00365
Rej. 2

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

LOS TEOREMAS DE GÖDEL

T E S I S

QUE PARA OBTENER EL TITULO DE:

M A E S T R I A   E N   M A T E M A T I C A S

PRESENTA

CARLOS TORRES ALCARAZ

México, D. F. 1988.

INDICE

PRESENTACION

No se pueden concebir la lógica y la filosofía matemática de nuestro tiempo sin la figura de Kurt Gödel, como imposible es mencionar a este ilustre matemático sin evocar sus célebres teoremas sobre la incompletud de la Aritmética. La importacia de estos teoremas se aprecia no sólo en el ámbito de las matemáticas, sino en esferas tan distantes domo lo son la literatura o la filosofía de la conciencia.[1] No obstante, al recorrer la vasta literatura sobre el tema llama la atención el hecho de que ningún autor asequible se ocupa por completo de la demostración del segundo de dichos teoremas.[2] El trato que se le da es desigual, y va desde una breve mención al equívoco planteamiento sobre el modo como se le debe demostrar. Tengo la convicción de que algunos autores ignoran en realidad como se demuestra dicho teorema, limitándose a repetir y en ocasiones a tersgiversar lo que han leído o escuchado sobre el tema. Entre otras cosas, este trabajo intenta llenar dicho vacío en la literatura presentando una demostración completa del mismo.

La demostración del segundo teorema de Gödel exige por parte del sistema formal considerado algo más que la simple binumeración de las relaciones recursivas primitivas. Es necesario, además, probar con variables libres las ecuaciones que las definen. Esta exigencia fue un factor decisivo al elegir un sistema formal que conviniese a este propósito: el sistema AR. En éste se dispone de un símbolo para cada función recursiva primitiva y, entre los axiomas, las ecuaciones que las definen. Tal peculiaridad significa un ahorro considerable de trabajo, pese a las complicaciones que induce al aritmetizar la sintaxis.

El trabajo se divide en seis capítulos.

El capítulo I está dedicado a la aritmética recursiva. En él se definen los conceptos de función recursiva y recursiva primitiva, se introducen algunos procedimientos que permiten definir nuevas funciones recursivas y se demuestra que varias operaciones conocidas caen en el ámbito de la recursión.

En el capítulo II se define el sistema formal AR y se derivan algunos teoremas que serán de utilidad más adelante. El énfasis se hace en las operaciones y relaciones aritméticas usuales como la suma, el producto, la divisibilidad o el orden. Por útimo se demuestra que AR tiene la capacidad de expresar numéricamente cada relación recursiva.

---

[1] El impacto de los teoremas en la filosofía no sólo de las matemáticas, sino de la filosofía en general fue enorme. Por ejemplo, J.R. Lucas inicia con estas palabras un polémico ariculo que titula <u>Las mentes, las máquinas y Gödel</u>: *"Tengo la impresión de que el teorema de Gödel demuestra que el mecanisismo es falso, es decir, que las mentes no pueden ser explicadas como las máquinas"*.

[2] Una forma simple de estos teoremas dice: En cualquier sistema formal para la teoría de los números que no sea demasiado restringido suceden dos cosas: (1) Se pueden construir proposiciones aritméticas P que son ciertas mas no derivables dentro del formalismo. (2) El sistema es incapáz de probar su consistencia (o bien, la fórmula C que expresa la consistencia del sistema no es derivable en 41).

En el capítulo III se codifica la sintaxis de AR en la aritmética recursiva a través de una correspondencia específica, y se muestra que nociones tales como las de *prueba* o *axioma* son recursivas primitivas. Se introduce, además, una importante operación de substitución sb(φv,v,t) que, dados los códigos φv, v y t, genera el código φt como resultado.

El capítulo IV está dedicado al primer teorema de incompletud de Gödel. En la demostración del teorema se recurre a la hipótesis especial de que AR es ω-consistente. Como testimonio de que la hipótesis de ω-consistencia se puede reemplazar por la más débil de consistencia simple, a continuación se demuestra la forma de Rosser del teorema de Gödel. Acto seguido se incluye una exposición informal del teorema en la cual se pone de manifiesto su semejanza con la llamada *Paradoja de Richard*. Por último se exponen condiciones generales para que el teorema se aplique a un sistema formal arbitrario y se exploran algunas de sus consecuencias.

En el capítulo V se demuestra el segundo teorema de incompletud de Gödel. Para ello se introducen las llamadas *condiciones de derivación de Hilbert y Bernays* y se demuestra que el sistema AR posee un *predicado de prueba* TEO(x) que las satisface. Hay dos demostraciones del teorema. La primera de ellas se apoya en dos resultados de importancia: el Lema Diagonal y el Teorema de Löb. La segunda demostración se hace con el propósito de exhibir la relación entre el enunciado de Gödel y los enunciados de consistencia. El capítulo termina con una discusión en torno al procedimiento que se sigue en la demostración del segundo teorema.

El capítulo VI está dedicado a la demostración de que el predicado TEO(x) que corresponde a la noción <*x es un teorema de* AR> es en realidad un *predicado de prueba* para AR. Para ello se demuestra que satisface las *condiciones de derivación de Hilbert y Bernays*. Al hacerlo se pone de manifiesto la capacidad que tiene el sistema AR para expresar los conceptos y razonamientos a que da lugar. Con ello se concluye la demostración del segundo teorema de Gödel y también este trabajo.

AGRADECIMIENTOS.— Al doctor Francisco Tomás Pons por la entusiasta acogida que dió a ésto cuando aún era un proyecto y por su ayuda en el desarrollo parcial del mismo. Al maestro Gonzalo Zubieta Russi por haber aceptado la dirección de este trabajo cuando el Dr. Tomás debió ausentarse por tiempo indefinido de nuestro medio académico. A él y al maestro Alejandro Odgers López mi más sincero agradecimiento por la atención que brindaron a la exposición de esta tesis y por sus valiosas críticas y comentarios. A todos ellos mi admiración y respeto por que con su labor y ejemplo engrandecen a nuestra Universidad.

Ciudad Universitaria, a 16 de Febrero de 1988

CAPITULO I

ARITMETICA RECURSIVA

En el año de 1931 Kurt Gödel, entonces un joven matemático de 23 años de edad, publica un novedoso trabajo que viene a revolucionar la Lógica contemporanea y a producir un viraje en la dirección de sus investigaciones. El trabajo lleva por título "Sobre proposiciones formalmente indecidibles en Principia Mathematica y sistemas afines". En él Gödel introduce un procedimiento original que le permite fijar límites a la capacidad de algunos sistemas formales para representar a la teoría que suplantan. Dicho procedimiento se conoce como *método de la aritmetización de la sintaxis*. Consiste, básicamente, en asociar números enteros a los objetos del sistema formal considerado. Con su ayuda es posible formular un extenso número de enunciados y razonamientos metateóricos en la aritmética. Su aplicación práctica descanza en la teoría de las funciones recursivas, por lo que resulta indispensable hacer una breve referencia a éstas.

En la Aritmética Recursiva sólo se utilizan métodos constructivos, especialmente dos: la recursión (que le da su nombre a la teoría) y la inducción. En términos más exactos, la Aritmética Recursiva es la parte de la teoría de los números que se construye con base en:

1) Operaciones lógicas elementales como la negación, la conjunción, la disyunción, la implicación y la cuantificación restringida a dominios finitos.
2) La relación de igualdad y el principio de substitución de iguales por iguales.
3) El principio de inducción finita y métodos equivalentes.
4) Las definiciones recursivas.

La teoría de la división, la del máximo común divisor y la de la descomposición en factores primos (incluyendo el teorema de la unicidad de la descomposición) forman parte de la Aritmética Recursiva. En este capítulo desarrollamos aquellas partes de la teoría que son relevantes para la comprensión de los teoremas de Gödel. No obstante, debemos señalar que esta teoría tiene un valor autónomo que va más allá de la investigación de los sistemas formales. Es, en cierto sentido, el estudio de las funciones efectivamente calculables, los procedimientos de decisión y los algorítmos.

I.1.- Las funciones recursivas

En esta sección desarrollamos una teoría informal acerca de ciertas funciones aritméticas llamadas Recursivas. En esta teoría, al igual que en las investigaciones metamatemáticas que le siguen, utilizamos sólo métodos constructvos o finitos.

La clase de las funciones recursivas surge al precisar el concepto de *función calculable*. Ciertas funciones iniciales —que se aceptan como calculables de inmediato— son llamadas recursivas. Para generar nuevas funciones de esta clase a partir de aquéllas previamente definidas se dispone de tres reglas. Cada una de éstas indica un algoritmo para calcular los valores de la nueva función una vez calculados los valores de las funciones que la definen.

(1) Funciones iniciales

a) La función sucesor $s:\mathbb{N}\longrightarrow\mathbb{N}$ de grado 1.
b) La función constante cero $0:\{\emptyset\}\longrightarrow\mathbb{N}$ de grado 0[3]. Esta función, repetimos, se denota K_{00}.

c) Para cada pareja (n,k) con $1\leq k\leq n$ una función proyección $P_{nk}:\mathbb{N}^n\longrightarrow\mathbb{N}$ definida por la ecuación $P_{nk}(x_1,x_2,\dots,x_n)=x_k$.

(2) Reglas para generar funciones

a) Composición.— Si g es una función de grado $m>0$ y $h_1,\dots,h_m$ son funciones de grado n, entonces la ecuación

$$f(x_1,\dots,x_n)=g(h_1(x_1,\dots,x_n),\dots,h_m(x_1,\dots,x_n))$$

define una función de grado n.

b) Recursión.— Si g es una función de grado n y h es una función de grado n+2, entonces las ecuaciones

$$f(x_1,\dots,x_n,0)=g(x_1,\dots,x_n)$$
$$f(x_1,\dots,x_n,sy)=h(x_1,\dots,x_n,y,f(x_1,\dots,x_n,y))$$

definen una función de grado n+1[4].

c) Minimalización (operador μ).— Si g es una función de grado n+1 con la propiedad de que para cada n números $k_1,\dots,k_n$ hay una k tal que $g(k_1,\dots,k_n,k)=0$, entonces la ecuación

$$f(x_1,\dots,x_n)=\mu y(g(x_1,\dots,x_n,y)=0)$$

define una función de grado n[5]. A μ se le llama OPERADOR MINIMAL.

Una función aritmética es RECURSIVA cuando es inicial o se genera a partir de las funciones iniciales aplicando las reglas de composición,

---

[3] Una función aritmética de grado n es una correspondencia $f:\mathbb{N}^n\longrightarrow\mathbb{N}$. Cuando n=0 el dominio es $\mathbb{N}^0=\{\emptyset\}$. En tal caso la función no es otra cosa que la elección de un elemento de $\mathbb{N}$ con el cual se le identifica. En el caso que nos ocupa la función es $0(\emptyset)=0$, que también se denota K_{00}.

[4] Si n=0, las ecuaciones son de la forma $f(0)=k$, $f(sy)=h(y,f(y))$, con k una constante. Se trata, en este caso, de una definición sin parámetros.

[5] La expresión $\mu y(g(k_1,\dots,k_n,y)=0)$ denota al menor número y que es un cero de la función $h(y)=g(k_1,\dots,k_n,y)$. En otras palabras, $\mu y(g(k_1,\dots,k_n,y)=0)$ es el mínimo del conjunto $\{y\mid g(k_1,\dots,k_n,y)=0\}$.

recursión y/o minimalización. Si en el proceso no se aplica la regla de minimalización, entonces se dice que la función es RECURSIVA PRIMITIVA.

[Una definición alternativa es la siguiente: la clase de las funciones recursivas es la mínima clase que contiene a las funciones iniciales y es cerrada bajo las operaciones de composición, recursión y minimalización. Si en la definición se omite la minimalización, entonces la clase es la de las funciones recursivas primitivas].

Por definición toda función recursiva primitiva es recursiva. Aunque aquí no lo haremos, se puede demostrar que el recíproco de esta proposición es falso.

Ejemplos

A continuación presentamos una lista de funciones recursivas primitivas junto con su definición. De la minimalización nos ocupamos al formalizar la Aritmética Recursiva, aunque este recurso es de poca importancia en nuestro estudio. De hecho, el método de la aritmetización de Gödel sólo hace uso de las funciones recursivas primitivas.

1.– $+(x,0)=P_{11}(x)$ función suma

$+(x,sy)=S(P_{33}(x,y,+(x,y)))$

2.– $s(0)$, $s(s(0))$, $s(s(s(0)))$, ... constantes 1,2,3,...

En el último inciso escribimos 0 en vez de K_{00}. En general cada función constante $K_{nk}(x_1,\dots,x_n)=k$ se denota con la constante misma, aunque esto de lugar a confusiones. Así mismo, en lo que sigue las ecuaciones que definen cada función se escriben en notación ordinaria y sin incurrir en detalles, los cuales debe cubrir el lector. Esto significa que al definir una función recursiva se omite la escritura de algunas funciones iniciales, algunas recursiones y algunas composiciones que en rigor se deben poner.

Por ejemplo, en vez de la escritura utilizada en la definición de la funcion suma, simplemente escribimos $x+0=x$ y $x+sy=s(x+y)$.

3.– $x\cdot 0=0$ función producto

$x\cdot sy=x\cdot y+x$

4.– $K_{1k}(0)=k$ función constante k de grado 1

$K_{1k}(sy)=k$

Las funciones constantes k de grado n>1 se definen inductivamente como sigue: $K_{n+1k}(X,0)=K_{nk}(X)$; $K_{n+1k}(X,sy)=K_{n+1k}(X,y)$.

[Nota.– Como de costumbre, X, Y, Z denotan sucesiones $x_1,\dots,x_n$, $y_1,\dots,y_m$, $z_1,\dots,z_k$ de parámetros. En adelante, $f(X,y)$, $g(Y,z)$ etc. representan expresiones de la forma $f(x_1,\dots,x_n,y)$, $g(y_1,\dots,y_m,z)$ etc. para alguna n, m, y k respectivamente.]

5.– $x^0=1$ función exponencial

$x^{sy}=x^y\cdot x$

6.— $0!=1$
$sx!=x!\cdot x$ factorial de x

7.— $pd(0)=0$
$pd(sx)=x$ predecesor de x

8.— $x\dot{-}0=0$
$x\dot{-}sy=pd(x\dot{-}y)$ diferencia positiva de x con y.
(si $x\geq y$, entonces $x\dot{-}y=x-y$)

9.— $min(x,y)=y\dot{-}(x\dot{-}y)$ menor número del conjunto $\{x,y\}$

Inductivamente se define la función mínimo para un número finito aunque arbitrario de argumentos. Sea $n\geq 1$ y supóngase definida la función $min_{(n+1)}$ de grado n+1. La función $min_{(n+2)}$ se define como sigue:

$min_{(n+2)}(x_1,\ldots,x_{n+1},x_{n+2})= min(min_{(n+1)}(x_1,\ldots,x_{n+1}),x_{n+2})$.

10.— $max(x,y)=x+(y\dot{-}x)$ mayor número del conjunto $\{x,y\}$

En forma análoga al #9, se define la función $max_{(n+2)}$ inductivamente como sigue: $max_{(n+2)}(x_1,\ldots,x_{n+1},x_{n+2})=max(max_{(n+1)}(x_1,\ldots,x_{n+1}),x_{n+2})$.

11.— $sg(0)=0$
$sg(sx)=1$ signo de x. $sg(x)=1 \Leftrightarrow x\neq 0$

12.— $sgc(0)=1$
$sgc(sx)=0$ signo contrario de x. $sgc(x)=0 \Leftrightarrow x\neq 0$

13.— $|x-y|=(x\dot{-}y)+(y\dot{-}x)$ valor absoluto de la diferencia de x con y

Proposición 1.— Si $f(X,y)$ es una función recursiva primitiva, entonces las funciones

$$\sigma_f(X,z)=\sum_{k=0}^{z} f(X,k) \quad y \quad \Pi_f=\prod_{k=0}^{z} f(X,k)$$ son recursivas primitivas[6].

Demostración

$\sigma_f(X,0)=f(X,0)$
$\sigma_f(X,sz)=\sigma_f(X,z)+f(X,sz)$ suma acotada de f

$\Pi_f(X,0)=f(X,0)$
$\Pi_f(X,sz)=\Pi_f(X,z)\cdot f(X,sz)$ producto acotado de f ∎

En el texto se utiliza la notación ordinaria Σf y Πf para estas funciones. El hecho de que la "variable" k no figura en ninguna de sus definiciones nos muestra que la misma es tan sólo aparente.

---

[6]Estas funciones son de grado n+1 al igual que f. Sin embargo, dependen de X y z, mientras que f depende de X y y.

Las funciones $\sum_{k=h}^{x} f(\bar{x},k)$ y $\prod_{k=h}^{x} f(\bar{x},k)$ son recursivas primitivas para cada h>0 que se elija. Sus definiciones son las siguientes:

$$\prod_{k=h}^{x} f(\bar{x},k)=\prod_{j=0}^{x\dot{-}h} f(\bar{x},h+j) \quad ; \quad \sum_{k=h}^{x} f(\bar{x},k)=\sum_{j=0}^{x\dot{-}h} f(\bar{x},h+j).$$

Ambas funciones son de grado n+2, pues dependen de $\bar{x}$, x y h.

I.2.- Relaciones y predicados recursivos

La teoría de las relaciones recursivas no es distinta de la de las funciones recursivas. La reducción de la primera a la segunda se logra a través de un artificio simple: una relación aritmética es *recursiva* si su función característica lo es.

En lo que resta de este capítulo presentamos algunos procedimietos que permiten definir e identificar nuevas funciones recursivas. Esto no incluye a las nociones de *relación decidible* y *relación enumerable* que, aunque centrales en la teoría, no serán consideradas en nuestro estudio.

Definición.- Si $R \subseteq \mathbb{N}^n$, entonces se dice que R es una *relación aritmética de grado* n y, cuando n=1, también que R es un *predicado aritmético*.

Sea R una relación aritmética de grado n y sea $\bar{x}=(x_1,\ldots,x_n)\in\mathbb{N}^n$. Para indicar que $\bar{x}$ es un elemento de R se escribe $R(x_1,\ldots,x_n)$, y para indicar que $\bar{x}$ no es un elemento de R se escribe $\neg R(x_1,\ldots,x_n)$.

Definición.- Sea R una relación aritmética de grado n. La *función característica* de R es la función $C_R:\mathbb{N}^n \longrightarrow \{0,1\}$ determinada por la condición de que para todo $\bar{x}\in\mathbb{N}^n$, $C_R(\bar{x})=0 \Leftrightarrow \bar{x}\in R$.[7]

Definición.- Una relación R es *recursiva* (*recursiva primitiva*) si su función característica C_R es recursiva (*recursiva primitiva*).

Los siguientes son ejemplos de relaciones recursivas primitivas. Como en el caso de las funciones recursivas, las relaciones aritméticas

---

[7] Una definición alternativa de uso frecuente es ésta: Una relación aritmética R es *recursiva* si existe una función recursiva $f_R:\mathbb{N}^n\longrightarrow\mathbb{N}$ tal que $f_R(\bar{x})=0 \Leftrightarrow \bar{x}\in R$. En ocasiones haremos uso de esta definición por ser más cómoda. A f_R le llamamos *función representante* de R. Es facil demostrar que ambas definiciones caracterizan la misma clase de relaciones recursivas: si f_R es una función representante de R, entonces $C_R(\bar{x})=sg(f_R(\bar{x}))$ para todo $\bar{x}\in\mathbb{N}^n$.

se escriben en notación ordinaria. Así, por ejemplo, se escribe $x=y$ en vez de $=(x,y)$ etc.

14.— $x\leq y$ una función representante es $x\dot{-}y$.

15.— $x<y$ una función representante es $sx\dot{-}y$.

16.— $x=y$ la función característica es $C_=(x,y)=sg|x-y|$.

17.— $x|y$ una función representante es $\prod_{k=0}^{y}|xk-y|$.

Sean $R(x_1,\dots,x_n)$ y $S(y_1,\dots,y_m)$ relaciones recursivas. Con $z_1,\dots,z_h$ denotamos una sucesión de variables cuyas n primeras componentes son $x_1,\dots,x_n$ y cuyas últimas m componentes son $y_1,\dots,y_m$. Esto significa que las variables $z_1,\dots,z_h$ estan indexadas de modo que $x_1=z_1,\dots,x_n=z_n$, $y_1=z_{h-m},\dots,y_m=z_h$.[a]

Definición.— Las relaciones $\neg R$, $R\&S$ y $R\vee S$ son las siguentes:

— $\mathfrak{X}\in\neg R$ si y sólo si $\mathfrak{X}\notin R$

— $\mathfrak{Z}\in R\&S$ si y sólo si $\mathfrak{X}\in R$ y $\mathfrak{Y}\in S$

— $\mathfrak{Z}\in R\vee S$ si y sólo si $\mathfrak{X}\in R$ o $\mathfrak{Y}\in S$.

Conforme al uso establecido escrbimos $R(\mathfrak{X})\&S(\mathfrak{Y})$ y $R(\mathfrak{X})\vee S(\mathfrak{Y})$ en vez de $(R\&S)(\mathfrak{Z})$ y $(R\vee S)(\mathfrak{Z})$ respectivamente. El grado de $\neg R$ es n, mientras que el de $R\&S$ y $R\vee S$ es h.[b]

Las relaciones $R\Rightarrow S$ y $R\Leftrightarrow S$ se definen, respectivmente, como $\neg R\vee S$ y $(R\Rightarrow S)\&(S\Rightarrow R)$.

Proposición 2 (cerradura).— Sean $R(\mathfrak{X})$ y $S(\mathfrak{Y})$ relaciones recursivas (recursivas primitivas). En tal caso:

i) $\neg R(\mathfrak{X})$ es recursiva (recursiva primitiva)

ii) $R(\mathfrak{X})\&S(\mathfrak{Y})$ es recursiva (recursiva primitiva)

iii) $R(\mathfrak{X})\vee S(\mathfrak{Y})$ es recursiva (recursiva primitiva).

---

[a] Si $\mathfrak{X}=\{x_1,\dots,x_n\}$ y $\mathfrak{Y}=\{y_1,\dots,y_m\}$, entonces $\{z_1,\dots,z_h\}=\mathfrak{X}\cup\mathfrak{Y}$. Cuando $\mathfrak{X}\cap\mathfrak{Y}\neq\emptyset$, hay al menos una terna de variables x_i,y_k,z_j tales que $x_i=y_k=z_j$. De lo anterior se desprende que h es número comprendido entre max(n,m) y n+m.

[b] Un ejemplo. Las relaciones $x<y$ y $y|z$ son ambas de grado 2. No obstante, la relación $(x<y)\&(y|z)$ es de grado 3, pues el parámetro $\langle y\rangle$ es común.

DEMOSTRACION

Por hipótesis las funciones $C_R(X)$ y $C_S(Y)$ son recursivas (rp)

i) La función característica de $\neg R$ es $\overline{sg}(C_R(X))$

ii) La función característica de R&S es $sg(C_R(X)+C_S(Y))$

iii) La función característica de $R \vee S$ es $C_R(X)\cdot C_S(Y)$ ∎

La proposición 2 asegura que el conjunto de relaciones recursivas (primitivas) es cerrado bajo las operaciones lógicas elementales de negación, conjunción y disyunción. No puede decirse lo mismo de la cuantificación, sea ésta universal o existencial.

Supongase que la función $f(X,z)$ es recursiva. Cuantificando se define la relación $P(X)$ como sigue: $P(X)\equiv\exists z(f(X,z)=0)$. Aunque la función f es calculable para valores arbitrarios de X y z, ello no es suficiente para decidir si $P(X)$ es verdadera o falsa en todos los casos.[10] Por ejemplo, si para una X dada no existe una z tal que $f(X,z)=0$, la falsedad de $P(X)$ no se podrá determinar mediante un cálculo. El problema radica en que la falsedad de $P(X)$ involucra el cálculo de todos los valores del conjunto $\{f(X,z)\,|\,z\in\mathbb{N}\}$ y dicho proceso es infinito. Nuestro ejemplo nos muestra que las relaciones $\exists zR(X,z)$ y $\forall zR(X,z)$ no son necesariamente recursivas aún cuando R lo sea. Esta limitación se subsana parcialmente al restringir la cuantificación a dominios acotados. La siguiente proposición nos indica cómo.

