su significado, consistencia y completitud, por ejemplo, preservando el sentido de los restantes. Entre estos últimos se centran los que ahora interesan. En primer lugar, LPO constituye un sistema finitamente axiomatizable para el cual es posible demostrar además, que aquellas fórmulas que resultan verdaderas bajo todo modelo admisible son teoremas de LPO -versión adaptada de la completitud. Puesto que LPO se comporta como un sistema deductivo caracterizable por el conjunto de sus teoremas, una de las preguntas que inmediatamente surgen es la de si LPO es decidible en el sentido de [3.v]. Usamos el Teorema [11] a través del Lema [12] para establecer el siguiente resultado originalmente establecido por Church en 1936 aunque con un formato y una demostración bastante distintas de las que a continuación se ofrecen.

[13] Teorema de indecidibilidad de Church*:* LPO no es decidible.

Esquema de la demostración*:* Puesto que *Q* es finitamente axiomatizable podemos considerar la fórmula $A_Q$ que resulta de poner en conjunción todos y cada uno de sus axiomas. Por la definición de teorema o fórmula

probable en *Q*, si B es un teorema de *Q*, la prueba de tal aserto adoptará la forma del enunciado de primer orden ($A_Q \rightarrow B$). Ahora bien, puesto que las derivaciones de teoremas en *Q* no apelan en ningún momento al significado de sus signos sino tan sólo a la forma de sus axiomas, la fórmula $A_Q \rightarrow B$ constituye un teorema de LPO si B es un teorema de *Q*. A continuación consideramos la función recursiva $\theta(x)$ la cual se caracteriza por satisfacer: $\theta(k)=[A_Q \rightarrow B]$ para $k=[\beta]$. Si el conjunto de teoremas de LPO es decidible, podremos afirmar que su función característica será recursiva. Pero si es así, y puesto que la fórmulas del tipo $A_Q \rightarrow B$ se encuentran entre los axiomas de LPO resultará que el conjunto {$k/\theta(k)$ es el código de un teorema de *Q*} será recursivo y por tanto el conjunto de teoremas de *Q* será decidible. Puesto que *Q* es una extensión –trivial- de *Q*, el lema [12] entra en contradicción con el resultado que se acaba de alcanzar.

En cierto modo no es tan sorprendente que parte de las limitaciones inherentes a una teoría axiomática de la Aritmética como *Q* se filtren a través de su estructura hasta alcanzar su esqueleto de primer orden. Lo que el Teorema [13] parece dejar claro es la porción de responsabilidad que compete a LPO en la demostración del Teorema [11]. Dicho de otro modo, qué porción de ese resultado es imputable al hecho de trabajar con una teoría cuya noción de prueba es, salvo por su contenido concreto, esencialmente de primer orden, la teorematicidad en *Q* sólo admite transformaciones puramente simbólicas de finitas expresiones, *axiomas*, mediante reglas de inferencia clásicas.

Corresponde a continuación ofrecer un ejemplo de lo que hemos denominado más arriba -resultado de tipo ascendente-. Escogemos para ello la teoría más rica en contenido aritmético de las que hemos considerado hasta el momento, la única además que resulta completa –trivialmente- en el sentido de [3.iv], a saber, Th(ù). El hecho de que Th(ù) esté formada por todos los enunciados *verdaderos* de la Teoría de números bajo su modelo estándar hace que el predicado de primer orden caracterizado como

[14] Tr([B]) syss B es un enunciado en $L_C$ verdadero en el modelo estándar,

resulte directamente afectado por el enunciado del Teorema 11. El siguiente teorema, reconocido en sus más diversas versiones bajo el rótulo de Teorema de Tarski, garantiza que la verdad, predicada de los enunciados aritméticos expresables en $L_C$, no resulta una noción más aprehensible que su contrapartida deductiva representada por $Pr_T$.

[15] Teorema de Tarski*:* El predicado Tr no es aritméticamente definible.

> Esquema de la demostración*:* Obsérvese que el conjunto de teoremas de Th(ù) es, por definición, el conjunto de fórmulas cuyos códigos satisfacen el predicado Tr. Si Tr fuera definible en Th(ù), indirectamente estaríamos afirmando que $Pr_N$ lo es a su vez. Pero Th(ù) es una extensión definicionalmente consistente de *Q* y por el Teorema 11 entonces, $Pr_N$ no es definible en Th(ù) y por tanto tampoco Tr.