<u>Proposición 3</u>.- Sea $R(X,z)$ una relación recursiva (rp) de grado n+1 y sea $f(Y)$ una función recursiva (rp). En tal caso:

i) $S(X,Y)\equiv\exists z(z\leq f(Y)\ \&\ R(X,z))$ es una relación recusiva (rp) en las variables $\{x_1,\ldots,x_n\}\cup\{y_1,\ldots,y_m\}$.

ii) $T(X,Y)\equiv\forall z(z\leq f(Y)\ \Rightarrow\ R(X,z))$ es una relación recursiva (rp) en las variables $\{x_1,\ldots,x_n\}\cup\{y_1,\ldots,y_m\}$.[11]

DEMOSTRACION

i) $C_S(X,Y)=sg(\prod_{k=0}^{fY}C_R(X.k))$. Esta función se define por substitución y es recursiva (rp) cuando f y C_R lo son.

ii) $C_T(X,Y)=sg(\sum_{k=0}^{fY}C_R(X.k))$. Mismo comentario que en (i). ∎

---

[10]La relación $R(X,z)\equiv f(X,z)=0$ si es recursiva. Su función característica es $C_=(f(X,z),0)$. La no recursividad de $P(X)$ sólo puede tener por causa la cuantificación irrestricta.

[11]El grado de S o T es igual al cardinal de del conjunto $\{x_1,\ldots,x_n\}\cup\{y_1,\ldots,y_m\}$ y es menor que n+m cuando la intersección de los conjuntos es no vacia.

I.3.- Los operadores μ y M acotados y la definición por casos

En esta sección describimos tres formas de definir funciones recursivas a partir de relaciones y funciones recursivas. Las dos primeras tienen como base la aplicación de sendos operadores aritméticos llamados *minimal* (*operador* μ) y *maximal* (*operador* M). La tercera es la *definición por casos*.

Los operadores μ y M transforman relaciones aritméticas en funciones aritméticas. Dicha transformación depende de la relación considerada y de la variable que se liga con él. Del operador μ hay dos formas: la libre y la acotada.

1) FORMA LIBRE.- Sea $\mathsf{R}(\mathbf{X},z)$ una relación aritmética de grado n+1. Con R y el operador μ se define una función de grado n en $\mathbf{X}$ -que se denota $\mu z\mathsf{R}(\mathbf{X},z)$- como sigue:

$$\mu z\mathsf{R}(\mathbf{X},z)=\begin{cases} z_0 & \text{si} \quad \{z\,|\,\mathsf{R}(\mathbf{X},z)\}\neq\emptyset \text{ y } z_0=\min\{z\,|\,\mathsf{R}(\mathbf{X},z)\} \\ 0 & \text{si} \quad \neg\exists z\mathsf{R}(\mathbf{X},z). \end{cases}$$

El operador μ en su forma libre no siempre lleva de relaciones recursivas a funciones recursivas. Como en el caso de la cuantificación existencial, cuando $\neg\exists z\mathsf{R}(\mathbf{X},z)$ es el caso, se está ante un proceso infinito de cálculo para determinar el valor de la función. Es por ello que se introduce el operador μ en su forma acotada.[12]

2) FORMA ACOTADA.- Cuando la relación $\mathsf{R}(\mathbf{X},z)$ es *recursiva* (*rp*) y se acota el dominio de la variable ligada por el operador, la función así definida es *recursiva* (*rp*). En este caso el valor de la función no sólo depende de $\mathbf{X}$ sino de $\mathbf{X}$ y el valor de la cota.

Sea $f(\mathbf{Y})$ una función aritmética. Para cada pareja $(\mathbf{X},\mathbf{Y})$ se define el conjunto RF como sigue:

$$\mathsf{RF}=\{n\in\mathbb{N}\,|\,n\leq f(\mathbf{Y}) \;\&\; \mathsf{R}(\mathbf{X},n)\}$$

<u>Proposición 4</u>.- Si $\mathsf{R}(\mathbf{X},z)$ y $f(\mathbf{Y})$ son recursivas (*rp*), la función

$$g(\mathbf{X},\mathbf{Y})=\begin{cases} \min\mathsf{RF} & \text{si } \mathsf{RF}\neq\emptyset \\ f(\mathbf{Y})+1 & \text{si } \mathsf{RF}=\emptyset \end{cases}$$

es recursiva (*rp*).

Demostración

$$g(\mathbf{X},\mathbf{Y})=\sum_{k=0}^{f\mathbf{Y}}\Big(\prod_{j=0}^{k} C_R(\mathbf{X},j)\Big) \text{ es recursiva } (rp) \text{ en } f \text{ y } C_R \blacksquare$$

El otro operador ya mencionado es el operador *maximal* M. Sean $f(\mathbf{X})$ una función aritmética y $\mathsf{R}(\mathbf{Y},z)$ una relación aritmética. la expresión

---

[12]Cuando para toda $\mathbf{X}$ hay una z tal que $\mathsf{R}(\mathbf{X},z)$ y R es recursiva (*r.p.*) la función $\mu z\mathsf{R}(\mathbf{X},z)$ también es recursiva (*r.p.*): $\mu z\mathsf{R}(\mathbf{X},z)=\mu z(C_R(\mathbf{X},z)=0)$.

$\mathrm{M}z(z\leq f(X)\ \&\ R(Y,z))$ se lee "*la mayor z menor o igual que* $f(X)$ *y tal que* $R(Y,z)$". Con el operador M se define una función en X y Y como sigue:

$$\mathrm{M}z(z\leq f(X)\ \&\ R(Y,z))=f(X)\dot{-}\sum_{i=0}^{fx}(\prod_{j=0}^{i}C_R(Y,f(X)\dot{-}j))$$

Es claro que si f y R son recursivas (rp), la función recién definida también lo es.

Las siguientes son algunas funciones aritméticas definidas con estos operadores.

18.– a) $mcm(x,y)=\mu z(1\leq z\leq xy\ \&\ x|z\ \&\ y|z)$ mínimo común multiplo y
b) $mcd(x,y)=\mathrm{M}z(z\leq x\ \&\ z|x\ \&\ z|y)$ máximo común divisor.

19.– a) $q(x,y)=\mathrm{M}z(z\leq x\ \&\ yz\leq x)$ cociente y residuo de
b) $r(x,y)=x\dot{-}q(x,y)\cdot y$ dividir x por y.

La tercera forma de definir funciones recursivas es procediendo por casos. En la proposición siguiente se indica cómo.

Proposición 5.– Sean $R_1(X),\dots,R_k(X)$ relaciones recursivas (rp) ajenas entre sí[18] y sean $g_1(X),\dots,g_k(X)$, $h(X)$ funciones recursivas (rp). La función f definida por las ecuaciones

$f(X)=g_1(X)\dots\dots$ si $R_1(X)$

$f(X)=g_2(X)\dots\dots$ si $R_2(X)$

.

.

$f(X)=g_k(X)\dots\dots$ si $R_k(X)$

$f(X)=h(X)\dots\dots$ en el caso restante

es recursiva (rp).

Demostración

$$f(X)=\sum_{i=1}^{k}(g_i(X)\cdot sgc(C_{R_i}(X)))+(\prod_{i=1}^{k}C_{R_i}(X))\cdot h(X)\ \blacksquare$$

I.4.– Descomposición en factores primos y definición por curso de valores

Al definir una función por recursión puede ocurrir que el valor de $f(X,sy)$ dependa no sólo de $f(X,y)$ sino de algunos o todos los valores $f(X,0)$, $f(X,1),\dots,f(X,y)$ que le preceden. A una definición de este tipo se le llama *recursión por curso de valores*. En esta sección demostramos que algunas funciones definidas por curso de valores son recursivas. Al hacerlo nos apoyamos en el Teorema Fundamental de la Aritmética: todo número natural mayor que la unidad es igual a un producto de factores primos que es único salvo el orden de dichos factores. Aunque no demostramos el teorema, si establecemos la recursividad de las diversas

---

[18] es decir, si $i,j\leq k$ y $j\neq i$, entonces $R_i\cap R_j=\emptyset$

nociones que en él figuran. En adelante las proposiciones 1-4 se aplican repetidas veces sin hacer mención explícita de ello.

Denotamos a las relaciones y a los predicados aritméticos con letras mayúsculas, mientras que a las funciones aritméticas las denotamos con letras minúsculas.

20.- PRIMO(0) es falso

$PRIMO(sx) \equiv \forall y(y \leq x \ \& \ y|sx \Rightarrow y=1)$.[14]

21.- $p(0)=1$

$p(sx)=\mu y(y \leq p(x)!+1 \ \& \ PRIMO(y) \ \& \ p(x)<y)$

Esta función enumera los números primos en orden creciente: $p(1)=2$, $p(2)=3$, $p(3)=5$, $p(4)=7$, $p(5)=11$, etc. En adelante al n-esimo número primo lo denotamos p_n en vez de $p(n)$.

22.- $fp(0,x)=1$

$fp(sy,x)=\mu z(z \leq x \ \& \ PRIMO(z) \ \& \ z|x \ \& \ fp(y,x)<z)$

$fp(n,x)$ enumera los factores primos de x en orden creciente sin repetición, siendo $fp(n,x)$ el n-esmo de ellos. Si x no tiene n factores primos distintos, entonces $fp(n,x)=sx$.

23.- $mpd(x)=My(y \leq x \ \& \ PRIMO(y) \ \& \ y|x)$ Mayor Primo que divide a x

24.- $e(0,x)=0$

$e(sn,x)=My(y \leq x \ \& \ p_{sn}^{y}|x)$ exponente de p_n en la descomposición de x

Esta función también se denota $(x)_n$ (de modo que $e(n,x)=(x)_n$). En el texto se utilizan ambas notaciones indistintamente.

En la siguiente proposición se indica un procedimiento que da lugar, a través de una definición por curso de valores, a una clase especial de funciones recursivas. Dicho procedimiento es un recurso importante en la aritmetización de la sintaxis de diversos sistemas formales como el que presentamos en el capítulo II.

<u>Proposición 8</u>.- Sea f la función definida por curso de valores como sigue:

$$f(\bar{X},0)=k$$

$$f(\bar{X},sy)=\prod_{i=0}^{y}(f(\bar{X},i)+g(\bar{X},i))$$

Se afirma que si g es recursiva (rp), entonces *f* es recursiva (rp).

DEMOSTRACION

Vamos a definir a f por composición a partir de funciones recursivas (rp). Para ello se requiere una función especial Cf que llamamos *función curso de valores para f*. Es la siguiente:

$$Cf=(\bar{X},y)=p_1^{f(\bar{X},0)}\cdot\ldots\cdot p_{sy}^{f(\bar{X},y)} \qquad (*)$$

---

[14] Una definición alternativa es ésta: $PRIMO(x) \equiv \forall y(1<y<x \Rightarrow \neg(y|x))$

Esta función Cf es una especie de archivo en el cual se encuentran registrados los valores sucesivos $f(\mathfrak{X},0),\ldots,f(\mathfrak{X},y)$ (**)

La relación entre f y Cf es obvia: dada la secuencia (**) de la función original se obtiene el valor de Cf a través de la definición (*). Recíprocamente, dado el número $Cf(\mathfrak{X},z)$ se puede calcular el valor de f en $(\mathfrak{X},k)$ para toda $k\leq z$ como sigue:

$$f(\mathfrak{X},k)=e(sk,Cf(\mathfrak{X},z)) \qquad (***)$$

Ahora definimos a Cf por recursión:

$$Cf(\mathfrak{X},0)=2^k$$

$$Cf(\mathfrak{X},sy)=CF(\mathfrak{X},y)\cdot p_{ssy}^{h(\mathfrak{X},y)} \qquad \text{con } h(\mathfrak{X},y)=\prod_{k=0}^{y}(e(sk,Cf(\mathfrak{X},y))+g(\mathfrak{X},k)).$$

Cuando g es recursiva (rp) Cf también lo es. Cabe señalar que en la definición de Cf el valor de $Cf(\mathfrak{X},sy)$ sólo depende de $Cf(\mathfrak{X},y)$. La función f resulta recursiva (rp) al quedar definida por composición a partir de Cf según (***).[15]

Una consecuencia importante de la proposición 8 en relación a los teoremas de Gödel es que si $R(x,y)$ es una relación recursiva (rp) y $P(x)$ es un predicado que satisface

$P(sx)\equiv\exists y(y\leq x \ \& \ R(x,y))$ (no importando si $P(0)$ es falso o verdadero)

entonces $P(x)$ también es recursivo (rp). La función característica de $P(x)$ es

$$C_P(0)=0 \quad (\text{o } C_P(0)=1) \quad ; \quad C_P(sx)=\prod_{k=0}^{x}(C_P(k)+C_R(x,k))$$

La forma de esta definición es la descrita en la proposición 8.

Como complemento de este capítulo se encuentra un apéndice al final del libro sobre *Recursividad y enumerabilidad recursiva.*

---

[15] Las definiciones por curso de valores son inevitables al aritmetizar la sintaxis de diversos sistemas formales. Ello se debe a que en la definición de ciertas nociones se procede de la misma forma, apoyándose en casos anteriores. Vease, por ejemplo, la definición de *fórmula* que se da en el Cálculo de Predicados.

CAPITULO II

FORMALIZACION DE LA ARITMETICA RECURSIVA

En este capítulo presentamos un sistema formal para la aritmética recursiva y estudiamos algunas de sus propiedades. Entre otras cosas demostramos que el sistema es una teoría de primer orden con igualdad y que binumera las relaciones recursivas.

II.1.- Definición del concepto de función recursiva primitiva

La definición de *función recursiva primitiva* que se dió en el capítulo I aunque adecuada para fines prácticos, no es la indicada si lo que se pretende es formalizar este concepto. Para ello es indispensable redefinirlo de un modo más riguroso como en esta sección. La definición que ofrecemos, como se verá, tiene un enorme parecido con la de *teorema* en los sistemas formales.

<u>Definición</u>.- Una función aritmética f se dice que es *recursiva primitiva* si existe una sucesión de funciones aritméticas $f_1, f_2, \ldots, f_n$ tal que:

1) $f = f_n$
2) para cada $i \in \{1, 2, \ldots, n\}$ se cumple alguna de las condiciones siguientes:
   a) f_i es inicial[1]
   b) f_i se define por recursión a partir de f_j y f_k y $j, k < i$.
   c) f_i se define por composición a partir de $f_j, f_{k1}, \ldots, f_{kr}$ y $k, k_1, \ldots, k_r < i$.

A la sucesión $f_1, \ldots, f_n$ se le llama *secuencia de formación de* f.*∎

Para demostrar que una función es recursiva primitiva se requiere exhibir una secuencia de formación de ella o, al menos, saber como se le puede construir. A manera de ejemplo demostramos que algunas de las funciones aritméticas de capítulo anterior son recursivas primitivas aplicando la nueva definición.

---

[1]Recuerdese que las funciones iniciales son las siguientes:
i) La función sucesor $s(x)$ de grado 1.
ii) La función constante cero K_{00} de grado 0.
iii) Para cada (n,k) con $1 \leq k \leq n$, una función proyección P_{nk} de grdo n.
*Nótese que la definición es efectiva en el sentido de que si se nos da una sucesión $f_1, \ldots, f_n$ de funciones aritméticas, siempre será posible decidir si la misma es o no es una secuencia de formación de la última de ellas. Tal cosa dejaría de ser cierta si la definición se extendiese al concepto de función recursiva con la adición de la cláusula siguiente:

d) f_i se define por recursión a partir de f_j y $j < i$.

Esta definición de *función recursiva* no sería efectiva, pues para aseverar que la cláusula (d) es aplicable se requeriría demostrar que $\forall x_1 \ldots \forall x_n \exists z (f_j(x_1, \ldots, x_n, z) = 0)$ es el caso, lo cual no siempre es posible.

#1.— $x+0=x$; $x+sy=s(x+y)$

1.— $s(x_1)$ .... inicial
2.— $P_{11}(x_1)$ .... inicial
3.— $P_{33}(x_1,x_2,x_3)$ .... inicial
4.— $s(P_{33}(x_1,x_2,x_3))$ .... composición 1 y 3

$$\left.\begin{array}{l} 5.-\ +(x_1,0)=P_{11}(x_1) \ \ldots\ldots \\ \quad +(x_1,sx_2)=s(P_{33}(x_1,x_2,+(x_1,x_2))) \ \ldots\ldots \end{array}\right\}\ \text{recursión de 2 y 4}$$

#2.— $x\cdot 0=0$; $x\cdot sy=x\cdot y+x$

Los pasos 1-5 son los mismos que en el #1

6.— K_{00} .... inicial
7.— P_{22} .... inicial

$$\left.\begin{array}{l} 8.-\ K_{10}(0)=K_{00} \ \ldots\ldots \\ \quad K_{10}(sx_1)=P_{22}(x_1,k_{10}(x_1)) \end{array}\right\}\ \text{recursión de 6 y 8}$$

9.— $P_{31}(x_1,x_2,x_3)$ .... inicial

10.— $+(P_{31}(x_1,x_2,x_3),P_{33}(x_1,x_2,x_3))$ .... composición 5,9 con 3

$$\left.\begin{array}{l} 11.-\ \cdot(x_1,0)=K_{10}(x_1) \ \ldots\ldots \\ \quad \cdot(x_1,sx_2)=+(P_{31}(x_1,x_2,\cdot(x_1,x_2)),P_{33}(x_1,x_2,\cdot(x_1,x_2))) \end{array}\right\}\ \text{recursión de 8 y 10}$$

En notación común la sucesión 6-8 se escribe 0, $P_{22}(x_1,x_2)=x_2$, $K_1(x_1)=0$

#3.— $s(0)$, $ss(0)$, etc. constantes 1,2, etc.

1.— $s(x_1)$ .... inicial
2.— K_{00} .... inicial (constante 0)
3.— $s(K_{00})$ .... composición 2 con 1 (constante 1)
4.— $s(s(K_{00}))$ .... composición 3 con 1 (constante 2)
5.— $s(s(s(K_{00})))$ .... composición 4 con 1 (constante 3)
6.— .... etc.

#4.— $K_{1k}(x)=k$ función constante k de grado 1

$$\left.\begin{array}{l} 1.-\ \ldots\ldots \\ \cdot \\ k+3.-\ k \ \ldots\ldots \end{array}\right\}\ \text{constante k. Los pasos del 1 al k+1 tal como se indica en el \#3}$$

k+4.— $P_{22}(x_1,x_2)$ .... inicial

$$\left.\begin{array}{l} k+5.-\ K_{1k}(0)=k \ \ldots\ldots \\ \quad K_{1k}(sx_1)=P_{22}(x_1,K_{1k}(x_1)) \ \ldots\ldots \end{array}\right\}\ \text{recursión de k+1 y k+2}$$

#5.— $x^0=1$; $x^{sy}=x^y\cdot x$ (el lector justificará cada línea)

1.— K_{00}
2.— $s(x_1)$
3.— $s(K_{00})$
4.— $P_{22}(x_1,x_2)$
5.— $K_{11}(0)=s(K_{00})$
$K_{11}(sx_1)=P_{22}(x_1,k_{11}(x_1))$
6.— $P_{31}(x_1,x_2,x_3)$

7.— $P_{33}(x_1, x_2, x_3)$
8.—

12.— $\cdot(x_1, x_2)$

Los mismos pasos que en el #2 salvo los incluidos en esta serie.

13.— $\cdot(P_{31}(x_1, x_2, x_3), P_{33}(x_1, x_2, x_3))$

14.— $exp(x_1, 0) = K_{11}(x_1)$

$$exp(x_1, sx_2) = \cdot(P_{31}(x_1, x_2, exp(x_1, x_2)), P_{33}(x_1, x_2, exp(x_1, x_2)))$$

El lector que esté familiarizado con la nueva definición de función recursiva primitiva no tendrá dificultades para entender el siguiente artificio simbólico. Con su ayuda denotamos a las funciones recursivas primitivas de un modo uniforme. Se trata, como veremos, de una escritura especial para esta clase de funciones.

1) FUNCIONES INICIALES.— Las funciones iniciales se denotan con los símbolos s, K_{00} e I_{nk} (con $1 \leq k \leq n$) respectivamente.[*]

2) OPERADORES PARA LA RECURSION.— Supóngase que las funciones g y h son recursivas primitivas y de grados n y n+2 respectivamente. Hay una función f que se define por recursión a partir de ellas. Para representarla introducimos un operador R_{n+1}. En nuestra notación la función f se escribe

$$[R_{n+1}gh]$$

y su grado es n+1.

3) OPERADORES PARA LA COMPOSICION.— Supóngase que la función g es recursiva primitiva y de grado $n \geq 1$. Supóngase, además, que las funciones $h_1, \ldots, h_n$ son recursivas y de grado k.

Hay una función f que se define componiendo $h_1, \ldots, h_n$ con g. Para representarla introducimos un operador C_{nk}. En nuestra notación la función f se escribe

$$[C_{nk}gh_1 \ldots h_n]$$

y su grado es k.

Ejemplos

Escribimos las sucesiones #1, #2 y #3 en la nueva notación.

##1.— x+0=0 ; x+sy=s(x+y)

1.— s
2.— I_{11}
3.— I_{33}
4.— $[C_{31}sI_{33}]$
5.— $[R_2I_{11}[C_{31}sI_{33}]]$ escritura de la función suma.

---

[*]Para las proyecciones se tienen ahora dos notaciones: P_{nk} e I_{nk}. Estas permiten diferenciar el nivel sintáctico en que se trabaja. La primera de ellas corresponde a la aritmética informal, mientras que la segunda corresponde a la aritmética formalizada. Podría hacerse lo mismo con las funciones cero y sucesor, pero se carece de una simbología adecuada para ello.

##2.— $x \cdot 0 = 0$; $x \cdot sy = x \cdot y + x$

6.— K_{00}
7.— I_{22}
8.— $[R_1 K_{00} I_{22}]$ escritura de la función $K_{10}(x)=0$
9.— I_{31}
10.— $[C_{32}[R_2 I_{11}[C_{31} s I_{33}]] I_{31} I_{33}]$
11.— $[R_2[R_1 K_{00} I_{22}][C_{32}[R_2 I_{11}[C_{31} s I_{33}]] I_{31} I_{33}]]$ escritura de la función $x \cdot y$

##3.— s(0), ss(0), etc.

1.— K_{00}
2.— s
3.— $[C_{01} s K_{00}]$ constante 1 de cero argumentos
4.— $[C_{01} s [C_{01} s K_{00}]]$ constante 2 de cero argumentos
5.— $[C_{01} s [C_{01} s [C_{01} s K_{00}]]]$ constante 3 de cero argumentos
6.— $[C_{01} s [C_{01} s [C_{01} s [C_{01} s K_{00}]]]]$ constante 4 de cero argumentos
....

II.2.— Morfología del sistema AR

Como primer paso en la descripción del sistema AR se define un lenguaje *formal* L_a para la aritmética *recursiva*. En él se incluyen los símbolos y la notación recien expuestos para las funciones recursivas primitivas, con lo cual se tiene una expresión formal para cada una de ellas.

SIMBOLOS.— Los símbolos se agrupan en diversas categorías para mejor entendimiento. Tal división sólo concierne a la metateoría.

<u>conectivos lógicos</u>: $\sim$; $\rightarrow$

<u>signos de puntuación</u>: (;)

<u>signos de relación</u>: =

<u>constantes individuales</u>: c_0

<u>variables individuales</u>: x_0, x_1, x_2, etc

<u>signos funcionales</u>: I_0, s ; para cada pareja (n,k) con $1 \leq k \leq n$ un signo I_{nk}

<u>operadores funcionales</u>: un operador de recursión R
un operador de composición C.[4]

CONSTANTES FUNCIONALES.— No sólo ciertos símbolos individuales denotan funciones. Por el contrario, algunas combinaciones de signos lo hacen.

Cláusula 1.— *Los signos* I_0, I_{nk} (con $1 \leq k \leq n$) *y* s *son constantes funcionales* de grado 0, *n y* 1 respectivamente.

---

[4]Los operadores R_n y C_{nk} (uno para cada $n \in \mathbb{N}$ y cada $k \in \mathbb{N}^+$) al igual que los paréntesis rectangulares "[" y "]" no son necesarios, aunque en ocasiones los utilizaremos por comodidad.

Cláusula 2.- Si g y h son constantes funcionales de grados n y n+2 respectivamente, entonces la expresión Rgh es una *constante funcional* de grado n+1.
Cláusula 3.- Si g es una constante funcional de grado *n* y $h_1,\ldots,h_n$ son constantes funcionales de grado *k*, entonces la expresión $Cgh_1\ldots h_n$ es una *constante funcional* de grado *k*.[5]

Cláusula 4.- Una expresión es una constante funcional si y sólo si se demuestra que lo es a partir de las cláusulas 1,2 y 3 precedntes.