Muy posiblemente lo más llamativo de este resultado no sea tanto la comparación o enfrentamiento entre verdad y teorematicidad sino su virtud para aclarar sus relaciones. Mientras que trabajamos con subteorías de Th(ù) aún podemos pensar -de forma algo paradójica si se quiere- que la verdad de nuestros enunciados de Teoría de números puede ser determinada de manera *efectiva* apelando a otros expedientes distintos. La equiparación de Tr y $Pr_N$ en Th(ù) informa de que esa otra manera de determinar la extensión de Tr por medios *efectivos* es, exactamente, lo que correspondería al significado formal e intuitivo de $Pr_N$ y por tanto algo matemáticamente irrealizable. En última instancia nos vemos obligados a reconocer que las verdades propias de la Teoría de números no pertenecen a la clase de los procedimientos efectivos que en parte son el objeto de esa teoría.

## *Indecidibilidad*

Un resultado clásico en Teoría de Modelos establece que toda teoría axiomatizable que resulte a su vez completa ha de ser decidible. Basándonos en ello y tomando el Teorema [11] a través del lema [12] como referencia obtenemos el siguiente corolario:

[16] Corolario*:* Toda teoría *T* que extienda a *Q* deja de satisfacer simultáneamente las siguientes propiedades:

i. *T* es consistente,
ii. *T* es axiomatizable, y
iii. *T* es completo.

Esquema de la demostración*:* Puesto que *T* extiende a *Q*, por el lema 12 si *T* es consistente entonces no es decidible y puesto que toda teoría axiomatizable y completa es decidible, debemos concluir que *T* no es a la vez consistente, completa y axiomatizable.

Este resultado, directamente emparentado con el Primer Teorema de Incompletitud de Gödel desarrolla la potencia del Teorema 12 utilizando *Q* para establecer algo similar a lo que sería un principio de indeterminación aplicable en los dominios de la teoría elemental de números. Podemos considerar teorías consistentes y axiomatizables que como *Q* o *AP* dejarán de ser completas, o teorías completas que como Th(ù) no son axiomatizables, pero disponer de todas estas bondades *a la vez* nos expulsa del dominio de las teorías consistentes en las cuales desearíamos ver recogido nuestro conocimiento acerca de la Aritmética.

Vemos pues que las esperanzas depositadas en la Lógica como herramienta de formalización y análisis finalizan con un resultado nada estimulante en una primera lectura. Durante los primeros años de este siglo la capacidad de la Lógica para dominar y

entender una noción tan general como la de *prueba* hizo pensar en la posibilidad de exportar sus métodos a cualquier doctrina informal. El resultado sería entonces una teoría axiomática dotada de una relación de prueba efectiva capaz de reducir fragmentos notables de la investigación a un mero ejercicio deductivo. En el peor de los casos, una teoría axiomática debería permitir un absoluto control sobre propiedades deseables en toda teoría tales como su consistencia. El decisivo avance que la Teoría de la Computación ha proporcionado a la Lógica y los fundamentos de la Matemática ha sido mostrar cómo la presunta neutralidad de la noción formal de prueba respecto a lo que es el lenguaje de la teoría que se intenta formalizar es radicalmente falsa. La capacidad para derivar teoremas a partir de axiomas y la capacidad de un lenguaje formal para expresar los enunciados de una teoría informal no viajan por separado coincidiendo felizmente para alumbrar una teoría axiomática. Por el contrario, vemos que la misma noción de prueba cae, a partir de un cierto punto, bajo el alcance de la potencia expresiva del lenguaje de la teoría que se pretende estudiar haciendo de ella una noción propia de esa teoría. En última instancia, si la noción de prueba es una noción matemática de la cual es posible hablar, antes o después habrá de constituir un objeto propio en una teoría matemática con aspiraciones a convertirse en teoría axiomática. El fragmento de la Aritmética representado por *Q* es la menor teoría en la que ese fenómeno puede ser estudiado extrayendo todas sus conclusiones.

Es posible que estas palabras puedan suponer una forma algo decepcionante de poner fin a la exposición de una de las aventuras intelectuales más intensas y excitantes de nuestro siglo, pero también han sido muchos los pensadores que, animados por el gusto filosófico de las últimas proposiciones que aquí se han comentado, han dejado volar su imaginación proponiendo las conclusiones más extravagantes. Las limitaciones que hemos hallado y de las cuales la incompatibilidad esencial resumida en el Corolario 16 es uno de los mejores ejemplos, pueden ser interpretadas de muchas formas, una de ellas, como un severo indicio de la debilidad de nuestra intuición matemática. Pero también es posible ver en tales limitaciones, y así lo preferimos aquí, la confirmación de nuestra capacidad para combinar en el dominio de la Matemática la *libertad creativa* con el verdadero *progreso* en el conocimiento.

**Orientación bibliográfica.**

La demostración y explicación que figura en **[Kleene, 1952]**, secc. 76 es, por una vez, especialmente clara. Una línea parecida es la que se adopta en **[Alonso, 1996]** , cap. 3, secc.3. También es de gran utilidad **[Boolos y Jeffrey, 1989]** cap. 15.