TERMINOS

Cláusula 1.- El símbolo c_0 es un *término*.

Cláusula 2.- Toda variable individual es un *término*.

Cláusula 3.- Si $t_1,\ldots,t_n$ son términos y *f* es una constante funcional de grado n, entonces la expresión $ft_1\ldots t_n$ es un *término*.[6]

Cláusula 4.- Una expresión es un *término* si y sólo si se demuestra que lo es a partir de las clúsulas 1,2,y 3 precedentes.

FORMULAS

Cláusula 1.- Si r y t son términos, entonces la expresión (r=t) es una *fórmula*.[7]

Cláusula 2.- Si A y B son fórmulas y x es una variable individual, entonces:

a) la expresión (A→B) es una *fórmula*.
b) la expresión ~A es una *fórmula*.
c) la expresión (x)A es una *fórmula*.

Cláusula 3.- Una expresión es una *fórmula* si y sólo si se demuestra que lo es a partir de las clúsulas 1 y 2 precedentes.

II.3.- Notación y abreviaturas

Se utiliza el signo "$\rightsquigarrow$" para introducir abreviaturas. "a$\rightsquigarrow$b" se lee <la expresión "a" es una abreviatura de la expresión "b">.

Toda abreviatura se puede remover. Basta escribir en su lugar la expresión abreviada por ella.

1) $f(t_1\ldots t_n) \rightsquigarrow ft_1\ldots t_n$; $f(t_1,\ldots,t_n) \rightsquigarrow f(t_1\ldots t_n)$
2) $0 \rightsquigarrow c_0$

---

[5] Las expresiones de la forma $[R_{mn}gh]$ y $[C_{nk}gh_1\ldots h_k]$ deben entenderse como representaciones metamatemáticas de ciertas combinaciones de signos. Su propósito es hacer inteligibles las expresiones consideradas.
[6] Si n=0, la expresión considerada es simplemente f.
[7] A las fórmulas de esta clase se les llama *fórmulas atómicas*.

3) Sea $k \in \mathbb{N}$. $\overline{k} \rightsquigarrow \overset{k \text{ veces}}{s s \ldots s} 0$

A $\overline{k}$ se le llama *numeral* de k. Los numerales son expresiónes ideadas para representar números naturales en el sistema. Los siguientes son algunos ejemplos: $\overline{0} \rightsquigarrow 0$, $\overline{1} \rightsquigarrow s0$, $\overline{2} \rightsquigarrow ss0$, $\overline{3} \rightsquigarrow sss0$.

4) $A \rightarrow B \rightsquigarrow (A \rightarrow B)$
5) $A \vee B \rightsquigarrow \sim A \rightarrow B$
6) $A \wedge B \rightsquigarrow \sim(A \rightarrow \sim B)$
7) $A \leftrightarrow B \rightsquigarrow (A \rightarrow B) \wedge (B \rightarrow A)$
8) $\exists x A \rightsquigarrow \sim(x) \sim A$
9) $r=t \rightsquigarrow (r=t)$
10) $r \neq t \rightsquigarrow \sim(r=t)$
11) $[R_{n+1} f g] \rightsquigarrow Rfg$
12) $[C_{nk} g h_1 \ldots h_k] \rightsquigarrow C g h_1 \ldots h_k$
13) $r+t \rightsquigarrow [R_2 I_{11} [C_{31} s I_{33}]](r,t)$
14) $r \cdot t \rightsquigarrow [R_2 [R_1 I_0 I_{22}] [C_{32} [R_2 I_{11} [C_{31} s I_{33}]] I_{31} I_{33}]](r,t)$

Al igual que con la suma y el producto, convenimos en abreviar algunas funciones recursivas mediante la escritura que nos es familiar. En cada caso se supone que el lector dispone de los medios para remover la abreviatura en cuestión. Por ejemplo, escribimos $x!$, x^y, $x \dot{-} y$, $|x-y|$, p_x etc. en vez de la expresión formal que denota a la función. Aunque esta notación carece de uniformidad, es mas clara al entendimiento.

15) $r \leq t \rightsquigarrow \exists x(r+x=t)$
16) $r<t \rightsquigarrow \exists x(r+t=x \wedge x \neq 0)$
17) $r \geq t \rightsquigarrow t \leq r$
18) $r>t \rightsquigarrow t<r$

Sea A una fórmula, x una variable y t un término. La expresión "$A(x/t)$" denota a la fórmula que se obtiene al reemplazar en A <u>todas</u> las ocurencias libres de x por t. Cuando el contexto lo permite se escribe $A(t)$ en vez de $A(x/t)$.

La fórmula A también se denota $A(x,x)$.
Si z es una variable individual, $A(x,z)$ denota una de las fórmulas que se obtienen al reemplazar en $A(x,x)$ <u>algunas</u> ocurrencias libres de x para las cuales z es libre, por z. Cabe señalar que en $A(x,z)$ puede haber ocurrencias libres de x, pues la substitución no es forzosa en caso alguno. Varias son las fórmulas que se pueden obtener de este modo. En cada situación $A(x,z)$ representa alguna de ellas.

II.4.- Axiomática del sistema $\mathcal{AR}$

AXIOMAS.- El sistema $\mathcal{AR}$ tiene 14 grupos de axiomas. Uno de ellos consta de una sóla fórmula, mientras que los trece restantes están formados cada uno de ellos por una infinidad de fórmulas. Estos se describen de un modo esqumático con la ayuda de variables sintácticas que no pertenecen al lenguaje formal sino al metalenguaje. Dichas variables se dividen en cuatro clases:

Las variables sintácticas A, B y C denotan fórmulas de L_a.
Las variables sintácticas x, y, z y v_i (con $i \in \mathbb{N}$) denotan variables individuales de L_a.

Las variables sintácticas r y t denotan términos de L_a.
Las variables sintácticas g, h y h_i (con $i \in N$) denotan constantes funcionales de L_a.

Las siguientes fórmulas son los axiomas de AR:

(G_1) $A \to (B \to A)$

(G_2) $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

(G_3) $(\sim A \to \sim B) \to ((\sim A \to B) \to A)$

(G_4) $(x)A(x) \to A(t)$ con t libre para x en $A(x)$

(G_5) $(x)(A \to B) \to (A \to (x)B)$ x una variable que no ocurre libre en A

(G_6) $x=x$

(G_7) $x=y \to (A(x, x) \to A(x, y))$

(G_8) $I_0=0$

(G_9) $\sim(sx=0)$

(G_{10}) $sx=sy \to x=y$

(G_{11}) $I_{nk}(v_1 \ldots v_k \ldots v_n)=v_k$ con $1 \leq k \leq n$

(G_{12}) $Rgh(v_1 \ldots v_n, 0)=g(v_1 \ldots v_n)$

(G_{13}) $Rgh(v_1 \ldots v_n, sv_0)=h(v_1 \ldots v_n, v_0, Rgh(v_1 \ldots v_n, v_0))$

(G_{14}) $Cgh_1 \ldots h_n(v_1 \ldots v_k)=g(h_1(v_1 \ldots v_k) \ldots h_n(v_1 \ldots v_k))$

En G_{12} y G_{13} g es una constante funcional de grado n y h es una constante funcional de grado $n+2$. Cuando $n=0$, $g(v_1 \ldots v_n)$ es g. En G_{14} g es una constante funcional de grado $n \geq 1$ y $h_1, \ldots, h_n$ son constantes funcionales de grado k. Cuando $k=0$, $h_i(v_1 \ldots v_k)$ es h_i para cada $i \leq n$.

Hemos agrupado los axiomas de AR en catorce clases de acuerdo a su forma. El conjunto de axiomas de AR es por definición $G_1 \cup \ldots \cup G_{14}$.

REGLAS DE INFERENCIA.— Toda regla de inferencia es una relación entre fórmulas. Sin embargo cuando se les describe de ese modo se obscurece su caracter operativo. En perjuicio del rigor enunciamos las reglas de inferencia de AR en forma esquemática. Nos valemos para ello de las variables sintácticas utilizadas en la descripción de los axiomas.

Las reglas de inferencia del sistema AR son las siguientes:

(MP) $\dfrac{A, \ A \to B}{B}$ (GEN) $\dfrac{A}{(x)A}$ (PI) $\dfrac{A(0), \ A(x) \to A(sx)}{A(x)}$

La tercera regla de inferencia —PI— corresponde a un modo específico de razonamiento y no forma parte de la lógica general. No formaliza del todo al postulado de Peano. Este se enuncia en un lenguaje de segundo orden así:

$$\forall P(P(0) \& \forall x(P(x)\rightarrow P(sx))\rightarrow \forall xP(x))$$

en este enunciado la variable "P" es una variable predicativa de segundo orden. Su utilización permite enunciar la propiedad inductiva para todos los subconjuntos del dominio de interpretación. Cuando el dominio es $\mathbb{N}$ se trata de $2^{\aleph_0}$ subconjuntos. Sin embargo, la cuantificación "PARA TODO SUBCONJUNTO DE ..." no se puede hacer en un lenguaje de primer orden. Por ello es que es necesario afirmar PARA CADA CONJUNTO DEFINIBLE EN L_a que éste cumple la propiedad inductiva. Pero en L_a sólo hay un número numerable de fórmulas, mientras que $\mathbb{N}$ tiene un número no numerable de subconjuntos. Se sigue de lo anterior que no todo subconjunto de $\mathbb{N}$ es definible en L_a y que la regla PI no corresponde por completo al principio de inducción. Es, de hecho, una forma debil de éste.

Por otra parte, la regla PI se puede eliminar en favor del grupo de axiomas

$$(G_{15})\ (A(0)\wedge(A(x)\rightarrow A(sx)))\rightarrow A(x)$$

No obstante, dicho cambio es irrelevante en la medida en que con él se genera la misma clase de teoremas.

PRUEBAS, DEDUCCIONES Y TEOREMAS.— Las definiciones de estos tres conceptos son las usuales. Hacemos notar que en las deducciones no se permite generalizar aquellas variables que ocurren libres en alguna de las hipótesis.

Para indicar que A es un teorema de AR se escribe $\vdash A$. En rigor se debe escribir $\vdash_{ar} A$, mas las circunstancias permiten omitir la referencia al sistema.

II.5.— Observaciones y comentarios relativos al sistema

Los grupos de axiomas $G_1,\ldots,G_5$ junto con las reglas de inferencia MP y GEN constituyen un cálculo de predicados para L_a. En consecuencia, las siguientes proposiciones son válidas respecto a AR:

(1) Teorema de completud de Gödel

Si $\Gamma\models A$, entonces $\Gamma\vdash A$

En particular si $\Gamma=\emptyset$, la proposición establece que toda fórmula universalmente válida es teorema de AR: Si $\models A$, entonces $\vdash A$.

(2) Metateorema de la deducción

Si $\Gamma, A\vdash B$, entonces $\Gamma\vdash A\rightarrow B$

(3) Regla E

Si B no contiene libre a x, $\Gamma\vdash\exists xA(x)$ y $\Gamma, A(x)\vdash B$, entonces $\Gamma\vdash B$

En los tres casos Γ reprsenta un conjunto de fórmulas de L_a.

Tanto la regla E como el metateorema de la deducción permiten demostrar (en la metateoría) que una fórmula es deducible de un conjunto (quizá vacío) de hipótesis sin tener que mostrar una deducción de ella.

Mostramos a través de un ejemplo la utilización práctica de la regla E. Demostramos que $(x)A(x),\ \exists x(A(x)\rightarrow B(x)) \vdash \exists xB(x)$.

1.- $(x)A(x)$	hipótesis
2.- $\exists x(A(x)\rightarrow B(x))$	hipótesis
3.- $(x)A(x)\rightarrow A(x)$	axioma
4.- $A(x)$	MP 1,3
5.- $A(x)\rightarrow B(x)$	REGLA E a 2
6.- $B(x)$	MP 4,5
7.- $\exists xB(x)$	$(\exists)$ a 6.

La regla $(\exists)$ que se aplica para deducir la linea 7 se explica más adelante. La sucesión 1-7 no satisface la definición de PRUEBA o DEDUCCION. El renglón 5 se justifica a través de la regla E. Se obtiene quitando el cuantificador existencial a la fórmula de la linea 2, con lo cual se tiene una hipótesis adicional. El procedimiento se enmarca en las hipótesis de la proposición que llamamos REGLA E. En la práctica la regla E se aplica "derivando" de una fórmula $\exists xA(x)$ la fórmula $A(x)$, la cual se incluye en la sucesión y se usa para inferir otras fórmulas. Al aplicar la regla E no se tiene una deducción efectiva sino el bosquejo de una deducción.

Otro procedimiento válido en el sistema AR es el de substitución de fórmulas por sus equivalentes. Esto también se fundamenta en el hecho de que los axiomas $G_1,\ldots,G_5$ junto con las reglas MP y GEN dan lugar aun cálculo de predicados. El procedimiento es el siguiente:

(4) Substitución de equivalentes

Si $\vdash A[B,B]$ y $\models B\leftrightarrow B'$, entonces $\vdash A[B,B']$

$A[B,B']$ representa una fórmula que se obtiene al reemplazar en A cero o más ocurrencias de B por B'.

Por último queremos señalar que los grupos de axiomas $G_1,\ldots,G_7$ junto con las reglas MP y GEN permiten derivar algunos principios de la igualdad cuya validez se acepta, sin más, en la matemática usual. Tales principios son los siguientes:

1) Todo objeto es igual a sí mismo.
2) Dos cosas iguales entre sí tienen las mismas propiedades.
3) Si x es igual a z, entonces z es igual a x.
4) Cosas iguales a una tercera son iguales entre sí.

Al principio (1) se le llama LEY REFLEXIVA de la igualdad.
Al principio (2) se le llama LEY DE LEIBNIZ.

Los grupos de axiomas G_6 y G_7 corresponden a los principios (1) y (2) respectivamente.

A Los principios (3) y (4) se les llama LEYES DE SIMETRIA y TRANSITIVIDAD. Todas las fórmulas de L_a que les corresponden son teoremas de AR:

1) $\vdash x=x$	(reflexividad)
2) $\vdash x=y \rightarrow (A(x,x) \rightarrow A(x,y))$	(ley de Leibniz)
3) $\vdash x=y \rightarrow y=x$	(simetría)
4) $\vdash x=y \rightarrow (y=z \rightarrow x=z)$	(transitividad)

La demostración de que tales fórmulas son en efecto teoremas de AR se dará más adelante. Por el momento sólo nos resta señalar que cuando una teoría satisface los incisos (1)-(4) precedentes se dice de ella que es una *teoría de primer orden con igualdad*.

II.6.- Deducción formal e inferncias metateóricas

Es en la metateoría del sistema donde se demuestra que ciertas fórmulas son teoremas de AR. En general la demostración consiste en inferir que hay una prueba para cada una de ellas, lo que no es igual a mostrar o exhibir dicha prueba. La certeza de su existencia tiene como origen el modo como se argumenta en la metateoría. Un procedimiento de uso común es el de *bosquejar* la prueba de cada una de las fórmulas de cierta clase. En ocasiones el argumento se completa con inferencias metateóricas que se apoyan en el conocimiento que se tiene del sistema. Ejemplo de ello son las inferencias basadas en el metateorema de la deducción: si se sabe que $\Gamma, A \vdash B$, se infiere en el metalenguaje que $\Gamma \vdash A \rightarrow B$. En tal caso la deducción formal de la fórmula $A \rightarrow B$ no se muestra: sólo se asegura su existencia. La forma de esta inferencia se representa a través de un diagrama como sigue:

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \qquad \text{(MTD)}$$

En general se indica con una doble raya el que una inferencia se lleva a cabo en el metalenguaje. Obsérvese que esta escritura sólo aparece asociada al signo "$\vdash$" de deducción. La forma general de estas inferencias es la siguiente:

$$\frac{\begin{array}{c}\Gamma_1 \vdash A_1 \\ \Gamma_2 \vdash A_2 \\ \vdots \\ \Gamma_n \vdash A_n\end{array}}{\Gamma \vdash A}$$

La interpretción del esquema es ésta: de las hipótesis $\Gamma_1 \vdash A_1$, $\Gamma_2 \vdash A_2, \ldots$ y $\Gamma_n \vdash A_n$ se infiere la existencia de una deducción de A a partir de Γ.

Algunos ejemplos son los siguientes:

$$\frac{\vdash A(0) \qquad \vdash A(x) \rightarrow A(sx)}{\vdash A(x)} \text{ (PI)} \qquad \frac{\vdash A \rightarrow B}{\vdash \sim B \rightarrow \sim A} \text{ (contraposición)}$$

$$\frac{A \vdash C, \quad B \vdash C}{A \vee B \vdash C} \text{ (dilema constructivo)} \qquad \frac{\Gamma \vdash \exists x A(x) \qquad \Gamma, A(x) \vdash B}{\Gamma \vdash B} \text{ (regla E)*}$$

$$\frac{A, B \vdash C, \quad A, \sim B \vdash C}{A \vdash C} \text{ (prueba por casos)} \qquad \frac{\vdash A, \quad \vdash B}{\vdash A \wedge B} \text{ (conjunción)}$$

Estos modos de argumentación metateórica guardan un vínculo muy estrecho con algunas reglas de inferencia derivadas de AR. De éstas nos ocupamos en la sección siguiente.

II.7.- Reglas derivadas de inferencia

En el estudio del cálculo de predicados se establecen algunas propiedades de la deducción formal que resultan más faciles de utilizar que la definición directa de *prueba* o *deducción*. Dichas propiedades se presentan en forma de esquemas y se les utiliza para demostrar la existencia de deducciones en el sistema. El procedimiento consiste en exhibir una lista de fórmulas, cada una de las cuales es una hipótesis o es derivable de anteriores aplicando alguno de los esquemas. éstos se aplican igual que las reglas de inferencia. Son, de hecho, *reglas derivadas de inferencia*. Todos tienen la forma $A_1, \ldots, A_n \vdash B$ que también representamos con el diagrama

$$\frac{A_1, \ldots, A_n}{B}$$

Algunas de uso frecuente en este trabajo son las siguientes:

$\dfrac{A(x/t)}{\exists x A(x)}$ (∃) t libre para x en A(x)

$\dfrac{(x)A(x)}{A(t)}$ (ESP) t libre para x en A(x)

$\dfrac{A \rightarrow B, \quad B \rightarrow C}{A \rightarrow C}$ (trans →) $\qquad \dfrac{r \leq s, \quad s \leq t}{r \leq t}$ (trans ≤)

$\dfrac{r = s, \quad s = t}{r = t}$ (trans =) $\qquad \dfrac{r = t, \quad A(r, r)}{A(r, t)}$ (sub =)

---

*En este caso la variable "x" no debe ocurrir libre en B.

$\frac{x=y}{y=x}$ (conm =) $\frac{A,\ B}{A\wedge B}$ (conjunción)

$\frac{A\wedge B}{A}\ ;\ \frac{A\wedge B}{B}$ (separación) $\frac{A\rightarrow(B\rightarrow C)}{B\rightarrow(A\rightarrow C)}$ (intercambio de premisas)

$\frac{A\rightarrow(B\rightarrow C)}{(A\wedge B)\rightarrow C}$ (importación) $\frac{(A\wedge B)\rightarrow C}{A\rightarrow(B\rightarrow C)}$ (exportación)

Cabe aclarar que algunas de las reglas (por ejemplo trans = o sub =) no son de validez general y no podrán utilizarse hasta que no sean demostradas para AR. Las demás se justifican con el cálculo de predicados que nos asegura que toda fórmula de L_a que es tautología o universalmente válida, es teorema de AR.

Es así que las *pruebas y deducciones* se presentan por lo general en forma abreviada. Al hacerlo las fórmulas se escriben en columna. A su derecha se acostumbra escribir un mensaje justificando su inclusión en la lista. Algunos de los mensajes son los siguientes:

$(\exists)$, k	Se aplicó la regla derivada de inferencia $(\exists)$ a la fórmula del reglón k
CL, $k_1 \ldots k_n$	La fórmula es consecuencia lógica de las fórmulas de los renglones $k_1 \ldots k_n$
TAUT; UV	La fórmula es tautología; La fórmula es universalmente válida
L. eq. k	La fórmula es lógicamente equivalente a la fórmula del renglón K
GEN k	La fórmula se infiere aplicando la regla (GEN) a la fórmula del renglón k
MP k_1, k_2	La fórmula se infiere aplicando la regla (MP) a las fórmulas de los renglones k_1 y K_2
PI k_1, k_2	La fórmula se infiere aplicando la regla (PI) a las fórmulas de los renglones k_1 y K_2
TEO N	La fórmula es un teorema tal como se demostró en la proposición N
Ded $k_1 \ldots k_n$ por N	La fórmula se infiere de las proposiciones $k_1 \ldots k_n$ como se demostró en la proposición N
Ax k	La fórmula es un axioma del grupo G_k
trans = k_1, k_2 trans $\rightarrow$ k_1, k_2 trans $\leq$ k_1, k_2 sub = k_1, k_2	La fórmula se infiere aplicando la regla derivada de inferencia trans =, trans $\rightarrow$, trans $\leq$ o sub = a las fórmulas de los renglones k_1 y k_2
conm = k	La fórmula se infiere aplicando la regla derivada de inferencia (conm =) a la fórmula del renglón k
Inst-Ax k	La fórmula es una instancia del esquema axiomático k

Inst-Teo N La fórmula es una instancia del teorema correspondiente a la proposición N.

Las instancias mencionadas el los dos últimos ejemplos se obtienen a través del siguiente procedimiento:

Inst-Ax k		Inst-Teo N	
$A(x)$	axioma k	$A(x)$	Teo N
$(x)A(x)$	GEN	$(x)A(x)$	GEN
$(x)A(x) \rightarrow A(t)$	axioma 4	$(x)A(x) \rightarrow A(t)$	axioma 4
$A(t)$	MP	$A(t)$	MP

En ambos casos t es un término libre para x en A(x).

II.8.- Teoremas relacionados con la igualdad, el orden, la función sucesor, la suma, el producto, la divisibilidad y la inducción matemática

Enumeramos a continuación una lista de proposiciones relativas a los teoremas de AR. El orden en que aparecen corresponde al orden en que se demuestran. Esto significa que para probar un teorema de la lista se pueden usar aquellos que le preceden. De la lista demostramos algunas proposiciones a manera de ejemplo.

[1] $\vdash x=y \rightarrow y=x$

[2] $\vdash x=y \rightarrow (y=z \rightarrow x=z)$

[3] $\vdash x_i=x_k \rightarrow f(x_1 \ldots x_i \ldots x_n)=f(x_1 \ldots x_k \ldots x_n)$

[4] $\vdash r=t \rightarrow sr=st$

[5] $\vdash r=t \rightarrow (A(r,r) \rightarrow A(r,t))$

[6] $\vdash r_o=r_1 \rightarrow t(r_o,r_o)=t(r_o,r_1)$

[7] $\vdash x+\bar{1}=sx$

[8] $\vdash x+(y+z)=(x+y)+z$

[9] $\vdash sx+y=x+sy$

[10] $\vdash 0+x=x$

[11] $\vdash x+y=y+x$

[12] $\vdash y+x=z+x \rightarrow y=z$

[13] $\vdash x=0 \vee \exists y(x=sy)$

[14] $\vdash x \leq x$

[15] $\vdash 0 \leq x$

[16] $\vdash x \leq sx$

[17] $\vdash x \leq y \wedge y \leq z \rightarrow x \leq z$

[18] $\vdash x \leq y \vee sy \leq x$

[19] $\vdash x+y=0 \rightarrow x=0$

[20] $\vdash x \leq y \wedge y \leq x \rightarrow x=y$

[21] $\vdash x \leq sy \rightarrow (x \leq y \vee x=sy)$

[22] $\vdash x\leq 0 \rightarrow x=0$

[23] $\vdash sx\leq y \leftrightarrow x<y$

[24] $\vdash x<sy \rightarrow x\leq y$

[25] $\vdash x<y \rightarrow sx<sy$

[26] $\vdash y\leq x \vee x<y$

[27] a) $\vdash A(\bar{0})\wedge\ldots\wedge A(\bar{k}) \rightarrow (x)(x\leq\bar{k} \rightarrow A(x))$

b) $\vdash (x)(x\leq y \rightarrow A(x))\wedge A(y+\bar{1}) \rightarrow (x)(x\leq y=\bar{1} \rightarrow A(x))$

c) $\vdash (x)(x\leq y \rightarrow A(x))\wedge z\leq y \rightarrow (x)(x\leq z \rightarrow A(x))$

[28] $\vdash A(\bar{k}) \rightarrow (x)(\bar{k}\leq x \rightarrow \exists y(y\leq x\wedge A(y)))$

[29] $\vdash (x)(x\leq y \rightarrow A(x))\wedge(x)(y<x \rightarrow B(x)) \rightarrow (x)(A(x)\vee B(x))$

[30] a) $\vdash (z)(x\leq z\leq y \rightarrow A(z))\wedge A(y+\bar{1}) \rightarrow (z)(x\leq z\leq y+\bar{1} \rightarrow a(z))$

b) $\vdash A(\bar{0})\wedge\ldots\wedge A(\overline{k-1}) \rightarrow (x)(x<\bar{k} \rightarrow A(x))$ con $k\in\mathbb{N}^{+}$

c) $\vdash A(\bar{k})\wedge\ldots\wedge A(\bar{k}+\bar{h}) \rightarrow (x)(\bar{k}\leq x\leq\bar{k}+\bar{h} \rightarrow A(x))$

[31] $\vdash x+y=\bar{1} \rightarrow (x=\bar{1}\vee y=\bar{1})$

[32] $\vdash x+y=x+z \rightarrow y=z$

[33] $\vdash \bar{2}+\bar{1}=\bar{3}$, $\vdash \bar{2}+\bar{2}=\bar{4}$, etc.

[34] $\vdash x\cdot y=y\cdot x$

[35] $\vdash x\cdot(y\cdot z)=(x\cdot y)\cdot z$

[36] $\vdash x\cdot\bar{1}=x$

[37] $\vdash \sim(x=0) \rightarrow (x\cdot y=0 \leftrightarrow y=0)$

[38] $\vdash \sim(x=0)\wedge\sim(y=0) \leftrightarrow \sim(x\cdot y=0)$

[39] $\vdash y=0 \leftrightarrow (x\cdot y=0)$

[40] $\vdash x=0 \rightarrow (y)(x\cdot y=0)$

[41] $\vdash x<y \rightarrow \sim(x=y)$

[42] $\vdash x\cdot y=0 \leftrightarrow (x=0\vee y=0)$

[43] $\vdash x\cdot y=\bar{1} \leftrightarrow (x=\bar{1}\wedge y=\bar{1})$

[44] $\vdash \sim(x=0) \rightarrow (x\cdot y=x\cdot z \rightarrow y=z)$

[45] $\vdash \bar{2}\cdot\bar{1}=\bar{2}$, $\vdash \bar{2}\cdot\bar{2}=\bar{4}$, etc

[46] $\vdash x\cdot\bar{2}=x+x$

[47] $\vdash x\cdot(y+z)=x\cdot y+x\cdot z$

[48] $\vdash \sim(x=0) \rightarrow (x=\bar{1}\vee\exists y(x=ssy))$

[49] $\vdash \sim(x=sx)$

[50] $\vdash x\leq y \rightarrow (y<z \rightarrow x<z)$

[51] $\vdash \sim(\bar{1}\leq x\leq y)\wedge\sim(x\leq\bar{1}) \rightarrow \sim(x\leq y)$

[52] $\vdash \sim(x\leq y)\wedge x\leq z \rightarrow y<x\leq z$

[53] a) $\vdash x<y \leftrightarrow x+z<y+z$

b) $\vdash x\leq y \rightarrow x+z\leq y+z$

[54] $\vdash x\leq y \leftrightarrow (x=y\vee x<y)$

[55] $\vdash x<y\vee x=y\vee y<x$

[56] $\vdash x\leq y\rightarrow z\cdot x\leq z\cdot y$

[57] a) $\vdash x<u\wedge y<w\rightarrow x\cdot y<u\cdot w$

b) $\vdash x\leq u\wedge y\leq w\rightarrow x\cdot y\leq u\cdot w$

c) $\vdash 0<x\leq u\wedge y\leq w\rightarrow x\cdot y<u\cdot w$

d) $\vdash \sim(x=0)\rightarrow(y<z\rightarrow x\cdot y<x\cdot z)$

[58] a) $\vdash x\leq y\rightarrow x\leq sy$

b) $\vdash x<y\rightarrow sx\leq y$

[59] $\vdash \sim(x<x)$

[60] $\vdash x<y\leftrightarrow\sim(y\leq x)$

[61] $\vdash x\leq y\rightarrow(y<z\rightarrow x<z)$

[62] a) $\vdash 0<sx$

b) $\vdash x<sx$

[63] $\vdash \sim(x<0)$

[64] $\vdash x\leq y\vee y\leq x$

[65] a) $\vdash x\leq x+y$

b) $\vdash \sim(y=0)\rightarrow x<x+y$

[66] a) $\vdash x<\bar{1}\rightarrow x=0$

b) $\vdash x\leq\bar{1}\rightarrow(x=0\vee x=\bar{1})$

[67] $\vdash x<y\leftrightarrow(x\leq y\wedge\sim(x=y))$

[68] a) $\vdash \sim(x=0)\rightarrow y\leq y\cdot x$

b) $\vdash \sim(x=0)\leftrightarrow 0<x$

[69] $\vdash 0<x\rightarrow(0<y\rightarrow 0<x\cdot y)$

[70] $\vdash \sim(x=0)\rightarrow(\bar{1}<y\rightarrow x<x\cdot y)$

[71] $\vdash \sim(x=0)\rightarrow(x\cdot y=x\cdot z\rightarrow y=z)$

[72] $\vdash \bar{0}<\bar{1}$, $\vdash \bar{1}<\bar{2}$, etc.

[73] a) $\vdash \sim(x=0)\wedge\sim(y=0)\rightarrow(x\cdot y=z\rightarrow x\leq z\wedge y\leq z)$

b) $\vdash \sim(x=0)\rightarrow(x\cdot y\leq z\rightarrow y\leq z)$

[74] a) $\vdash x+y=z\wedge\sim(x+u=z)\rightarrow\sim(y=u)$

b) $\vdash x\leq y+z\rightarrow(x\leq y\vee y<x\leq x+z)$

[75] $\vdash \sim(y=0)\rightarrow\exists q\exists r(x=y\cdot q+r\wedge r<y)$

[76] a) $\vdash x=\bar{0}\vee\ldots\vee x=\bar{k}\rightarrow x\leq\bar{k}$

b) $\vdash x=\bar{0}\vee\ldots\vee x=\overline{k-1}\rightarrow x<\bar{k}$ con $k\in\mathbb{N}^{+}$

[77] $\vdash x|x$ [p]

[78] $\vdash x|y\rightarrow(y|z\rightarrow x|z)$

---

[p] La expresión $x|y$ es una abreviatura de $\exists z(x\cdot z=y)$.

[79] a) $\vdash x|0$

b) $\vdash \bar{1}|x$

[80] $\vdash x|x\cdot y$

[81] $\vdash 0|x\rightarrow x=0$

[82] $\vdash x|y\wedge y|x\rightarrow x=y$

[83] $\vdash \sim(x=0)\rightarrow(y|x\rightarrow y\leq x)$

[84] $\vdash x|z\leftrightarrow \exists y(y\leq z\wedge x\cdot y=z)$

[85] $\vdash x|y\rightarrow x|y\cdot z$

[86] $\vdash x|y\wedge x|z\rightarrow x|u\cdot y+w\cdot z$

[87] $\vdash \bar{1}<x\rightarrow(x|sy\rightarrow\sim(x|y))$

[88] $\vdash x|\bar{1}\rightarrow x=\bar{1}$

[89] $\vdash x|y\wedge\sim(z|y)\rightarrow\sim(x=z)$

[90] $\vdash x|y\wedge x|sy\rightarrow x=\bar{1}$

[91] $\vdash \bar{1}<x\wedge(y)(\bar{1}<y\wedge y|x\rightarrow x\leq y)\rightarrow(z)(z|x\rightarrow z=\bar{1}\vee z=x)$

[92] $\vdash P(\bar{2})$ [10]

[93] $\vdash P(\bar{3})$

[94] $\vdash \sim P(\bar{4})$

[95] $\vdash \exists x(x<y\wedge x|y\wedge P(x))\rightarrow\sim P(y)$

[96] $\vdash ((x)(x<y\rightarrow A(x))\rightarrow A(y))\rightarrow A(y)$ inducción completa

[97] $\vdash \exists yA(y)\rightarrow\exists y(A(y)\wedge(x)(A(x)\rightarrow y\leq x))$ buen orden

[98] $\vdash (A(y)\rightarrow\exists x(x<y\wedge A(x)))\rightarrow\sim A(y)$ descenso infinito

[99] $\vdash A(\bar{k})\wedge(x)(A(x)\rightarrow A(sx))\rightarrow(x)(\bar{k}\leq x\rightarrow A(x))$.

Ejemplos

[1] $\vdash x=y\rightarrow y=x$

1.- $x=y\rightarrow(x=x\rightarrow y=x)$	Ax 7
2.- $x=x\rightarrow(x=y\rightarrow y=x)$	intercambio de premisas a 1
3.- $x=x$	Ax 6
4.- $x=y\rightarrow y=x$	MP 2,3

[2] $\vdash x=y\rightarrow(y=z\rightarrow x=z)$

1.- $y=z\rightarrow(x=y\rightarrow x=z)$	Ax 7
2.- $x=y\rightarrow(y=z\rightarrow x=z)$	intercambio de premisas a 1

De los axiomas G_6 y G_7 y las proposiciones [1] y [2] se sigue que AR es una teoría de primer orden con igualdad.

---

[10] $P(x)$ es abreviatura de la fórmula $(z)(z|x\rightarrow z=\bar{1}\vee z=x)$.

Las proposiciones [1] y [2] dan lugar a las reglas derivadas de inferencia (conm =) y (Trans =) respectivamente.

[3] Si f es una constante funcional de grado $n\geq 1$ y $1\leq i\leq n$, entonces $\vdash x_i=x_k\rightarrow f(..x_i..)=f(..x_k..)$

1.- $x_i=x_k\rightarrow(f(..x_i..)=f(..x_i..)\rightarrow f(..x_i..)=f(..x_k..))$	Ax 7
2.- $f(..x_i..)=f(..x_i..)\rightarrow(x_i=x_k\rightarrow f(..x_i..)=f(..x_k..))$	int. prem. 1
3.- $f(..x_i..)=f(..x_i..)$	Inst-Ax 6
4.- $x_i=x_k\rightarrow f(..x_i..)=f(..x_k..)$	MP 3,4

De acuerdo a las abreviaturas introducidas, los axiomas G_{12} y G_{13} para la suma se escriben

$$(G_{12},+)\ x+0=I_{11}(x)$$
$$(G_{12},+)\ x+sy=[C_{32}sI_{33}](x,y,x+y)$$

Sin embargo, y con base en los axiomas G_{11} y G_{14}, se prueba en AR que $[C_{32}sI_{33}](x,y,x+y)=s(x+y)$. Debido a ello las fórmulas para la suma se escriben, como es habitual, $t+0=t$ y $r+st=s(r+t)$, de modo que los axiomas G_{12} y G_{13} se abrevian como sigue:

$$(G_{12},+)\ x+0=x$$
$$(G_{13},+)\ x+sy=s(x+y)$$

Un argumento análogo nos muestra que los axiomas G_{12} y G_{13} para la multiplicación se abrevian como sigue:

$$(G_{12},\cdot)\ x\cdot 0=0$$
$$(G_{13},\cdot)\ x\cdot sy=x\cdot y+x$$

En el texto utilizamos estas notaciones más familiares en el entendimiento de que se trata de abreviaturas facilmente eliminables.

[7] $\vdash x+\bar{1}=sx$

1.- $x+sy=s(x+y)$	Ax 13 para +
2.- $(y)(x+sy=s(x+y))$	GEN 1
3.- $(y)(x+sy=s(x+y))\rightarrow(x+s0=s(x+0))$	Ax 4
4.- $x+s0=s(x+0)$	MP 2,3
5.- $x+0=x$	Ax 12 para +
6.- $x+s0=sx$	sub = 4,5
7.- $x+\bar{1}=sx$	abreviatura de 6

[8] $\vdash x+(y+z)=(x+y)+z$

Inducción sobre la variable "z" en AR

$A(0)$: $x+(y+0)=(x+y)+0$

1.- $(x+y)+0=x+y$	Ax 12 para +
2.- $y+0=y$	Ax 12 para +
3.- $(x+y)+0=x+(y+0)$	Sub = 1,2
4.- $x+(y+0)=(x+y)+0$	conm = 3

$A(x) \rightarrow A(sx)$

1.− $x+(y+z)=(x+y)+z$ hip.
2.− $(x+y)+sz=s((x+y)+z)$ Ax 13 para +
3.− $(x+y)+sz=s(x+(y+z))$ sub = 1,2
4.− $s(x+(y+z))=x+s(y+z)$ Ax 13 para +
5.− $s(y+z)=y+sz$ Ax 13 para +
6.− $(x+y)+sz=x+s(y+z)$ sub = 3,4
7.− $(x+y)+sz=x+(y+sz)$ sub = 5,6
8.− $x+(y+sz)=(x+y)+sz$ conm = 7

$$\frac{x+(y+z)=(x+y)+z \vdash x+(y+sz)=(x+y)+sz}{\vdash x+(y+z)=(x+y)+z \rightarrow x+(y+sz)=(x+y)+sz}\ \text{MTD}$$

$$\frac{\vdash x+(y+0)=(x+y)=0}{\vdash x+(y+z)=(x+y)+z}\ \text{PI}$$

[17] $\vdash x\leq y \wedge y\leq z \rightarrow x\leq z$

1.− $x\leq y \wedge y\leq z$ hip
2.− $x\leq y$ separación 1
3.− $y\leq z$ separación 1
4.− $\exists u(x+u=y)$ de 2, que es su abreviatura
5.− $\exists v(y+v=z)$ de 3, que es su abreviatura
6.− $x+u=y$ Regla E a 4
7.− $y+v=z$ Regla E a 5
8.− $(x+u)+v=z$ sub = 6,7
9.− $(x+u)+v=x+(u+v)$ Teo [8]
10.− $x+(u+v)=z$ sub = 8,9
11.− $\exists w(x+w=z)$ $(\exists)$ a 10
12.− $x\leq z$ abreviatura de 11

$$\frac{x\leq y \wedge y\leq z \vdash x\leq z}{\vdash x\leq y \wedge y\leq z \rightarrow x\leq z}\ \text{MTD}$$

Con la proposición [17] se justifica la regla derivada de inferencia Trans $\leq$.

[18] $\vdash x\leq y \vee sy\leq x$

Inducción en AR sobre la variable "x".

A(0): $0\leq y \vee sy\leq 0$

1.− $0\leq y$ Teo [15]
2.− $0\leq y \vee sy\leq 0$ CL 1: $A/A\vee B$

La prueba del paso inductivo se hace por casos. Curiosamente, en uno de ellos se procede a su vez por casos.

CASO 1.− $sy\leq x \vdash sx\leq y \vee sy\leq sx$

1.− $sy\leq x$ hip.
2.− $x\leq sx$ Teo [16]

3.— $sy\leq sx$	Trans $\leq$ 1,2
4.— $sx\leq y\vee sy\leq sx$	CL 3: $A/A\vee B$

<u>CASO 2</u>.— $x\leq y\vdash sx\leq y\vee sy\leq sx$

<u>subcaso-2.1</u>.— $x\leq y, z=0\vdash sx\leq y\vee sy\leq sx$

1.— $x\leq y$	hip.
2.— $z=0$	hip.
3.— $\exists z(x+z=y)$	quitando la abreviatura 1
4.— $x+z=y$	Regla E a 3
5.— $x+0=y$	sub = 2,4
6.— $x+0=x$	Ax 12
7.— $x=y$	sub = 5,6
8.— $x=y\rightarrow sx=sy$	teo [3]
9.— $sx=sy$	MP 7,8
10.— $sy+0=sy$	Inst-Ax 13
11.— $sx=sy+0$	sub = 9,10
12.— $sy+0=sx$	conm = 11
13.— $\exists z(sy+z=sx)$	($\exists$) a 12
14.— $sy\leq sx$	abrviatura de 13
15.— $sx\leq y\vee sy\leq sx$	CL 14: $A/B\vee A$

<u>subcaso 2.2</u>.— $x\leq y, \sim(z=0)\vdash sx\leq y\vee sy\leq sx$

1.— $x\leq y$	hip.
2.— $\sim(z=0)$	hip
3.— $\exists z(x+z=y)$	quitando la abreviatura 1
4.— $x+z=y$	regla E a 3
5.— $\sim(z=0)\rightarrow\exists w(z=sw)$	teo [13]
6.— $\exists w(z=sw)$	MP 2,5
7.— $z=sw$	regla E 6
8.— $x+sw=y$	sub = 4,7
9.— $x+sw=s(x+w)$	Ax 13
10.— $x+w=w+x$	Teo [11]
11.— $s(x+w)=y$	sub = 8,9
12.— $s(w+x)=y$	sub = 10,11
13.— $s(w+x)=w+sx$	Ax 13
14.— $w+sx=y$	sub = 12,13
15.— $sx+w=w+sx$	Teo [11]
16.— $sx+w=y$	sub = 14,15
17.— $\exists w(sx+w=y)$	($\exists$) 16
18.— $sx\leq y$	abreviatura de 16
19.— $sx\leq y\vee sy\leq sx$	CL 18: $A/A\vee B$

$x\leq y, z=0\vdash sx\leq y\vee sy\leq sx$	subcaso 2.1
$x\leq y, \sim(z=0)\vdash sx\leq y\vee sy\leq sx$	subcaso 2.2
————————————	(prueba por casos)
$x\leq y\vdash sx\leq y\vee sy\leq sx$	CASO 2
$sy\leq x\vdash sx\leq y\vee sy\leq sx$	CASO 1
————————————	(dilema constructivo)
$x\leq y\vee sy\leq x\vdash sx\leq y\vee sy\leq sx$	
————————————	MTD
$\vdash(x\leq y\vee sy\leq x)\rightarrow(sx\leq y\vee sy\leq sx)$	paso inductivo
$\vdash 0\leq y\vee y\leq 0$	base de la inducción
————————————	PI
$\vdash x\leq y\vee y\leq x$	lcqd.■

[27] a) Si $k \in \mathbb{N}$, entonces $\vdash A(\overline{0}) \wedge \ldots \wedge A(\overline{k}) \rightarrow (x)(x \leq \overline{k} \rightarrow A(x))$

En este caso la demostración se hace por inducción sobre k en la metateoría.

Base de la inducción: k=0

Por demostrar: $\vdash A(\overline{0}) \rightarrow (x)(x \leq \overline{0} \rightarrow A(x))$

1.– $A(\overline{0})$	hip.
2.– $x \leq \overline{0}$	hip.
3.– $x \leq \overline{0} \rightarrow x = \overline{0}$	Teo [22]
4.– $x = \overline{0}$	MP 2,3
5.– $A(x)$	sub = 1;4

$$\cfrac{\cfrac{\cfrac{A(\overline{0}),\ x \leq \overline{0} \vdash A(x)}{A(\overline{0}) \vdash x \leq \overline{0} \rightarrow A(x)}\ \text{MTD}}{A(\overline{0}) \vdash (x)(x \leq \overline{0} \rightarrow A(x))}\ \text{por GEN (x no ocurre libre en la hipótesis)}}{\vdash A(\overline{0}) \rightarrow (x)(x \leq \overline{0} \rightarrow A(x))}\ \text{MTD}$$

Hipótesis de inducción: $\vdash A(\overline{0}) \wedge \ldots \wedge A(\overline{k}) \rightarrow (x)(x \leq \overline{k} \rightarrow A(x))$

Por demostrar: $\vdash A(\overline{0}) \wedge \ldots \wedge A(s\overline{k}) \rightarrow (x)(x \leq s\overline{k} \rightarrow A(x))$ [11]

1.– $A(\overline{0}) \wedge \ldots \wedge A(\overline{k}) \rightarrow (x)(x \leq \overline{k} \rightarrow A(x))$	Teo por hipótesis de inducción
2.– $A(\overline{0}) \wedge \ldots \wedge A(\overline{k}) \wedge A(s\overline{k})$	hip
3.– $A(\overline{0}) \wedge \ldots \wedge A(\overline{k})$	separación a 2
4.– $(x)(x \leq \overline{k} \rightarrow A(x))$	MP 1,3
5.– $(x)(x \leq \overline{k} \rightarrow A(x)) \rightarrow (x \leq \overline{k} \rightarrow A(x))$	Ax 4
6.– $x \leq \overline{k} \rightarrow A(x)$	MP 4,5
7.– $x = s\overline{k} \rightarrow (A(s\overline{k}) \rightarrow A(x))$	Inst-Ax 7
8.– $A(s\overline{k}) \rightarrow (x = s\overline{k} \rightarrow A(x))$	intercambio de premisas a 7
9.– $A(s\overline{k})$	separación a 2
10.– $x = s\overline{k} \rightarrow A(x)$	MP 8,9
11.– $(x \leq \overline{k} \vee x = s\overline{k}) \rightarrow A(x)$	dilema constructivo a 6 y 10
12.– $x \leq s\overline{k} \rightarrow (x \leq \overline{k} \vee x = s\overline{k})$	Inst-Teo [21]
13.– $x \leq s\overline{k} \rightarrow A(x)$	Trans $\rightarrow$ 12,11
14.– $(x)(x \leq s\overline{k} \rightarrow A(x))$	GEN 13

---

[11] Recordemos que $\overline{k+1}$ es por definición $s\overline{k}$. Es por ello que $A(\overline{k+1})$ se escribe $A(s\overline{k})$ y $x \leq \overline{k+1}$ como $x \leq s\overline{k}$.

Argumentando en la metateoría tenemos que

$$\frac{\dfrac{\vdash A(\bar{0})\wedge\ldots\wedge A(\bar{k})\rightarrow(x)(x\leq\bar{k}\rightarrow A(x))}{A(\bar{0})\wedge\ldots\wedge A(s\bar{k})\vdash(x)(x\leq s\bar{k}\rightarrow A(x))}\ \text{(esto lo acabamos de demostrar)}}{\vdash A(\bar{0})\wedge\ldots\wedge A(s\bar{k})\rightarrow(x)(x\leq s\bar{k}\rightarrow A(x))}\ \text{MTD}$$

y por inducción en la metateoría queda demostrada la proposición [27]. ■

II.9.- Semántica: AR y la aritmética recursiva

Todas las proposiciones hasta aquí expuestas describen propiedades sintácticas de AR. Ahora estudiamos algunas de sus propiedades semánticas. Nos ocupamos en particular de la relación existente entre el sistema formal y la Aritmética Recursiva. Con ello se hace intervenir un dominio de objetos —los Números Naturales— que se pueden representar en el sistema y sirven como base para una interpretación del mismo.

Las propiedades semánticas que nos interesan son dos: para las funciones aritméticas la de ser *representibles* y para las relaciones aritméticas la de ser *expresables* en el sistema.

Definición.- Una función $f:\mathbb{N}^n\longrightarrow\mathbb{N}$ es *representable* en AR si y sólo si hay una fórmula $A(x_1,\ldots,x_n,x_{n+1})$ que satisface las siguientes condiciones:

R_1) $VL(A)=\{x_1,\ldots,x_n,x_{n+1}\}$. [12]

R_2) Para todo $(k_1,\ldots,k_n)\in\mathbb{N}^n$:

R_{21}) Si $f(k_1,\ldots,k_n)=k$, entonces $\vdash A(\bar{k}_1,\ldots,\bar{k}_n,\bar{k})$, y

R_{22}) $\vdash\exists_1 x_{n+1}A(\bar{k}_1,\ldots,\bar{k}_n,x_{n+1})$ [13]

Si R_{22} se cambia por

R_{23}) $\vdash\exists_1 x_{n+1}A(x_1,\ldots,x_n,x_{n+1})$

entonces se dice que f es *fuertemente representable* en AR.

definición.- Una relación aritmética $R\subseteq\mathbb{N}^n$ es *expresable* en AR si y sólo si hay una fórmula $A(x_1,\ldots,x_n)$ que satisface las condiciones siguientes:

E_1) $VL(A)=\{x_1,\ldots,x_n\}$

E_2) Para todo $(k_1,\ldots,k_n)\in\mathbb{N}^n$:

E_{21}) Si $(k_1,\ldots,k_n)\in R$, entonces $\vdash A(\bar{k}_1,\ldots,\bar{k}_n)$. y

E_{22}) Si $(k_1,\ldots,k_n)\notin R$, entonces $\vdash\sim A(\bar{k}_1,\ldots,\bar{k}_n)$.

---

[12] Por definición, VL(p) es el conjunto de variables de L_a que ocurren libres en p.

[13] $\exists_1 xA(x)\equiv\exists xA(x)\wedge(x)(y)(A(x)\wedge A(y)\rightarrow x=y)$

Para demostrar que toda función recursiva es fuertemente representable en $\mathbb{AR}$ introducimos dos nociones útiles. La primera de ellas es la de *nivel* de una función recursiva. La segunda es la de *nominación* de una función recursiva primitiva que presentamos a través de un mapeo especial.

NIVEL.– La definición dada de función recursiva primitiva se extiende de un modo natural a las funciones recursivas:

> Una función aritmética f es *recursiva* si y sólo si existe una sucesión de funciones $f_1, \ldots, f_n$ tal que cada una de ellas es inicial o se define a partir de otras, de índice menor al suyo, mediante las reglas de composición, recursión u operador μ no acotado.

Se llama *nivel* de una función recursiva a la longitud de la serie más corta de funciones que es necesaria para definirla. El nivel de una función recursiva f se denota $N(f)$ y es un número natural mayor o igual a 1.

La función constante k_{00}, la función sucesor y Las proyecciones P_{nk} son de nivel 1 o primero. Son, además, las únicas de dicho nivel.

NOMINACION.– Las constantes funcionales de L_a sirven como nombres para las funciones recursivas primitivas. Dicha *nominación* se precisa a través de un mapeo "–" que se define recursivamente de acuerdo al nivel de cada función como sigue:

1) $N(f)=1$ (funciones iniciales)

   1.1) $\overline{K_{00}}=I_0$
   1.2) $\overline{suc}=s$ [14]
   1.3) $\overline{P_{nk}}=I_{nk}$

2) $N(f)>1$ (funciones no iniciales)

   2.1) Si f se define componiendo $h_1, \ldots, h_n$ con g, entonces $\bar{f}=C\bar{g}\bar{h}_1\ldots\bar{h}_n$
   2.2) Si f se define por recursión de g y h, entonces $\bar{f}=R\bar{g}\bar{h}$

Con esto queda definido un mapeo $^{-}: RP \longrightarrow CF$ del conjunto de funciones recursivas primitivas en el conjunto de constantes funcionles. A la constante funcional $\bar{f}$ se le llama *nominación* de f.

<u>Proposición 7</u>.– Si $h,k \in \mathbb{N}$, entonces $\vdash \overline{h \oplus k}=\bar{h}+\bar{k}$. [15]

DEMOSTRACION

Inducción sobre k en la metateoría

---

[14] Llamamos "SUC" a la función en vez de "S" con el fin de no confundir la notación de la aritmética formal con la de la aritmética informal.

[15] El símbolo "⊕" representa a la suma de números naturales en la aritmética informal, mientras que el símbolo "+" es la abreviatura de una constante funcional de $\mathbb{AR}$.

Base de la inducción: $\vdash \overline{h\oplus 0}=\bar{h}+\bar{0}$

1.– $\bar{h}+\bar{0}=\bar{h}$	Inst-Ax 12
2.– $\bar{h}+\bar{0}=\overline{h\oplus 0}$	lo mismo que 1, pues $h\oplus 0=h$
3.– $\overline{h\oplus 0}=\bar{h}=\bar{0}$	conm = 2.

Hipótesis de inducción: $\vdash \overline{h\oplus k}=\bar{h}+\bar{k}$

Por demostrar: $\vdash \overline{h\oplus (k\oplus 1)}=\bar{h}+(\overline{k\oplus 1})$

1.– $\overline{h\oplus k}=\bar{h}+\bar{k}$	Teo por hipótesis de inducción
2.– $\overline{h\oplus k}=\bar{h}+\bar{k}\rightarrow s(\overline{h\oplus k})=s(\bar{h}+\bar{k})$	Ins-Teo [3]
3.– $s(\overline{h\oplus k})=s(\bar{h}+\bar{k})$	MP 1,2
4.– $\bar{h}+s\bar{k}=s(\bar{h}+\bar{k})$	Inst-Ax 13,+
5.– $s(\overline{h\oplus k})=\bar{h}+s\bar{k}$	sub = 3,4
6.– $\overline{h\oplus (k\oplus 1)}=\bar{h}+(\overline{k\oplus 1})$	lo mismo que 5 [16]

<u>Proposición 8.</u>– Si $h,k\in\mathbb{N}$ y $h\neq k$, entonces $\vdash \sim(\bar{h}=\bar{k})$

Demostración

Introducimos la siguiente abreviatura: $s^n o \rightsquigarrow \overbrace{s\ldots\ldots s}^{n\text{ veces}}o$

Suponemos, sin pérdida de generalidad, que $h<k$.

1.– $\bar{h}=\bar{k}$	hip
2.– $s^h o=s^k o$	quitando abreviaturas de 1
3.– $s^h o=s^k o\rightarrow s^{h-1}o=s^{k-1}o$	Inst-Ax 10
4.– $s^{h-1}o=s^{k-1}o$	MP 2,3
....	(se repite el procedimiento h-1 veces)
2h+2.– $o=s^{k-h}o$	MP 2h,2h+1
2h+3.– $\sim(o=s^{k-h}o)$	Inst-Ax 9
2h+4.– $o=s^{k-h}o\wedge\sim(o=s^{k-h}o)$	conjunción 2h+2,2h+3

$\therefore\ \bar{h}=\bar{k}\vdash o=s^{k-h}o\wedge\sim(o=s^{k-h}o)$ (una contradicción)

Por reducción al absurdo en AR, $\vdash\sim(\bar{h}=\bar{k})$. [17]

---

[16] Por definición, $\overline{(k\oplus 1)}=s\bar{k}$. Los renglones 5 y 6 involucran los mismos términos.

[17] Llamase "reducción al absurdo" a la siguiente proposición, válida en el cálculo de predicados: Si $A\vdash B\wedge\sim B$, entonces $\vdash\sim A$.

Proposición 8.- Si f es una función recursiva primitiva de grado n y $k_1,\dots,k_n \in \mathbb{N}$, entonces $\vdash \overline{f(k_1\dots k_n)} = \bar{f}(\bar{k}_1\dots\bar{k}_n)$.

Demostración

Procedemos por inducción sobre $N(f)$ en la metateoría.

Base de la inducción: $N(f)=1$

caso 1.- $f=K_{00}$. Como $gr(K_{00})=0$, la proposición equivale a $\vdash I_0 = I_0$.
caso 2.- $f=suc$. Como $suc(k)=k\oplus 1$, entonces $\overline{suc(k)}=\overline{k\oplus 1}$.

Tenemos la siguiente prueba en AR:

1.- $\overline{suc(k)}=\overline{k\oplus 1}$ Ins-Ax 6 (suc(k) y $k\oplus 1$ son el mismo número)
2.- $\overline{k\oplus 1}=\bar{k}+\bar{1}$ Teo proposición 7
3.- $s\bar{k}=\bar{k}+\bar{1}$ Inst-teo [7]
4.- $\overline{suc(k)}=\bar{k}+\bar{1}$ sub = 1,2
5.- $\overline{suc(k)}=s\bar{k}$ sub = 3,4
6.- $\overline{suc(k)}=\overline{suc}(\bar{k})$ lo mismo que 5: $s=\overline{suc}$

caso 3.- $f=P_{nr}$. Como $P_{nr}(k_1\dots k_n)=k_r$, entonces $\overline{P_{nr}(k_1\dots k_n)}=\bar{k}_r$.

Tenemos la siguiente prueba en AR:

1.- $\overline{P_{nr}(k_1\dots k_n)}=\bar{k}_r$ Inst-Ax 6
2.- $I_{nr}(\bar{k}_1\dots\bar{k}_n)=\bar{k}_r$ Inst-Ax 11
3.- $\overline{P_{nr}(k_1\dots k_n)}=I_{nr}(\bar{k}_1\dots\bar{k}_n)$ sub = 1,2
4.- $\overline{P_{nr}(k_1\dots k_n)}=\bar{P}_{nr}(\bar{k}_1\dots\bar{k}_n)$ lo mismo que 3: $\bar{P}_{nr}=I_{nr}$

Hipótesis de inducción: si $N(f)\le m+1$, entonces $\vdash \overline{f(k_1\dots k_n)}=\bar{f}(\bar{k}_1\dots\bar{k}_n)$
Por demostrar : si $N(f)\le m+2$, entonces $\vdash \overline{f(k_1\dots k_n)}=\bar{f}(\bar{k}_1\dots\bar{k}_n)$

Sea f una función recursiva primitiva de nivel $m+2$.
como $N(f)>1$, f no es inicial y se define por recursión o composición.

caso 1.- f se define por composición de $h_1,\dots,h_j$ con g. En este caso $\bar{f}=[C_{nj}\bar{g}\bar{h}_1 \quad \bar{h}_j]$ y $N(g), N(h_1),\dots,N(h_j)\le m+1$.

Tenemos la siguiente prueba en AR:

1.- $\overline{f(k_1..k_n)}=\overline{g(h_1(k_1..k_n)..h_j(k_1..k_n))}$ Inst-Ax 6
2.- $\overline{g(h_1(k_1..k_n)..h_j(k_1..k_n))}=\bar{g}(\overline{h_1(k_1..k_n)}..\overline{h_j(k_1..k_n)})$ Teo HI.
3.- $\overline{h_1(k_1..k_n)}=\bar{h}_1(\bar{k}_1\dots\bar{k}_n)$ Teo HI.
...
j+2.- $\overline{h_j(k_1..k_n)}=\bar{h}_j(\bar{k}_1..\bar{k}_n)$ Teo HI.

$j+2.-\ \overline{g(h_1(k_1..k_n)..h_j(k_1..k_n))}=\bar{g}(\bar{h}_1(\bar{k}_1..\bar{k}_n)..\overline{h_j(k_1..k_n)})$ sub= 1,2

...

$2j+2.-\ \overline{g(h_1(k_1..k_n)..h_j(k_1..k_n))}=\bar{g}(\bar{h}_1(\bar{k}_1..\bar{k}_n)..\bar{h}_j(\bar{k}_1..\bar{k}_n))$ sub= j+2,2j+3

$2j+3.-\ \bar{f}(\bar{k}_1..\bar{k}_n)=\bar{g}(\bar{h}_1(\bar{k}_1..\bar{k}_n)..\bar{h}_j(\bar{k}_1..\bar{k}_n))$ Inst-Ax 14

$2j+4.-\ \overline{f(k_1..k_n)}=\bar{g}(\bar{h}_1(\bar{k}_1..\bar{k}_n)..\bar{h}_j(\bar{k}_1..\bar{k}_n))$ sub= 1,2j+2

$2j+5.-\ \overline{f(k_1..k_n)}=\bar{f}(\bar{k}_1..\bar{k}_n)$ sub= 2j+3,2j+4

caso 2.— f se define por recursión a partir de g y h. En este caso $gr(g)=n$, $\bar{f}=[R_m\bar{g}\bar{h}]$ y $N(g), N(h)\leq m+1$.

Sean $k_1,\dots,k_m\in\mathbb{N}$. Vamos a demostrar por inducción sobre k_m que $\vdash\overline{f(k_1...k_m)}=\bar{f}(\bar{k}_1...\bar{k}_m)$. A esta segunda inducción le llamamos *inducción anidada* para distinguirla de aquella de la cual forma parte o principal.

Base de la inducción anidada: $k_m=0$.

Por demostrar: $\vdash\overline{f(k_1...k_n,0)}=\bar{f}(\bar{k}_1...\bar{k}_n)$

Tenemos la siguiente prueba en AR:

$1.-\ \overline{f(k_1...k_n,0)}=\overline{g(k_1...k_n)}$ Inst-Ax 5: $f(k_1,\dots,k_n,0)=g(k_1...k_n)$

$2.-\ \overline{g(k_1...k_n)}=\bar{g}(\bar{k}_1...\bar{k}_n)$ teo HI.

$3.-\ \overline{f(k_1...k_n,0)}=\bar{g}(\bar{k}_1...\bar{k}_n)$ sub= 1,2

$4.-\ \bar{f}(\bar{k}_1...\bar{k}_n)=\bar{g}(\bar{k}_1...\bar{k}_n)$ Inst-Ax 12

$5.-\ \overline{f(k_1...k_n,0)}=\bar{f}(\bar{k}_1...\bar{k}_n)$ sub= 3,4

Paso inductivo: $k_m=k\oplus1$

Hipótesis de inducción (anidada): $\vdash\overline{f(k_1...k_n,k)}=\bar{f}(\bar{k}_1...\bar{k}_n,\bar{k})$

Por demostrar: $\vdash\overline{f(k_1...k_n,k\oplus1)}=\bar{f}(\bar{k}_1...\bar{k}_n,\overline{k\oplus1})$

Tenemos la siguiente prueba en AR:

$1.-\ \overline{f(k_1..k_n,k\oplus1)}=\overline{h(k_1..k_n,k,f(k_1..k_n,k))}$ Inst-Ax 6

$2.-\ \overline{h(k_1..k_n,k,f(k_1..k_n,k))}=\bar{h}(\bar{k}_1..\bar{k}_n,\bar{k},\overline{f(k_1..k_n,k)})$ Teo HI.

$3.-\ \overline{f(k_1...k_n,k)}=\bar{f}(\bar{k}_1...\bar{k}_n,\bar{k})$ Teo HI anidada

$4.-\ \overline{h(k_1..k_n,k,f(k_1..k_n,k))}=\bar{h}(\bar{k}_1..\bar{k}_n,\bar{k},\bar{f}(\bar{k}_1...\bar{k}_n,\bar{k}))$ sub = 2,3

$5.-\ \overline{f(k_1..k_n,k\oplus1)}=\bar{h}(\bar{k}_1..\bar{k}_n,\bar{k},\bar{f}(\bar{k}_1...\bar{k}_n,\bar{k}))$ sub = 1,4

$6.-\ \bar{f}(\bar{k}_1...\bar{k}_n,\overline{k\oplus1})=\bar{f}(\bar{k}_1...\bar{k}_n,\overline{k\oplus1})$ Inst-Ax 5

$7.-\ \overline{k\oplus1}=s\bar{k}$ Inst-Ax 6

$8.-\ \bar{f}(\bar{k}_1...\bar{k}_n,\overline{k\oplus1})=\bar{f}(\bar{k}_1...\bar{k}_n,s\bar{k})$ sub = 6,7

$9.-\ \bar{f}(\bar{k}_1...\bar{k}_n,s\bar{k})=\bar{h}(\bar{k}_1..\bar{k}_n,\bar{k},\bar{f}(\bar{k}_1...\bar{k}_n,\bar{k}))$ Inst-Ax 13

$10.-\ \overline{f(k_1..k_n,k\oplus1)}=\bar{f}(\bar{k}_1...\bar{k}_n,s\bar{k})$ sub = 5,9

$11.-\ \overline{f(k_1..k_n,k\oplus1)}=\bar{f}(\bar{k}_1...\bar{k}_n,\overline{k\oplus1})$ sub = 10,8

Y con la inducción anidada concluye también la inducción principal. ∎

Proposición 10.— Si f es una función recursiva primitiva de grado n, entonces la fórmula $\bar{f}(x_1 \ldots x_n)=x_{n+1}$ la representa fuertemente en AR.

Demostración

$R_{1)}$ Sea $f(k_1 \ldots k_n)=k$. Por demostrar: $\vdash \bar{f}(\bar{k}_1 \ldots \bar{k}_n)=\bar{k}$.

Tenemos la siguiente prueba en AR:

1.— $\overline{f(k_1 \ldots k_n)}=\bar{k}$	Inst-Ax 6
2.— $\overline{f(k_1 \ldots k_n)}=\bar{f}(\bar{k}_1 \ldots \bar{k}_n)$	Teo por la proposición 9
3.— $\bar{f}(\bar{k}_1 \ldots \bar{k}_n)=\bar{k}$	sub= 1,2

$R_{2)}$ Por demostrar: $\vdash \exists_1 x_{n+1}(\bar{f}(x_1 \ldots x_n)=x_{n+1})$

Existencia

1.— $\bar{f}(x_1 \ldots x_n)=\bar{f}(x_1 \ldots x_n)$	Inst-Ax 6
2.— $\exists x_{n+1}(\bar{f}(x_1 \ldots x_n)=x_{n+1})$	($\exists$), 1

Unicidad

1.— $\bar{f}(x_1 \ldots x_n)=x \wedge \bar{f}(x_1 \ldots x_n)=y$	hip
2.— $\bar{f}(x_1 \ldots x_n)=x$	separación 1
3.— $\bar{f}(x_1 \ldots x_n)=y$	separación 1
4.— $x=y$	Trans = 2,3

$$\frac{\bar{f}(x_1 \ldots x_n)=x \wedge \bar{f}(x_1 \ldots x_n)=y \vdash x=y}{\vdash (x)(y)\bar{f}(x_1 \ldots x_n)=x \wedge \bar{f}(x_1 \ldots x_n)=y \rightarrow x=y} \quad \text{MTD y GEN dos veces}$$

$$\frac{\vdash \exists x_{n+1}(\bar{f}(x_1 \ldots x_n)=x_{n+1})}{\vdash \exists_1 x_{n+1}(\bar{f}(x_1 \ldots x_n)=x_{n+1})} \quad \text{conjunción}$$

■

Proposición 11.— Sea $g(x_1, \ldots, x_n, y)$ una función aritmética y sea $G(x_1 \ldots x_n, y, z)$ una fórmula que la representa fuertemente en AR. Si $g(k_1 \ldots k_n, k)=a$ y $a \neq b$, entonces $\vdash \sim G(\bar{k}_1 \ldots \bar{k}_n, \bar{k}, \bar{b})$.

Demostración

1.— $G(\bar{k}_1 \ldots \bar{k}_n, \bar{k}, \bar{a})$	Teo
2.— $\exists z G(x_1 \ldots x_{n+1}, z) \wedge (x)(y)(G(x_1 \ldots x_n, x) \wedge G(x_1 \ldots x_{n+1}, y) \rightarrow x=y)$	Teo
3.— $\exists z G(\bar{k}_1 \ldots \bar{k}, z) \wedge (x)(y)(G(\bar{k}_1 \ldots \bar{k}, x) \wedge G(\bar{k}_1 \ldots \bar{k}, y) \rightarrow x=y)$	Inst, 2
4.— $(x)(y)(G(\bar{k}_1 \ldots \bar{k}, x) \wedge G(\bar{k}_1 \ldots \bar{k}, y) \rightarrow x=y)$	eparación 3
5.— $G(\bar{k}_1 \ldots \bar{k}, \bar{a}) \wedge G(\bar{k}_1 \ldots \bar{k}, \bar{b}) \rightarrow \bar{a}=\bar{b}$	ESP 4
6.— $\sim(\bar{a}=\bar{b}) \rightarrow \sim(G(\bar{k}_1 \ldots \bar{k}, \bar{a}) \wedge G(\bar{k}_1 \ldots \bar{k}, \bar{b}))$	contrapositiva 7
7.— $\sim(\bar{a}=\bar{b}) \rightarrow (\sim G(\bar{k}_1 \ldots \bar{k}, \bar{a}) \vee \sim G(\bar{k}_1 \ldots \bar{k}, \bar{b}))$	L.eq a 6
8.— $\sim(\bar{a}=\bar{b}) \rightarrow (G(\bar{k}_1 \ldots \bar{k}, \bar{a}) \rightarrow \sim G(\bar{k}_1 \ldots \bar{k}, \bar{b}))$	L.eq a 7
9.— $\sim(\bar{a}=\bar{b})$	Teo; Prop. 8

10.- $G(\bar{k}_1..\bar{k},\bar{a})\rightarrow\sim G(\bar{k}_1..\bar{k},\bar{b})$ MP 9,9

11.- $\sim G(\bar{k}_1..\bar{k},\bar{b})$ MP 1,10 ∎

Las funciones recursivas definidas a través del operador μ no acotado carecen de símbolos especiales para su representación en AR. No obstante, es posible definir fórmulas que las representan como se indica en la siguiente proposición.

Proposición 12.- Sea $g(x_1,\ldots,x_n,y)$ una función aritmética tal que:

(1) Para todo $(k_1,\ldots,k_n)\in\mathbb{N}^n$ existe $k\in\mathbb{N}$ tal que $g(k_1,\ldots,k_n,k)=0$

(2) La fórmula $G(x_1,\ldots,x_n,y,z)$ la representa fuertemente en AR.

En tal caso la función $f(x_1,\ldots,x_n)=\mu y(g(x_1,\ldots,x_n,y)=0)$ está fuertemente representada en AR por la fórmula

$F(x_1\ldots x_n,y)\equiv G(x_1\ldots x_n,y,\bar{0})\wedge(z)(z<y\rightarrow\sim G(x_1\ldots x_n,z,\bar{0}))$.

Demostración

R_{21}) Sean $k_1,\ \ ,k_n,k\in\mathbb{N}$ tales que $f(k_1,\ldots,k_n)=k$

Por demostrar: $\vdash F(\bar{k}_1\ldots\bar{k}_n,\bar{k})$

De nuestra hipótesis se sigue que $g(k_1,\ldots,k_n,0)\neq 0$(a menos que $k=0$), ... $g(k_1,\ldots,k_n,k-1)\neq 0$ y $g(k_1,\ldots,k_n,k)=0$.

Tenemos la siguiente prueba en AR:

1.- $G(\bar{k}_1\ldots\bar{k}_n,\bar{k},\bar{0})$ Teo por hipótesis

2.- $\sim G(\bar{k}_1\ldots\bar{k}_n,\bar{0},\bar{0})$ Teo: proposición 11

....

k.- $\sim G(\bar{k}_1\ldots\bar{k}_n,\overline{k-1},\bar{0})$ Teo: proposición 11

k+1.- $(z)(z<\bar{k}\rightarrow\sim G(\bar{k}_1\ldots\bar{k}_n,z,\bar{0}))$ CL 2,k: prop. [30]

k+2.- $G(\bar{k}_1\ldots\bar{k}_n,\bar{k},\bar{0})\wedge(z)(z<\bar{k}\rightarrow\sim G(\bar{k}_1\ldots\bar{k}_n,z,\bar{0}))$ adición 1,k+1

k+3.- $F(\bar{k}_1\ldots\bar{k}_n,\bar{k})$ abreviatura de k+2

R_{22}) Por demostrar: $\vdash\exists_1 x_{n+1}F(x_1\ldots x_n,x_{n+1})$. Por comodidad escribimos $\mathbf{X}$ en vez de $x_1\ldots x_n$. Como primer paso demostramos que $F(\mathbf{X},u),F(\mathbf{X},w)\vdash u=w$.

1.- $G(\mathbf{X},u,0)\wedge(z)(z<u\rightarrow\sim G(\mathbf{X},z,0))$ hip: $F(\mathbf{X},u)$

2.- $G(\mathbf{X},w,0)\wedge(z)(z<w\rightarrow\sim G(\mathbf{X},z,0))$ hip: $F(\mathbf{X},w)$

3.- $G(\mathbf{X},w,0)$ separación a 2

4.- $(z)(z<u\rightarrow\sim G(\mathbf{X},z,0))$ separación a 1

5.- $w<u\rightarrow\sim G(\mathbf{X},w,0)$ ESP a 4

6.- $w<u$ hip

7.- $\sim G(\mathbf{X},w,0)$ MP 5,6

8.- $G(\mathbf{X},w,0)\wedge\sim G(\mathbf{X},w,0)$ adición 3,7

$\therefore\ F(\mathbf{X},u),F(\mathbf{X},w),w<u\vdash G\wedge\sim G$.

Por reducción al absurdo en AR, $F(X, u), F(X, w) \vdash \sim(w<u)$.

En forma análoga se demuestra que $F(X, u), F(X, w) \vdash \sim(u<w)$.

Ahora sucede lo siguiente en AR:

1.– $F(X, u)$	hip
2.– $F(X, w)$	hip
....	
h.– $\sim(w<u)$	Ded 1,2
....	
k.– $\sim(u<w)$	Ded 1,2
k+1.– $(u<w)\vee(w<u)\vee(u=w)$	Teo. proposición [95]
k+2.– $\sim(w<u)\rightarrow(\sim(u<w)\rightarrow u=w))$	L. eq. a k+1
k+3.– $\sim(u<w)\rightarrow u=w)$	MP h, k+2
k+4.– $u=w$	MP k, k+3

$$\therefore\ F(X, u)\wedge F(X, w)\vdash u=w$$

$$\frac{\therefore\ F(X, u)\wedge F(X, w)\vdash u=w}{\vdash (u)(w)(F(X, u)\wedge F(X, w)\rightarrow u=w)}\ \text{MTD y GEN}$$

$$\frac{\vdash \exists y F(X, y)}{\vdash \exists_1 y F(X, y)}\ \text{adición} \qquad \blacksquare$$

Proposición 13.– Si $f: \mathbb{N}^n \longrightarrow \mathbb{N}$ es una función recursiva, entonces f es fuertemente representable en AR.

La demostración se hace por inducción sobre $N(f)$ y es inmediata a partir de las proposiciones 10 y 12. Hacemos caso omiso de la misma.

La representabilidad de las funciones recursivas es garantía de que toda relación recursiva es expresable en AR. Si $R(x_1 \ldots x_n)$ es una relación recursiva, $C_r(x_1 \ldots x_n)$ su función característica y $(k_1 \ldots k_n) \in \mathbb{N}^n$, sabemos que:

$$(k_1 \ldots k_n) \in R \Rightarrow C_r(k_1 \ldots k_n)=0$$
$$(k_1 \ldots k_n) \notin R \Rightarrow C_r(k_1 \ldots k_n)=1$$

Como C_r es recursiva, hay una fórmula $A(x_1 \ldots x_{n+1})$ que la representa en AR (si C_r es recursiva primitiva la fórmula es $\overline{C}_r(x_1 \ldots x_n)=x_{n+1}$). Sabemos que:

Si $C_r(k_1 \ldots k_n)=0$, entonces $\vdash A(\bar{k}_1 \ldots \bar{k}_n, \bar{0})$ (proposición 13)

Si $C_r(k_1 \ldots k_n)=\bar{1}$, entonces $\vdash \sim A(\bar{k}_1 \ldots \bar{k}_n, \bar{0})$ (proposición 11)

De lo anterior se sigue que $A(x_1 \ldots x_n, \bar{0})$ expresa a R en AR. En adelante dicha fórmula se denota $\overline{R}(x_1 \ldots x_n)$. Si R es recursiva primitiva, entonces $\overline{R}(x_1 \ldots x_n) \equiv \overline{C}_r(x_1 \ldots x_n)=\bar{0}$. Ahora podemos escribir:

$$\text{Si } R(k_1 \ldots k_n), \text{ entonces } \vdash \overline{R}(\bar{k}_1 \ldots \bar{k}_n)$$
$$\text{Si } \neg R(k_1 \ldots k_n), \text{ entonces } \vdash \sim\overline{R}(\bar{k}_1 \ldots \bar{k}_n).$$

Notese que en la aritmética informal se emplean las mismas variables que en $\mathcal{AR}$. Esto es posible en virtud de que las variables aritméticas se pueden restrigir a un conjunto predeterminado. La similitud en la notación no debe llevar a confusiones.

Hemos demostrado la siguiente

Proposición 14.- Toda relación recursiva es expresable en $\mathcal{AR}$.

La proposición 14 afirma:

Si la relación R se verifica para los enteros $k_1,\ldots,k_n$, entonces el *enunciado* $\bar{R}(\bar{k}_1\ldots\bar{k}_n)$ es *derivable* en $\mathcal{AR}$, y si la relación R no se verifica para los enteros $k_1,\ldots,k_n$, entonces el *enunciado* $\bar{R}(\bar{k}_1\ldots\bar{k}_n)$ es *refutable* en $\mathcal{AR}$. [18]

Lo anterior significa que la *verdad* del enunciado aritmético $R(k_1\ldots k_n)$ se refleja en el sistema a través de la *derivación* de la fórmula cerrada $\bar{R}(\bar{k}_1\ldots\bar{k}_n)$ que lo representa, mientras que la *falsedad* de dicho enunciado se refleja en $\mathcal{AR}$ a través de la *derivación* de $\sim\bar{R}(\bar{k}_1\ldots\bar{k}_n)$ que es la *negación* de la fórmula que lo representa.

Se concluye que la Aritmética Recursiva admite formalización en $\mathcal{AR}$, pues a todo *enunciado verdadero* de dicha teoría corresponde una fórmula *derivable* en el sistema. Cabe aclarar que esta afirmación sólo obedece, como observa J. Ladriere, a un punto de vista heurístico que puede conducir a equívocos. En rigor no se puede establecer un vínculo entre un sistema formal y una estructura informal vagamente definida. En este caso la noción de verdad considerada en la Aritmética Recursiva se fija por medio de criterios intuitivos y, por lo mismo, no rigurosos. Tales criterios no han de confundirse con la *noción de verdad* de Tarski, en la cual se relacionan los lenguajes formales y las estructuras algebraicas. Pese a ello la afirmación que hacemos al inicio de este párrafo puede justificarse de dos modos distintos: primero, que la definición de Tarski se inspira en las propiedades de los enunciados de la Aritmética informal y, segundo, que al interior de una metateoría adecuada puede definirse la Aritmética Recursiva como una estructura algebraica.

---

[18] *refutable* significa que su negación es derivable en el sistema.

ARITMETIZACION DE LA SINTAXIS DE AR

Enunciados como ‹*t es un término de* AR› o ‹*la fórmula* G *no es un teorema de* AR› no forman parte de L_a sino de su metateoría. Para expresar tales nociones metateóricas en un sistema como AR Gödel ideó un dispositivo mediante el cual los enunciados metamatemáticos se traducen en enunciados aritméticos. Dado que el sistema formaliza parte de la Aritmética, es posible formalizar en él parte de su metateoría, su descripción y propiedades.

$$
\begin{tikzcd}
 & \boxed{\text{metateoría}} \arrow[dl, "\text{(2) traducción}"'] & \\
\boxed{\text{Aritmética informal}} \arrow[rr, "\text{(3) formalización}"] & & \boxed{\text{sistema AR}} \arrow[ul, "\text{(1) descripción}"']
\end{tikzcd}
$$

Antes de Gödel era poco clara la relación entre la metateoría y la Aritmética informal. A través de un análisis de la naturaleza de los sistemas formales, Gödel profundizó en el entendimiento de sus relaciones mutuas. Como se sabe, un sistema formal es un conjunto de expresiones formales organizado conforme a reglas explícitas. De acuerdo a la concepción original de Hilbert, la metateoría de cualquier sistema se enmarca en el ámbito de la argumentación intuitiva, contrastando en ello con el sistema mismo. Gödel dio un paso adelante al descubrir que la metamatemática es suceptible a su vez de tratamiento formal. Su merito consistió en observar que, desde un punto de vista general, la naturaleza específica de los signos que se utilizan al construir un sistema formal es irrelevante. "*Las fórmulas de un sistema formal, en su aspecto externo, son secuencias de signos primitivos...y es facil establecer con toda precisión cuáles secuencias de signos primitivos son fórmulas y cuáles no. Análogamente, las pruebas, desde un punto de vista formal, no son otra cosa que secuencias finitas de fórmulas. Para las consideraciones metamatemáticas resulta indiferente qué objetos usamos como signos primitivos, asi que nosotros utilizaremos números naturales para tal fin. En consecuencia una fórmula es una secuencia finita de números naturales y una prueba una secuencia finita de secuencias finitas de números naturales. Asi, las nociones metamatemáticas se convierten en nociones relativas a los números naturles o secuencias de éstos y por tanto pueden (al menos parcialmente) ser expresadas con los símbolos del sistema formal*" (Gödel: Sobre enunciados formalmente indecidibles en PRINCIPIA MATHEMATICA Y sistemas afines Parte I). Al reemplazar los símbolos de un sistema formal con números naturales, los enunciados metamatemáticos se convierten en enunciados aritméticos. Si la Aritmética es lo que se formaliza, también la metateoría se puede formalizar.

Al procedimiento de reemplazar cada símbolo primitivo por un número natural se le llama *Aritmetización de la sintaxis*. Dicho procedimiento sirve como base para una codificación.

III.1.– Correspondencia de Gödel

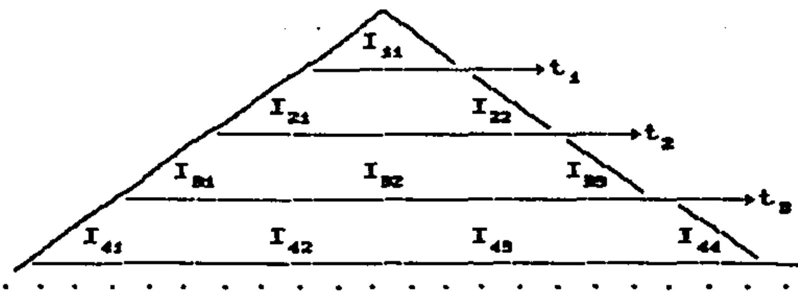
Aplicamos el procedimiento de Gödel al lenguaje L_0. Para ello definimos una correspondencia δ como se indica en la tabla siguiente:

$\sim$	$\rightarrow$	(	)	R	C	=	c_0	s	I_{00}	x_n	I_{nk} $(1\leq k\leq n)$
3	5	7	9	11	13	15	17	19	21	$23+4n$	$17+4(t_n+k)$ [1]

Al número asociado a cada símbolo S se le llama *número de correspondencia* de S y se le denota δS. Escribimos:

$\delta\sim=3$, $\delta\rightarrow=5$, ..., $\delta I_0=21$, $\delta x_0=23$, $\delta I_{00}=25$, $\delta x_1=27$, $\delta I_{11}=29$, etc. [2]

El siguiente diagrama nos muestra cómo se numeraron los símbolos funcionales.



I_{nk}: la pareja (n,k) está en la base del triángulo (equilátero) de lado n y ocupa el k–esimo lugar en dicha linea. Se le asocia el número t_n+k. Como $1\leq k\leq n$, se tiene que $t_n<t_n+k<t_{n+1}$. Se sigue de lo anterior que ningún número triangular corresponde a alguna pareja (n,k).

$I_{11} \longrightarrow$ 2

$I_{21}, I_{22} \longrightarrow$ 4, 5

$I_{31}, I_{32}, I_{33} \longrightarrow$ 7, 8, 9

$I_{41}, I_{42}, I_{43}, I_{44} \longrightarrow$ 11, 12, 13, 14

No figuran en la correspondencia los números 1, 3, 6, 10, 15, 21, ... (números triangulares).

La correspondencia de Gödel es tal que a los símbolos de distintas categorías les corresponden números de distintas clases residuales:

---

[1] t_n es el n–esimo número *triangular*: $t_n=1+2+...+n$. Por otra parte escribimos I_{00} en vez de I_0 por que así nos convendrá más adelante.

[2] Se puede demostrar que la correspondencia de Gödel es una codificación, aunque aquí no lo haremos.

Símbolos funcionales $\longrightarrow$ números de la clase residual [1] (módulo 4)
Variables individuales $\longrightarrow$ números de la clase residual [3] (módulo 4)

Hay que aclarar que no todo número de la clase residual [1] es imagen de un símbolo funcional. $x\in[1]$ es imagen de algún símbolo I_{nk} $\Leftrightarrow$ $x\geq 21$ y $q(x+17,4)$ no es triangular.

En el ejemplo que sigue mostramos a la izquierda una sucesión de fórmulas y a la derecha la sucesión de sucesiones de sus números de corresondencia:

$\sim(sx_0=0)$	3, 7, 19, 23, 15, 17, 9
$(x_0)\sim(sx_0=0)$	7, 23, 9, 3, 7, 19, 23, 15, 17, 9
$((x_0)\sim(sx_0=0)\rightarrow\sim(s0=0))$	7, 7, 23, 9, 3, 7, 19, 23, 15, 17, 9, 5, 3, 7, 19, 17, 15, 17, 9, 9
$\sim(s0=0)$	3, 7, 19, 17, 15, 17, 9

Si $a_1,\ldots,a_n$, es una sucesión de números naturales, definimos un número natural $\langle a_1,\ldots,a_n\rangle$ con la ecuación

$$\langle a_1,\ldots,a_n\rangle=p_1^{a_1}\cdot\ldots\cdot p_n^{a_n}$$

de modo que si $a=\langle a_1,\ldots,a_n\rangle$, entonces $a_1=(a)_1,\ldots,a_n=(a)_n$.

Ejemplo.- Dada la sucesión 3,5,2,1 tenemos que:

$\langle 3,5,2,1\rangle=2^3\cdot 3^5\cdot 5^2\cdot 7^1=340200$, de modo que $(340200)_1=3$, $(340200)_2=5$, $(340200)_3=2$ y $(340200)_4=1$. Notese que $(340200)_k=0$ para todo $k>4$.

La correspondencia de Gödel es un primer paso la aritmetización de la metateoría de AR. Con su ayuda es posible asignar a cada *expresión* E de AR un único número γE como sigue: [3]

$$\text{Si } E=a_1\ldots a_n, \text{ entonces } \gamma E=\langle a_1,\ldots,a_n\rangle$$

Al número γE se le llama *número de Gödel* de la expresión E.

Con el mismo recurso podemos asignar a cada secuencia finita S de expresiones $E_1,\ldots,E_m$ un único número $\gamma^2 S$ como sigue:

$$\gamma^2 S=\langle\gamma E_1,\ldots,\gamma E_n\rangle$$

Al número $\gamma^2 S$ se le llama *número de secuencia* de S.

En las definiciones anteriores hemos supuesto que las expresiones son secuencias finitas de números. Con base en la correspondencia de Gödel es factible hacer dicha identificación. Si el lector lo prefiere, puede imaginar que los signos primitivos fueron reemplazados por

---

[3] Una *expresión* es una sucesión finita de signos del alfabeto de L_a.

números. Algo similar sucede con los números de Gödel y los números de secuencia. Aquéllos se corresponden uno a uno con las expresiones de $\mathbb{L}_a$ y éstos con las secuencias finitas de expresiones. Ya no carecen de sentido expresiones como <*n es un axioma de* $\mathbb{AR}$> o <*m es una prueba de n*> cuando m y n son números naturales. Con base en lo anterior tomamos por expresiones de $\mathbb{AR}$ a los números de Gödel y por secuencias de expresiones a los números de secuencia.

ejemplos y comentarios

(1) Un número $n\in\mathbb{N}$ es de correspondencia si y sólo si:

i) es impar.
ii) es mayor que 1.
iii) si $n\geq 27$ y $r(n,4)=3$, entonces $q(n+11,4)$ no es triangular.
iv) si $n\geq 29$ y $r(n,4)=1$, entonces $q(n+13,4)$ no es triangular.

(2) Un número $n\in\mathbb{N}$ es de Gödel si y sólo si:

i) si $k\leq n$, $1\leq h<k$ y $p_k|n$, entonces $p_h|n$.
ii) si $1\leq k\leq n$ y $p_k|n$, entonces $(n)_k$ es número de correspondencia.

De lo antes dicho se sigue que para que un número sea de Gödel es necesario que sea par y que al descomponerlo como producto de factores primos, cada uno de dichos factores tenga exponente impar.

(3) Un número $n\in\mathbb{N}$ es de secuencia si y sólo si:

i) si $k\in\{1,\dots,n\}$, $h\in\{1,\dots,k-1\}$ y $p_k|n$, entonces $p_h|n$
ii) para todo $k\in\{1,\dots,n\}$, si $p_k|n$ entonces $(n)_k$ es número de Gödel.

Comparando (1), (2) y (3) tenemos:

(1) vs (2)&(3).- Ningún número de correspondencia es de Gödel o de secuencia y <u>viceversa</u>: aquéllos son impares y éstos pares.

(2) vs (3).- Ningún número de Gödel es de secuencia y <u>viceversa</u>: Los primeros tienen factores primos elevados a potencias impares en su descomposición, mientras que los segundos tienen factores primos elevados a potencias pares en su descomposición.

(4) Se dispone de tres categorías o niveles N_1, N_2 y N_3 de números según sean de correspondencia, de Gödel o de secuencia. Algunos objetos de $\mathbb{AR}$ tienen asociados números en cada una de ellas.

En la siguiente tabla se muestran los números asociados a los símbolos '$\sim$' y '$\longrightarrow$' según se les considere signos primitivos (N_1) expesiones (N_2) o sucesiones finitas de expresiones (N_3):

Símbolo:	$\sim$	$\longrightarrow$	
N_1:	3	5	# corespondencia
N_2:	$2^3=8$	$2^5=32$	# Gödel
N_3:	$2^8=256$	$2^{32}=4\ 294\ 967\ 296$	# secuencia.

Cuando una expresión consta de más de un símbolo primitivo, en el nivel N_1 se tiene una sucesión de números en vez de uno sólo.

Por ejemplo, si la expresión es '$s(c_0)$' tenemos:

expresión:	$s(c_0)$	
N_1:	19, 7, 17, 9	# correspondencia
N_2:	$2^{19}\cdot 3^{7}\cdot 5^{17}\cdot 7^{9}$	# Gödel
N_3:	$2^{85'801'335'403'523'706'054'687'500'000}$	# secuencia

(5) Sin entrar en detalles diremos que el método recién expuesto es una *codificación* de los objetos de L_0. Los números de secuencia son los números de código de los símbolos, expresiones y sucesiones de expresiones de AR. Dejamos esta afirmación sin demostrar.

(6) No sólo trabajamos con números de secuencia, sino que también hacemos uso de los números de correspondencia y de Gödel cuando resulte conveniente. No obstante, la teoría puede desarrollarse por completo sin recurrir a estos últimos.

III.2.— Transcripción de la sintaxis de AR a la Aritmética Recursiva

Con el método de la aritmetización es posible traducir las reglas de formación y deducción del sistema AR a la Aritmética Recursiva, pues cada relación, propiedad u operación sintáctica induce una relación, propiedad u operación aritmética entre los números correspondientes. Su recursividad tiene por origen el carácter constructivo y/o efectivo de las nociones consideradas.

Mostramos a continuación que la sintaxis del sistema AR forma parte de la Aritmética Recursiva. Lo hacemos exhibiendo una lista de funciones y relaciones recursivas que forman parte de su descripción metateórica.

NOCIONES GENERALES

25.— $t_0=0$
$t_{n+1}=t_n+(n+1)$ [4] — t_k es el k-esimo número triangular

26.— $TRIANG(x)\equiv\exists k(k\leq x\ \&\ x=t_k)$ [5] — x es un número triangular

---

[4] La numeración 25, 26, etc. es continuación de la que inicia en el capítulo I.

[5] Las relaciones y propiedades aritméticas se denotan con letras mayúsculas y las funciones y operaciones aritméticas con letras minúsculas. El nombre otorgado a algunas de ellas sugiere la noción de que se trata. Vgr PRIMO(x) por <x es *primo*>.

27.- $l(x)=\mu y(y\leq x \ \& \ p_y|x)$ longitud de x

Cuando $x=\gamma E$ y E es una expresión de L_a, $l(x)$ es el número de símbolos que hay en E, y si $x=\gamma^2 S$ y S es una sucesión de fórmulas, entonces $l(x)$ es la longitud de la sucesión (Vgr la longitud de una prueba).

28.- $x*y=\prod_{k=0}^{l(x)} p_k^{(x)_k}\cdot\prod_{k=0}^{l(y)} p_{l(x)+k}^{(y)_k}$

Si $x=\langle a_1,\ldots,a_n\rangle$ y $y=\langle b_1,\ldots,b_m\rangle$, entonces $x*y=\langle a_1,\ldots,a_n,b_1,\ldots,b_m\rangle$. Esta operación es asociativa y corresponde a la operación sintáctica de *concatenación*: dadas las expresiones E_1 y E_2, $\gamma E_1*\gamma E_2=\gamma E_1E_2$.

29.- $pp(x)=2^7*x*2^9$

Poner paréntesis a la expesión x. Si $x=\gamma E$, entonces $pp(x)=\gamma(E)$.

NOCION DE CONSTANTE FUNCIONAL

Al construir una constante funcional f tienen lugar dos procesos paralelos. Por una parte se tiene la construcción de la expresión formal "f" y por la otra la determinación de su grado gr(f). En esta sección demostramos que la relación

$$CFG=\{(f,q) \mid f \text{ es una constante funcional de grdo } q\}$$

es recursiva primitiva.

Toda constante funcional f de grado q se forma a través de una secuencia $(f_1,q_1),\ldots,(f_m,q_m)$ de pares ordenados que satisfacen las siguientes condiciones:

1) $f_m=f$ y $q_m=q$
2) Para cada $i\in\{1,\ldots,m\}$ se cumple alguna de las siguientes cláusulas:

   a) (f_i,q_i) es $(s,1)$
   b) (f_i,q_i) es $(I_{00},0)$
   c) (f_i,q_i) es (I_{nk},n) para alguna n y alguna k tales que $1\leq k\leq n$
   d) (f_i,q_i) es $(Rgh,n+1)$ y para algunas $j,k\in\{1,\ldots,i-1\}$ (f_j,q_j) es (g,n) y (f_k,q_k) es $(h,n+2)$
   e) (f_i,q_i) es $(Cgh_1\ldots h_j)$, para alguna $k\in\{1,\ldots,i-1\}$ (f_k,q_k) es (g,m) y para cada $r\in\{1,\ldots,m\}$ hay una k(r) tal que (f_{kr},q_{kr}) es (h_r,q_r).

A la secuencia $(f_1,q_1),\ldots,(f_m,q_m)$ so lo llama *socuoncia do formación* de f_m. Se el asigna el número

$$\langle\langle f_1,q_1\rangle,\ldots,\langle f_m,q_m\rangle\rangle=\langle 2^{f_1}\cdot 3^{q_1},\ldots,2^{f_m}\cdot 3^{q_m}\rangle=2^{2^{f_1}\cdot 3^{q_1}}\cdot\ \ldots\ \cdot p_m^{2^{f_m}\cdot 3^{q_m}}$$

En el factor $p_i^{2^{f_i}\cdot 3^{q_i}}$ el exponente f_i es el número de Gödel de una constante funcional y q_i es su grado.

Para representar en la Aritmética Recursiva el encadenamiento de m constantes funcionales $h_1, \ldots, h_m$ como se pide en el inciso 2(e), se requiere de la siguiente función recursiva:

30.— $conc(x,0)=1$
$conc(x,sn)=conc(x,n)*(x)_m$

$conc(x,n)$ es la expresión que resulta al *concatenar* las expresiones codificadas en los primeros n exponentes al descomponer x como producto de factores primos.

31.— $SECFORMCF(x) \equiv \neg(x=0) \& \forall i(1 \leq i \leq l(x) \Rightarrow INI((x)_i) \vee REC((x)_i) \vee COMP((x)_i))$

x es el número de una secuencia de formación de una constante funcional. En la definición ocurren los siguientes predicados:

$INI((x)_i) \equiv (x)_i = \langle \gamma s, 1 \rangle \vee (x)_i = \langle \gamma I_{00}, 0 \rangle \vee \exists n \exists k(1 \leq k \leq n \leq x \ \& \ (x)_i = \langle \gamma 13+4(t_n+k), n \rangle)$

$REC((x)_i) \equiv \exists j \exists k(1 \leq j, k < i \ \& \ (x)_i = \langle \gamma 11 * (x)_{j1} * (x)_{k1}, (x)_{j2}+1 \rangle \ \& \ (x)_{k2} = (x)_{j2}+1)$,[6] y

$COMP((x)_i) \equiv \exists g \exists h \exists n(g,h,n \leq x \ \& \ l(h) < i \ \& \ (x)_i = \langle \gamma 13 * g * conc(h, l(h), n \rangle \ \&$
$\forall k(1 \leq k \leq l(h) \Rightarrow \exists m(1 \leq m < i \ \& \ (x)_m = \langle (h)_k, n \rangle) \ \& \ \exists j(1 \leq j < i \ \& \ (x)_j = \langle g, l(h) \rangle)$.

La definición recién expuesta es posible en virtud de la siguiente proposición que enunciamos sin demostrar:

<u>Proposición</u>.— Si f es una constante funcional, entonces:

1) $\gamma f > gr(f)$
2) hay una secuencia de formación de f cuya longitud es menor o igual que $l(\gamma f)$. ■[7]

Se sigue de lo antes dicho que una expresión f es una constante funcional si y sólo si hay una secuencia de formación de f de longitud $l(f)$ y exponentes con valor menor o igual a $2^f \cdot 3^f$.

---

[6] $(x)_{nj} \rightsquigarrow ((x)_n)_j$.

[7] El inciso (1) se puede demostrar por inducción sobre $N(f)$.
El inciso (2) se sigue del hecho de que hay una construción de f en la que en cada paso se introduce uno de los signos que la integran, de modo que la construcción tiene tantos pasos como signos f. Este hecho se torna evidente al considerar algunos ejemplos como el siguiente:

Dada la secuencia de formación

1.— $(s,1)$
2.— $(I_{11},1)$
3.— $(I_{33},3)$
4.— $(CsI_{33},3)$
5.— $(RI_{11}CsI_{33},2)$

podemos observar que en cada paso se introduce un nuevo signo según se indica en la siguiente tabla:

PASO	5	2	4	1	3
SIGNO	R	I_{11}	C	s	I_{33}

32.– $CFG(x,n)\equiv\exists y(y\leq l(x)\cdot p_{l(x)}^{\omega x\omega}\ \&\ SECFORMCF(y)\ \&\ x=(y)_{l(y),1}\ \&\ n=(y)_{l(y),2})$

33.– $CF(x)\equiv\exists n(n\leq x\ \&\ CFG(x,n))$

x es una constante funcional.

34.– $gr(x)=n$ si $CF(x)$ y $n=\mu y(y\leq x\ \&\ CFG(x,y))$
$gr(x)=0$ si $\neg CF(x)$

grado de la constante funcional x.

NOCION DE TERMINO

Todo término se construye a través de una *secuencia de formación* $t_1,\ldots,t_n$ con las características siguientes:

(1) Para cada $i\in\{1,\ldots,n\}$ alguna de las condiciones siguientes se cumple:

a) t_i es c_0
b) t_i es x_k para alguna $k\in\mathbb{N}$
c) t_i es $ft_{k1}\ldots t_{kr}$ con f una constante funcional de grado r y $t_{k1},\ldots,t_{kr}$ términos previos a t_i en la sucesión (es decir, $k_1,\ldots,k_r<i$)

(2) $t=t_n$.

Mostramos en lo que sigue que la propiedad <x *es el número de secuencia de una secuencia de formación de un término*> es recursiva primitiva.

35.– $VAR(x)\equiv\exists y(y\leq x\ \&\ x=23+4y)$ x es el número de correspondencia de una variable. [*]

36.– $TERMSIMP(x)\equiv 2=\mathrm{M}p(p\leq x\ \&\ PRIM(x)\ \&\ p|x)\ \&\ (VAR((x)_1)\vee (x)_1=17)$

x es el número de Gödel de una variable o de la constante c_0 (un término simple).

37.– $SECFORMTERM(x)\equiv\sim(x=0)\ \&\ \forall i(1\leq i\leq l(x)\Rightarrow TERMSIMP((x)_i)\vee TERMCOMP((x)_i))$

donde $TERMCOMP((x)_i)$ es la propiedad

$\exists y\exists z(y,z<x\ \&\ CF(y)\ \&\ l(z)=gr(y)\ \&\ \forall j(1\leq j\leq l(z)\Rightarrow\exists k(1\leq k<l(x)\ \&$
$(x)_k=(z)_j)\ \&\ (x)_i=y*conc(z,l(z)))$.

x es el número de secuencia de una secuencia de formación de un término.

38.– $TERM(x)\equiv\exists y(y\leq l(x)\cdot p_{l(x)}^{x}\ \&\ SECFORM(y)\ \&\ x=(y)_{l(y)})$ x es un término

---

[*] En este caso trabajamos con el número de correspondencia en vez del número de Gödel por comodidad, como más adelante se verá.

La definición anterior se apoya en la siguiente proposición que enunciamos sin demostrar:

Proposición.— Si t es un término, entonces hay una secuncia de formación $t_1, \ldots, t_n$ de t tal que:

(1) $\gamma t_i \leq \gamma t$ para cada $i \in \{1, \ldots, n\}$
(2) $n \leq l(\gamma t)$. ■

Se sigue de esta proposición que todo término t tiene una secuencia de formación acotada por el número $l(n) \cdot p_{l(n)}^{n}$ con $n = \gamma t$.

39.— $nml(0) = 2^{17}$

$nml(sx) = 2^{19} * nml(x)$

$nml(k)$ es el número de Gödel del numeral de k: $nml(k) = \gamma \bar{k}$.

NOCION DE FORMULA

40.— $AT(x) \equiv \exists y \exists z(y, z < x \ \& \ TERM(y) \ \& \ TERM(z) \ \& \ x = 2^7 * y * 2^{15} * z * 2^9)$

x es una fórmula atómica.

41.— $neg(x) = 2^9 * x$ número de Gödel de $\sim x$

42.— $gen(x, v) = 2^7 * 2^v * 2^9 * x$ número de Gödel de $(v)x$

43.— $imp(x, y) = 2^7 * x * 2^5 * y * 2^9$ número de Gödel de $(x \rightarrow y)$

44.— $FORM(0)$ es falso
$FORM(sx) \equiv AT(sx) \vee \exists y(y < sx \ \& \ FORM(y) \ \& \ sx = neg(y)) \vee$
$\exists y \exists v(y, v < sx \ \& \ FORM(y) \ \& \ VAR(V) \ \& \ sx = gen(y, v)) \vee$
$\exists y \exists z(y, z < sx \ \& \ FORM(y) \ \& \ FORM(z) \ \& \ sx = imp(y, z))$.

x es una fórmula.

SUBSTITUCIONES

45.— $AC(v, n, x) \equiv VAR(v) \ \& \ \exists y \exists z \exists w(y, z, w < x \ \& \ x = y * gen(w, v) * z \ \& \ (x)_n = v \ \&$
$l(y) < n \leq l(y) + l(gen(w, v)))$.

la variable v ocurre acotada en la posición n de la expresión x.

46.— $LIB(v, n, x) \equiv VAR(v) \ \& \ (x)_n = v \ \& \ \neg AC(v, n, x)$

la variable v ocurre libre en la posición n de la expresión x.

47.— $lol(0, v, x) = 0$
$lol(sn, v, x) = \mu y(y \leq l(x) \ \& \ LIB(v, y, x) \ \& \ lol(n, v, x) < y)$

$lol(n, v, x)$ es la posición de la n-esima ocurrencia libre de v en x.

48.— $nol(v,x)=\sum_{k=1}^{l(x)} sg(l(x)\dot{-}lol(k,v,x))$

49.— $seg(0,x)=1$

$seg(sn,x)=seg(n,x)*p_{sn}^{(x)_{sn}}$

$seg(n,x)$ es el segmento inicial de x formado por sus primeros n signos.

50.— $reemp(x,0,y)=x$

$reemp(x,sn,y)=seg(n,x)*y*\prod_{k=0}^{l(x)-n} p_k^{(x)_{n+k+1}}$

$reemp(x,n,y)$ es la expresión que resulta de reemplazar en la expresión x el n—esímo símolo por la expresión y.

51.— $sub(0,x,v,t)=x$

$sub(sn,x,v,t)=reemp(sb_n(n,x,v,t),n(l(t)\dot{-}1)+lol(n+1,v,x),t)$

$sub(n,x,v,t)$ es la fórmula que resulta al substituir en x las n primeras ocurrencias libres de v por el término t.

52.— $sb(x,v,t)=sub(nol(v,x),x,v,t)$

$sb(x,v,t)$ es la fórmula que resulta al substituir en x todas las ocurrencias libres de v por t.

Relacionada con la operación sintáctica de *substitución* se encuentra la noción de *libertad relativa de un término respecto de una variable en una fórmula*. Las siguientes relaciones la definenen la Aritmética Recursiva.

53.— $SF(x,y)\equiv FORM(x)\ \&\ FORM(y)\ \&\ \exists z\exists w(z,w\leq y\ \&\ y=z*x*w)$

x es una subfórmula de y.

54.— $OC(v,t)\equiv VAR(v)\ \&\ TERM(t)\ \&\ \exists k(1\leq k\leq l(t)\ \&\ (t)_k=v)$

la variable v ocurre en el término t.

55.— $LP(t,v,x)\equiv\neg\exists y\exists w\exists h\exists j\exists k(y,w\leq x\ \&\ h,j,k\leq l(x)\ \&\ h<j\leq h+k\ \&\ OC(w,t)\ \&$
$FORM(gen(y,w))\ \&\ seg(h+k,x)=seg(h,x)*gen(y,w)\ \&$
$LIB(v,j,x))$

El término t es libre para la variable v en x.

NOCION DE PRUEBA

56.— $AX(x)\equiv A_1(x)\vee\ldots\vee A_{14}(x)$

x es un axiona de AR. Cada uno de los predicados $A_1,\ldots,A_{14}$ corresponde a un grupo de axiomas de AR. Como ejemplos definimos algunos de ellos:

$A_4(x)\equiv\exists y\exists v\exists t(y,v,t\leq x\ \&\ FORM(y)\ \&\ VAR(v)\ \&\ TERM(t)\ \&\ LIB(t,v,y)\ \&$
$x=imp(gen(y,v),sb(y,v,t))$

$A_{13}(x)\equiv\exists g\exists h\exists z(g,h,z\leq x \ \& \ CF(g) \ \& \ CF(h) \ \& \ x=2^{11}*g*h*z*2^{15}*g*z \ \&$
$\quad \forall k(1\leq k\leq l(z)\Rightarrow\exists v(v\leq z \ \& \ VAR(v) \ \& \ (z)_k=v))$

57.- $MP(x,w,z)\equiv FORM(x) \ \& \ FORM(w) \ \& \ FORM(z) \ \& \ (w=imp(z,x) \vee z=imp(w,x))$

x se infiere de w y z por medio de la regla (MP).

58.- $GEN(x,z)\equiv FORM(x) \ \& \ FORM(z) \ \exists v(v\leq x \ \& \ VAR(v) \ \& \ x=gen(z,v))$

x se infiere de z por medio de la regla (GEN).

59.- $PI(x,z,w)\equiv FORM(x) \ \& \ FORM(z) \ \& \ FORM(w) \ \& \ \exists v(v\leq x \ \& \ VAR(v) \ \&$
$\quad z=sb(x,v,2^{19}) \ \& \ w=imp(x,sb(x,v,2^{19}*2^{v})))$

x se infiere de z y w por medio de la regla (PI).

60.- $CI(x,z,w)\equiv MP(x,z,w) \vee GEN(x,z) \vee GEN(x,w) \vee PI(x,z,w)$

x es consecuencia inmediata de z y w.

61.- $PRUEBA(x)\equiv l(x)\geq 1 \ \& \ \forall k(1\leq k\leq l(x)\Rightarrow(AX((x)_k) \vee \exists i\exists j(1\leq i,j<k \ \&$
$\quad CI((x)_k,(x)_i,(x)_j))))$

x es una prueba.

62.- $PR(x,y)\equiv PRUEBA(x) \ \& \ FORM(Y) \ \& \ y=(x)_{l(x)}$

x es una prueba de y.

Queda demostrado que la relación sintáctica <*la sucesión $A_1,\ldots,A_n$ es una prueba de la fórmula A*> es recursiva primitiva. A partir de ella se define la propiedad sintáctica <*A es un teorema*> como sigue:

$$TEO(x)\equiv\exists yPR(y,x)$$

En esta definición se cuantifica la variable 'y' en forma irrestricta. Debido a ello no se puede aseverar (aunqe tampoco negar) que la propiedad es recursiva o recursiva primitiva. No obstante, este hecho debe considerarse como un indicativo de tal imposibilidad. Parece imposible que las formulas de AR porten en su estructura rasgos que indique su derivabilidad y dentro de que rango se encuentra una de sus pruebas.

EL PRIMER TEOREMA DE GÖDEL

Con el método de la aritmetización se muestra que la sintaxis de diversos sistemas formales es parte de la Aritmética Recursiva. Este vínculo entre dominios distintos (Metateoría-Aritmética Recursiva) es similar al que estableció R. Descartes entre el Algebra y la Geometría. En nuestro caso el homólogo del método de las coordenadas es la correspondencia de Gödel. Este método pone de manifiesto una similitud estructural entre campos en apariencia distintos.

A partir del trabajo de Gödel se sabe de enunciados aritméticos que *describen* la estructura de sistemas formales. Más aún, se conocen enunciados metateóricos cuya verdad es equivalente a la de ciertos enunciados aritméticos. Esta es la similitud estructural referida en el pasaje anterior, y constituye el derrotero a nuevas e insospechadas investigaciones metateóricas.

Como primer paso en esta dirección Gödel se ocupa de un problema planteado por Hilbert en la década de los veintes: ¿es posible definir un conjunto de axiomas para la Aritmética Elemental que sea consistente y completo? [1] Como veremos dicha interrogante se responde con una negativa: ningún sistema formal que contenga una representación de la Aritmética Recursiva puede ser a la vez axiomático, consistente y completo. Cabe señalar que en su demostración Gödel se ve forzado a adoptar una *hipótesis más poderosa* que la de consistencia simple: para sus fines ha de suponer que el sistema formal es ω-consistente. Esto constituye un defecto en su demostración que fue corregido por J.B. Rosser en el año de 1936.

En la primera parte de este capítulo se define el concepto de ω-consistencia y se muestra su relación con el de consistencia simple. Acto seguido se construye el enunciado de Gödel y se demuestra su indecidibilidad en AR a partir de la hipótesis ya mencionada. Finalmente se demuestra el teorema de Gödel-Rosser y se plantean algunas consideraciones de caracter general en relación a dichos teoremas.

IV.1.- La ω-consistencia

Hay dos definiciones de *consistencia sintáctica* para los sistemas formales. Son las siguientes:

(1) Un sistema formal SF es *consistente* si y sólo si hay una fórmula $\varphi \in L_{sf}$ que no es derivable en él.

---

1 Sea $\mathbb{N}=\langle \mathbb{N},+,\cdot,s,=,0\rangle$ y $T(\mathbb{N})=\{p \in L_a \mid \mathbb{N} \models p\}$. Podemos replantear el problema como sigue: ¿hay un conjunto decidible de fórmulas $A \subset L_a$ tal que $\bar{A}=T(\mathbb{N})$? De hecho Hilbert creyó que sí lo había y tenía como base la formalización de los axiomas de Peano en un lenguaje de primer orden. En nuestro caso Dicha formalización corresponde a la reducción siguiente: los grupos de axiomas G_{12} y G_{13} se limitan a las constantes funcionales '+' y '·' y el grupo G_{14} se excluye por completo.

(2) Un sistema formal SF es *consistente* si y sólo si no es posible derivar en él una fórmula y su negación.

Estas definiciones no tienen el mismo alcance, pues es obvio que la segunda de ellas sólo se aplica a sistemas formales con operador de *negación*. No obstante, para la mayoría de los sistemas de éste tipo las definiciones son equivalentes. Tal es el caso del sistema AR.

La *ω-consistencia* es un tipo particular de consistencia sintáctica que sólo es aplicable a sistemas con operadores para la negación, la cuantificación universal y que contienen expresiones para representar números naturales. Cuando tal es el caso, hay en el sistema constantes individuales (o numerales) que denotamos $\bar{0}, \bar{1}, \bar{2}$, etc. que representan a los números naturales 1,2,3, etc.

Definición.— Un sistema formal SF es *ω-inconsistente* si y sólo si hay una fórmula $A(x) \in L_{sf}$ tal que:

i) para todo $k \in \mathbb{N}$, $\vdash_{sf} A(\bar{k})$

y

ii) $\vdash_{sf} \sim(x)A(x)$.

Un sistema formal que no es ω-inconsistente es *ω-consistente*. La ω-consistencia se expresa así:

Para toda $A(x) \in L_{sf}$, si $\vdash_{sf} A(\bar{k})$ para todo $k \in \mathbb{N}$, entonces $\nvdash_{sf} \exists x \sim A(x)$. *

No es dificil demostrar que todo sistema formal que es ω-consistente es consistente. Empero, el recíproco de este enunciado no es cierto: hay ejemplos de sistemas formales que son consistentes y ω-inconsistentes.

IV.2.— El enunciado de Gödel

El enunciado de Gödel representa una proposición autorreferente, semejante a las que dan lugar a las paradojas del Mentiroso y de Richard. Su diferencia frente a ellas es que no ocurre en antinomia. Gödel considera la noción de ser *una fórmula inderivable* y construye un enunciado que en cierto sentido afirma de sí mismo tal propiedad. Dicha construcción tiene como base una función especial de substitución que hace posible la "autorreferencia" en los lenguajes formales. Ello permite "emular" las paradojas dando lugar a los llamados *teoremas limitativos*: resultados que afirman que el sistema es incapaz de efectuar ciertas cosas como, por ejemplo, formular su semántica o derivar todos los enunciados verdaderos en cierta interpretación.

La función de substitución que aparece en el enunciado de Gödel se obtiene como sigue:

La función sb(x,v,nml(x)), definida por composición a partir de las funciones sb(x,v,t) y nml(x), es recursiva primitiva. Como casos específicos de esta función tenemos las llamadas *funciones diagonales*:

---

* Paráfrasis: Si $A(\bar{k})$ es derivable en SF para todo $k \in \mathbb{N}$, entonces es imposible derivar en SF la fórmula $\exists x \sim A(x)$. Esto en modo alguno significa que $\vdash_{sf}(x)A(x)$.

$diag_0(x)=sb(x,23,nml(x))$
$diag_1(x)=sb(x,27,nml(x))$
......
$diag_k(x)=sb(x,23+4k,nml(x))$
.....

El nombre de *función diagonal* se explica en lo que sigue. Sea, por ejemplo, $A_1(x_1),\ldots,A_n(x_1),\ldots$ una *enumeración* de las fórmulas que tienen libre a la variable x_1 y sea $g_1,\ldots,g_n,\ldots$ la sucesión de sus números de Gödel. Representamos la substitución $x_1/\bar{g}_k$ en la siguiente tabla:

	$A_1(x_1)$	$A_2(x_1)$	$A_3(x_1)$	...
g_1	$\boxed{A_1(\bar{g}_1)}$	$A_2(\bar{g}_1)$	$A_3(\bar{g}_1)$	...
g_2	$A_1(\bar{g}_2)$	$\boxed{A_2(\bar{g}_2)}$	$A_3(\bar{g}_2)$	...
g_3	$A_1(\bar{g}_3)$	$A_2(\bar{g}_3)$	$\boxed{A_3(\bar{g}_3)}$	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Los elementos $A_1(\bar{g}_1)$, $A_2(\bar{g}_2)$, $A_3(\bar{g}_3)$, etc. de la diagonal se generan con la función $diag_1$:

$$diag_1(k)=\gamma A_k(\bar{g}_k)$$

(procedimiento diagonal de Cantor)

En la construcción del enunciado de Gödel se utiliza la función $diag_2(x)=sb(x,31,nml(x))$ como a continuación se indica:

La relación $PR(x,sb(y,31,nml(y)))$ es recursiva primitiva. La fórmula que la representa en AR es $\overline{PR}(x_1,\overline{sb}(x_2,\overline{31},\overline{nml}(x_2))$, cuyas únicas variables libres son x_1 y x_2. Sea $G(x_2)$ la fórmula

$$(x_1)\sim\overline{PR}(x_1,\overline{sb}(x_2,\overline{31},\overline{nml}(x_2)))$$

$G(x_2)$ corresponde al enunciado metateórico: <*No es teorema de* AR *la fórmula que se obtiene al reemplazar en x la variable x_2 por el numeral de x*>. Se considera, pues, la propiedad de no ser una fórmula derivable en el sistema. [3] $G(x_2)$ se transforma en un *enunciado* de L_a al momento de substituir x_2 por un término constante (vgr por un numeral).

$$\text{Sea } g=\gamma(x_1)\sim\overline{PR}(x_1,\overline{sb}(x_2,\overline{31},\overline{nml}(x_2))$$

---

[3] Cabe señalar que la fórmula que se dice es inderivable es el resultado de efectuar ciertas operaciones formales con los signos y expresiones de AR. En modo alguno se trata de una descripción basada en rasgos contingentes o empíricos de las fórmulas.

El enunciado de Gödel es $G(\bar{g}) \equiv (x_1) \sim \overline{PR}(x_1, \overline{sb}(\bar{g}, \overline{31}, \overline{nml}(\bar{g})))$

$G(\bar{g})$ corresponde al enunciado metateórico <*No es un teorema de* AR *la fórmula que se obtiene al reemplazar en* $G(x_2)$ *la variable* x_2 *por el numeral de* $\gamma G(x_2)$>. Nótese que al efectuar la operación descrita en $G(\bar{g})$ se arriba al enunciado $G(\bar{g})$. Es en este sentido que el enunciado de Gödel "afirma" su no derivabilidad en AR: interpretado en la metateoría dice <$G(\bar{g})$ *no es un teorema de* AR>.

IV.3.- El primer teorema de Gödel

Primer teorema de incompletud para AR

a) Si AR es consistente, entonces $\nvdash G(\bar{g})$.

b) Si AR es ω-consistente, entonces $\nvdash \sim G(\bar{g})$.

Demostración

(a) Procedemos por contraposición en la metateoría.

Supongase que $\vdash G(\bar{g})$. (1)

En tal caso hay una prueba $A_1, \ldots, A_n$ del enunciado en AR.

Sea $k = \gamma^2 A_1, \ldots, A_n$ el número de secuencia de la prueba. La relación aritmética $PR(x, sb(y, 31, nml(y)))$ es cierta para (k, g). Dado que la fórmula $\overline{PR}(x_1, \overline{sb}(x_2, \overline{31}, \overline{nml}(x_2)))$ la representa en AR, se tiene:

$\vdash \overline{PR}(\bar{k}_1, \overline{sb}(\bar{g}, \overline{31}, \overline{nml}(\bar{g})))$

por la regla ($\exists$)

$\vdash \exists x_1 \overline{PR}(x_1, \overline{sb}(\bar{g}, \overline{31}, \overline{nml}(\bar{g})))$

y por equivalencias lógicas

$\vdash \sim (x_1) \sim \overline{PR}(x_1, \overline{sb}(\bar{g}, \overline{31}, \overline{nml}(\bar{g})))$ (2)

De (1) y (2) se sigue que $\vdash G(\bar{g}) \wedge \sim G(\bar{g})$ y AR es inconsistente.

Conclusión: Si $\vdash G(\bar{g})$, entonces AR es inconsistente.
Por contraposición en la metateoría queda demostrado el inciso (a).

(b) Supongase que AR es ω-consistente.

De la hipóesis se sigue que AR es consistente.

De la consistencia de AR se sigue que $\nvdash G(\bar{g})$ (inciso (a)).

Esto último significa que ningún número natural es el número de secuencia de una prueba de $G(\bar{g})$. Debido a ello los enunciados aritméticos

$\neg PR(0, sb(g, 31, nml(g)))$

$\neg PR(1, sb(g, 31, nml(g)))$

.....

$\neg PR(k, sb(g, 31, nml(g)))$

.....

son todos verdaderos. En virtud de que $\sim\overline{PR}(x_1, \overline{sb}(x_2, \overline{31}, \overline{nml}(x_2)))$ representa a esta relación en AR, tenemos

$\vdash \sim\overline{PR}(\bar{0}, \overline{sb}(\bar{g}, \overline{31}, \overline{nml}(\bar{g})))$

$\vdash \sim\overline{PR}(\bar{1}, \overline{sb}(\bar{g}, \overline{31}, \overline{nml}(\bar{g})))$

.....

$\vdash \sim\overline{PR}(\bar{k}, \overline{sb}(\bar{g}, \overline{31}, \overline{nml}(\bar{g})))$

.....

Como AR es ω-consitente, entonces $\nvdash \sim(x_1)\sim\overline{PR}(x_1, \overline{sb}(\bar{g}, \overline{31}, \overline{nml}(\bar{g})))$.

conclusión: $\nvdash \sim G(\bar{g})$.

IV.4.- Observaciones y comentarios

1.- De la hipótesis de que AR es ω-consistente se sigue que $\nvdash G(\bar{g})$ y $\nvdash \sim G(\bar{g})$. Dicho en otras palabras, si AR es ω-consistente, entonces $G(\bar{g})$ es indecidible y el sistema es (sintácticamente) incompleto.

2.- Un sistema *formal* en el cual es posible probar $A(\bar{0}), A(\bar{1}), \ldots, A(\bar{k}), \ldots$ pero *no* $(x)A(x)$ se dice que es ω-incompleto. El teorema de Gödel deja ver *en su primera parte* que si AR es consistente, entonces es ω-incompleto (o incompleto respecto a la universalización).

3.- La indecidibilidad de $G(\bar{g})$ (supuesta la ω-consistencia del sistema) muestra *que* el conjunto de axiomas de AR es incompleto. Tal parece que este defecto se puede corregir añadiendo nuevos axiomas. No obstante, toda extensión consistente de AR que tenga un conjunto recursivo de axiomas será incompleta. La *razón* es que el método de demostración aplicado a AR es igualmente aplicable a tales sistemas. De hecho la incompletud *tiene* raices más *profundas* y no se debe a la omisión de algún axioma o *conjunto* de axiomas. La *incompletud* está indisolublemente ligada a la *naturaleza* del sistema. Este rasgo es aún más notorio a la luz del teorema de Gödel-Rosser.

4.- El enunciado $G(\bar{g})$ *corresponde* intuitivamente al enunciado <*La fórmula* $G(\bar{g})$ *es inderivable en* AR>. En este sentido es autorreferente y afirma su inderivabilidad. Notese que bajo su interpretación "canónica" $G(\bar{g})$ es verdadero $\Leftrightarrow \nvdash G(\bar{g}) \Leftrightarrow$ AR es consistente. Resulta así que el teorema de Gödel conduce al programa de Hilbert a un callejón sin salida: es imposible recoger en un sistema formal TODOS los enunciados aritméticos verdaderos. El programa tendiente a formalizar por completo la aritmética jamás podrá llevarse a cabo. El teorema de Gödel nos coloca ante un enunciado indecidible que la intuición reconoce como verdadero. En todo caso los criterios formales de deducibilidad fracasan ante las proposiciones indecidibles. Podemos decir que en esta clase de sistemas lo deducible no coincide con lo (intuitivamente) verdadero: La sintaxis no coincide con la semántica. [4]

---

[4] Para algunos autores el teorema de Gödel permite hablar de una primacía del criterio material sobre el criterio formal de verdad: la indecidibilidad de una proposición aritmética contrasta con la posibilidad de resolverla intuitivamente. Lo que es un hecho es que el teorema elimina la pretensión del formalismo extremo que privilegia la sintaxis como único criterio de verdad. A partir de Gödel sabemos que ningún formalismo agota los contenidos de la Aritmética, siendo ésta más rica.

IV.5.- Teorema de Gödel-Rosser

En la demostración del teorema de Gödel es necesario asumir una hipótesis más poderosa que la de consistencia simple: la ω-consistencia. Esto de suyo plantea el problema de si la incompletud de la Aritmética Formal se sigue de su sóla consistencia. Históricamente, este problema fue resuelto por J.B. Rosser en 1936, cuando demostró que la hipótesis de consistencia simple es suficiente. Para ello, Rosser considera un caso más complejo de fórmula indecidible.

Sea R(x) la fórmula

$$(x_1)(\sim\overline{PR}(x_1,\overline{sb}(x_2,\overline{31},\overline{nml}(x_2)))\vee\exists x_3(x_3\leq x_1\wedge\overline{PR}(x_3,\overline{neg}(\overline{sb}(x_2,\overline{31},\overline{nml}(x_2))))))$$

Sea $r=\gamma R(x_2)$. El enunciado de Rosser es la fórmula $R(\bar{r})$:

$$(x_1)(\sim\overline{PR}(x_1,\overline{sb}(\bar{r},\overline{31},\overline{nml}(\bar{r})))\vee\exists x_3(x_3\leq x_1\wedge\overline{PR}(x_3,\overline{neg}(\overline{sb}(\bar{r},\overline{31},\overline{nml}(\bar{r}))))))$$

Desde la perspectiva de la aritmetización de la sintaxis, $R(\bar{r})$ se interpreta como el enunciado que afirma que para cualquier prueba de $R(\bar{r})$ en $\mathcal{AR}$ hay una prueba de $\sim R(\bar{r})$ con un número de secuencia menor o igual al de aquélla. Dice, en otras palabras, que si ella es derivble, también su negación lo es y tiene una prueba con menor número de secuencia.

Hacemos uso de las siguientes abreviaturas:

$P(x,y) \rightsquigarrow PR(x, sb(y, 31, nml(y)))$
$PN(x,y) \rightsquigarrow PR(x, neg(sb(y, 31, nml(y))))$

en conformidad, $R(\bar{r})$ y $\sim R(\bar{r})$ se escriben

$$R(\bar{r})\equiv(x_1)(\sim\bar{P}(x_1,\bar{r})\vee\exists x_3(x_3\leq x_1\wedge\overline{PN}(x_3,\bar{r})))$$
$$\sim R(\bar{r})\equiv\exists x_1(\bar{P}(x_1,\bar{r})\wedge(x_3)(x_3\leq x_1\rightarrow\sim\overline{PN}(x_3,\bar{r})))$$

<u>Teorema de incompletud de Gödel-Rosser</u>.- Si $\mathcal{AR}$ es consistente, entonces $R(\bar{r})$ es un enunciado indecidible en el sistema.

Demostración

La demostración se divide en dos partes:

a) Si $\mathcal{AR}$ es consistente, entonces $\nvdash R(\bar{r})$
b) Si $\mathcal{AR}$ es consistente, entonces $\nvdash \sim R(\bar{r})$

en ambas se procede por reducción al absurdo.

(a) Supóngase que $\mathcal{AR}$ es consistente y que $\vdash R(\bar{r})$

Como $R(\bar{r})$ es un teorema, existe $k\in\mathbb{N}$ tal que $P(k,r)$.
Como $\sim R(\bar{r})$ no es un teorema (por consistencia), $PN(n,r)$ es falso para todo $n\in\mathbb{N}$. En consecuencia los enunciados aritméticos

$$P(k,r), \neg PN(0,r), \neg PN(1,r), \ldots, \neg PN(k,r)$$

son verdaderos. Dado que se trata de relaciones recursivas, éstas son expesables en AR. Tenemos la siguiente prueba:

	.....	
h.–	$\bar{P}(\bar{k},\bar{r})$	TEO prop. 14
	.....	...
	$\sim\overline{PN}(\bar{0},\bar{r})$	TEO prop. 14
	.....	...
	$\sim\overline{PN}(\bar{k},\bar{r})$	TEO prop. 14
	.....	...
n.–	$\sim\overline{PN}(\bar{0},\bar{r})\wedge\ldots\wedge\sim\overline{PN}(\bar{k},\bar{r})$	conjunción...
	.....	...
n+m.–	$\sim\overline{PN}(\bar{0},\bar{r})\wedge\ldots\wedge\sim\overline{PN}(\bar{k},\bar{r})\rightarrow(x_2)(x_2\leq\bar{k}\rightarrow\sim\overline{PN}(x_2,\bar{r}))$	Teo [27]
n+m+1.–	$(x_2)(x_2\leq\bar{k}\rightarrow\sim\overline{PN}(x_2,\bar{r}))$	MP n,n+m
n+m+2.–	$\bar{P}(\bar{k},\bar{r})\wedge(x_2)(x_2\leq\bar{k}\rightarrow\sim\overline{PN}(x_2,\bar{r}))$	conjunción h,n+m+1
n+m+3.–	$\exists x_1(\bar{P}(x_1,\bar{r})\wedge(x_2)(x_2\leq x_1\rightarrow\sim\overline{PN}(x_2,\bar{r})))$	($\exists$) a n+m+2

Concluimos que si AR es consistente y $\vdash R(\bar{r})$, entonces $\vdash\sim R(\bar{r})$, lo cual es un absurdo. En consecuencia, $\nvdash R(\bar{r})$ lcqd.

(b) Supongamos que AR es consistente y que $\vdash\sim R(\bar{r})$.

Como $\sim R(\bar{r})$ es un teorema, hay una $k\in\mathbb{N}^+$ tal que $PN(k,r)$.
Como $R(\bar{r})$ no es un teorema (por consistencia), $P(n,r)$ es falso para todo $n\in\mathbb{N}$. En consecuencia los enunciados aritméticos

$$PN(k,r),\neg P(0,r),\neg P(1,r),\ldots,\neg P(k-1,r)$$

son verdaderos. Como se trata de relaciones recursivas, éstas son representables en AR:

	.....	
h.–	$\overline{PN}(\bar{k},\bar{r})$	TEO prop. 14
	.....	...
	$\sim\bar{P}(\bar{0},\bar{r})$	TEO prop. 14
	.....	...
	$\sim\bar{P}(\overline{k-1},\bar{r})$	TEO prop. 14
	.....	...
n.–	$\sim\bar{P}(\bar{0},\bar{r})\wedge\ldots\wedge\sim\bar{P}(\overline{k-1},\bar{r})$	conjunción...
	.....	...
n+m.–	$\sim\bar{P}(\bar{0},\bar{r})\wedge\ldots\wedge\sim\bar{P}(\overline{k-1},\bar{r})\rightarrow(x_1)(x_1<k\rightarrow\sim\bar{P}(x_1,\bar{r}))$	TEO [30]
n+m+1.–	$(x_1)(x_1<k\rightarrow\sim\bar{P}(x_1,\bar{r}))$	MP n,n+m
n+m+2.–	$\overline{PN}(\bar{k},\bar{r})\rightarrow(x_1)(\bar{k}\leq x_1\rightarrow\exists x_2(x_2\leq x_1\wedge\overline{PN}(x_2,\bar{r})))$	TEO [28]
n+m+3.–	$(x_1)(\bar{k}\leq x_1\rightarrow\exists x_2(x_2\leq x_1\wedge\overline{PN}(x_2,\bar{r})))$	MP h,n+m+2
n+m+4.–	$(x_1)(\sim\bar{P}(x_1,\bar{r})\vee\exists x_2(x_2\leq x_1\wedge\overline{PN}(x_2,\bar{r})))$	CL n+m+1,n+m+3 y TEO [29]

Concluimos que si AR es consistente y $\vdash\sim R(\bar{r})$, entonces $\vdash R(\bar{r})$, lo cual constituye un absurdo. En consecuencia $\nvdash\sim R(\bar{r})$ lcqd. ■

IV.6.– Comentarios adicionales

1.– El teorema de incompletud de Gödel–Rosser no se limita al sistema AR. En realidad es aplicable a un gran número de sistemas formales basados en el Cálculo de Predicados de primer orden. Del análisis de la demostración se concluye que cualquier sistema formal SF que satisfaga las siguientes condiciones será objeto de su aplicación:

1°) Las nociones de *axioma*, *consecuencia inmediata* y *prueba* de SF son recursivas.

2°) Toda relación recursiva es expresable en SF y toda función recursiva es representable en SF (en breve: SF contiene una representación de la Aritmética Recursiva).

3°) La operación de *substituir todas las ocurrencias libres de una variable por un término* es recursiva.

4°) Para todas las fórmulas $A(x)$ y $B(x) \in L_{ar}$ y para todo $k \in \mathbb{N}$ son teoremas de SF las siguientes fórmulas:

$$A(\bar{0}) \wedge \ldots \wedge A(\bar{k}) \rightarrow (x)(x \leq \bar{k} \rightarrow A(x))$$

$$A(\bar{k}) \rightarrow (x)(\bar{k} \leq x \rightarrow \exists y(y \leq x \wedge A(y)))$$

$$A(\bar{0}) \wedge \ldots \wedge A(\overline{k-1}) \rightarrow (x)(x < \bar{k} \rightarrow A(x))$$

$$((x)(x \leq y \rightarrow A(x)) \wedge (x)(y < x \rightarrow B(x))) \rightarrow (x)(A(x) \vee B(x))$$

Cosas similares se pueden afirmar en relación al teorema de Gödel. Si un sistema formal SF satisface estas cuatro condiciones, entonces de su consistencia se sigue su incompletud.

2.– Si el teorema de Gödel–Rosser se aplica a un sistema formal SF, también se aplica a todas extensiones recursivamente axiomatizables.

3.– Hay una versión semántica del Teorema de Gödel.

Supongase que el sistema AR es *correcto* en el sentido de que todos sus teoremas son verdaderos en la Aritmética. ..... (1)

$G(\bar{g})$ corresponde al enunciado aritmético $(x_1){\sim}PR(x_1, sb(g, 31, nml(g)))$ que, a su vez, corresponde al enunciado metateórico <*La fórmula* $G(\bar{g})$ *no es derivable en* AR>.

En otras palabras, $G(\bar{g})$ corresponde al enunciado metateórico <$G(\bar{g})$ *no es un teorema de* AR>. ..... (2)

Si $\vdash G(\bar{g})$, entonces (2) es falso, lo cual contradice (1).

${\sim}G(\bar{g})$ corresponde al enunciado aritmético $\exists x PR(x, sb(g, 31, nml(g)))$ que, a su vez, corresponde al enunciado metateórico <*La fórmula* $G(\bar{g})$ *es derivable en* AR>.

En otras palabras, ${\sim}G(\bar{g})$ corresponde al enunciado metateórico <$G(\bar{g})$ *es un teorema de* AR>. ..... (3)

Si $\vdash {\sim}G(\bar{g})$, entonces (3) es verdadero y $\vdash G(\bar{g})$.

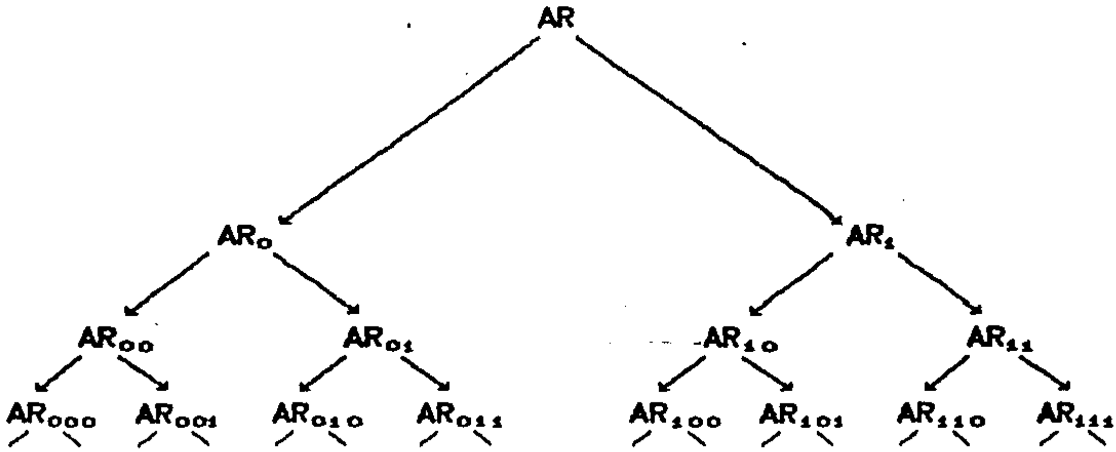
Conclusión: si AR es consistente y correcto, entonces $G(\bar{g})$ es indecidible.

4.- Si AR esconsistente, entonces el enunciado de Rosser $R(\bar{r})$ es indecidible. No obstante, en la metateoría se puede decidir si $R(\bar{r})$ es falso o verdadero (bajo la hipótesis de consistencia $R(\bar{r})$ es verdadero).

Al ser $R(\bar{r})$ indecidible, las extensiones $AR_0=AR\cup\{R(\bar{r})\}$ y $AR_1=AR\cup\{\sim R(\bar{r})\}$ son consistentes. Como las propiedades <*ser axioma de* AR_0> y <*ser axioma de* AR_1> son recursivas, ambos sistemas son incompletos. Hay un enunciado R_0 indecidible en AR_0 y un enunciado R_1 indecidible en AR_1. Ahora de definen sendas parejas de extensiones como sigue:

$$AR_{00}=AR_0\cup\{R_0\} \quad ; \quad AR_{01}=AR_0\cup\{\sim R_0\}$$
$$AR_{10}=AR_1\cup\{R_1\} \quad ; \quad AR_{11}=AR_1\cup\{\sim R_1\}$$

De nuevo estos cuatro sistemas formales son consistentes e incompletos. Prosiguiendo de la misma manera se pueden construir un número ilimitado de extensiones propias de AR todas ellas consistentes e incompletas. El patrón se representa en el diagrama siguiente:



i) Toda sucesión finita de ceros y unos representa una extensión de AR. Por ejemplo, 100010 representa a la extensión AR_{100010}.

ii) Si una sucesión de dígitos $d_1\ldots d_n$ contiene un uno, entonces en $AR_{d_1\ldots d_n}$ hay teoremas que son aritméticamente falsos.

iii) Para toda sucesión finita de ceros 0...0, los teoremas de la extensión $AR_{00\ldots 0}$ son aritméticamente ciertos (bajo la suposición de que AR es *correcto*).

iv) Sea $d_1\ldots d_n$ una sucesión que contiene al menos un uno. Como $AR_{d_1\ldots d_n}$ es consistente, tiene un modelo. Este es esencialmente distinto a la Aritmética usual (estandar). Es lo que se llama un modelo *no estandar*. Siendo modelo de $AR_{d_1\ldots d_n}$ también lo es de AR. Esto demuestra que AR no es *α–categórico* para ningún cardinal $\alpha\geq\aleph_0$.

5.- La conclusión última a la que se llega es que la Teoría Aritmética $T(N)$ no es axiomática, es decir, no se le puede caracterizar a través de un formalismo consistente y completo.

CAPITULO V

PRUEBAS DE CONSISTENCIA. SEGUNDO TEOREMA DE GÖDEL

En este capítulo demostramos que ciertos enunciados que a la luz de la codificación afirman la consistencia de AR, son inderivables en AR. Este teorema, debido a Gödel, nos muestra en su forma general que nuestras teorías formales de primer orden sufren una severa limitación cuando se trata de comprobar su consistencia.

Gödel, al igual que muchos otros expositores, no demuestra su segundo teorema. En vez de ello se limita a ofrecer algunas indicaciones sobre el modo de hacerlo. Aunque inexacto en cuanto al procedimiento a seguir, en su relato deja entrever las consideraciones que lo llevaron a su hallazgo. Son las siguientes:

En el primer teorema de Gödel se establece que

Si [EL SISTEMA ES CONSISTENTE], entonces [$G(\bar{g})$ ES INDERIVABLE] (*)

Si una demostración de la consistencia del sistema nos fuese dada, prefijándola a la anterior (es decir, a la demostración de (*)) se completaría una demostración de la inderivabilidad de $G(\bar{g})$. Después, usando la representación de fórmulas por números de Gödel, podríamos expresarla como una demostración de la Aritmética Informal. ¿Sería posible formalizar dicha demostración? Si tal fuese el caso, la fórmula $G(\bar{g})$ sería la formalización de lo que se demuestra:

$$\overset{\text{Metateoría}}{\boxed{G(g) \text{ es inderivable en AR}}} \xrightarrow{\text{formalización}} \overset{\text{Teoría AR}}{\boxed{G(g)}}$$

Conclusión: una demostración formalizada de [$G(\bar{g})$ ES INDERIVABLE] sería una prueba de $G(\bar{g})$. Como sabemos, tal prueba no puede existir en caso de que el sistema sea consistente (primer teorema de Gödel).

Con base en lo antes dicho podemos decir que si la parte

Si [EL SISTEMA ES CONSISTENTE], entonces [$G(\bar{g})$ ES INDERIVABLE] (*)

se formaliza en el sistema, entonces la parte

[EL SISTEMA ES CONSISTENTE]

no puede, a su vez, ser formalizada (supuesta la consistencia de AR). Esto da lugar al procedimiento sugerido por Gödel: *en principio*, demostrar que la demostración de (*) es formalizable en AR. decimos "*en principio*" porque en la práctica lo que sucede es algo distinto: Si CON es una fórmula que a la luz de la codificación de Gödel expresa la consistencia de AR, entonces se demuestra que

$$\vdash CON \rightarrow G(\bar{g}) \qquad (**)$$

Esto último tiene como consecuencia directa al Segundo Teorema de Gödel, a saber, que

Si AR es consistente, entonces $\nvdash CON$.

En particular, Gödel selecciona como enunciado de consistencia a la fórmula

$$CON \equiv \exists x_2(\overline{FORM}(x_2) \wedge (x_1) \sim \overline{PR}(x_1, x_2))$$

(hay una fórmula que no es teorema). Nótese que la fórmula en (**) expresa al enunciado (*) en caso de que CON exprese adecuadamente la noción de consistencia.

En la primera parte de este capítulo demostramos que bajo ciertas condiciones específicas (existencia de un *predicado de prueba*), la consistencia del sistema es inderivable. Esto se hace de un modo general y en relación a cualquier predicado $P(x_0)$ que corresponda a la propiedad sintáctica <x_0 es un *teorema*>. En la parte final demostramos que cierto predicado $TEO(x_0)$ (que en breve definiremos) satisface las condiciones impuestas a $P(x_0)$ y, en consecuencia, le es aplicable el segundo teorema de Gödel.

V.1.- Predicados de prueba

A través de la codificación cada fórmula A tiene asociado un único número de Gödel γA. Si ahora consideramos el numeral $\overline{\gamma A}$ tenemos un nombre (un código) para la fórmula en AR. Este término desempeña un papel tan importante en lo que haremos, que resulta conveniente denotarlo de un modo especial.

<u>Definición</u>.- Sea E una expesión de AR. Se define $\ulcorner E \urcorner$ (el nombre de E) a través de la igualdad

$$\ulcorner E \urcorner = \overline{\gamma E}$$ [1]

<u>Definición</u>.- *Una fórmula* $P(x_0)$ *cuya única variable libe es* x_0 *se dice que es un* *predicdo de prueba* para un sistema SF, si para toda pareja de enunciados A y B se cumplen las siguientes condiciones:

D_1.- Si $\vdash_{SF} A$, entonces $\vdash_{SF} P(\ulcorner A \urcorner)$.

D_2.- $\vdash_{SF} P(\ulcorner A \urcorner) \rightarrow P(\ulcorner P(\ulcorner A \urcorner) \urcorner)$.

D_3.- $\vdash_{SF} (P(\ulcorner A \rightarrow B \urcorner) \wedge P(\ulcorner A \urcorner)) \rightarrow P(\ulcorner B \urcorner)$.

A D_1, D_2 y D_3 se les llama *condiciones de derivación* de Hilbert y Bernays.

Si pensamos que la fórmula $P(\ulcorner A \urcorner)$ "dice" <A *es* un *teorema de* SF>, entonces las condiciones de derivación adquieren el siguiente sentido:

D_1.- Cada vez que una fórmula A es un teorema, se prueba en el sistema formal la fórmula que eso afirma.

D_2.- Formalización del enunciado metateórico D_1.

---

[1] $\ulcorner\ \urcorner$ define un mapeo que a cada expresión E le asocia un término cerrado, aún cuando E contenga variables. Si, por ejemplo, una fórmula A(x) contiene libre a la variable "x", eso no hace de $\ulcorner A(x) \urcorner$ un término abierto. Al codificar, la variable "x" en A(x) es vista como un objeto sintáctico, no como un parámetro.

D_3.- Formalización del enunciado "Si $\vdash_{SF} A \rightarrow B$ y $\vdash_{SF} A$, entonces $\vdash_{SF} B$".

Las condiciones de derivción son necesarias (más no suficientes) para afirmar que un predicado $P(x_o)$ expresa adecuadamente en SF la noción de <*ser un teorema de* SF>.

En el caso del sistema AR el predicado $P(x_o)$ es la fórmula

$$TEO(x_o) \equiv \exists x_1 \overline{PR}(x_1, x_o)$$

Por su construcción, $\overline{PR}(x_1, x_o)$ es una transcripción de la definición de "*prueba de...*" al lenguaje de AR. En consecuencia, $TEO(x_o)$ transcribe la idea de que x_o es el número de Gödel de una fórmula derivable (un teorema). Como veremos más adelante, se trata de un *predicado de prueba* para AR. Por el momento asumimos este hecho como una hipótesis.

Hipótesis (que demostraremos más adelante): $TEO(x_o)$ satisface las condiciones de derivación D_1, D_2 y D_3 de Hilbert y Bernays.

V.2.- Lema diagonal

Demostramos en esta sección un teorema de punto fijo (conocido como *lema diagonal*) que ocupa un lugar de importancia el la consecución de otros resultados en este capítulo.

Proposición 15 (lema diagonal).- Si $A(x_k) \in L_a$ y $VL(A)=\{x_k\}$, entonces existe un enunciado (*fórmula sin variables libres*) $B \in L_a^o$ tal que $\vdash B \leftrightarrow A(\overline{\ulcorner B \urcorner})$.

Demostración

Considerese la función diagonal $diag_k(x)=sb(x, 23+4k, nml(x))$ definida en el capítulo IV. Esta función es recursiva primitiva y con la propiedad siguiente: si $a=\gamma A(x_k)$, entonces $diag_k(a)=\gamma A(\bar{a})$.

Sea $\beta(x_k)=A(\overline{diag_k}(x_k))$ y $b=\gamma\beta(x_k)$.
Sea, finalmente, $B=\beta(\bar{b})$.

Se afirma que B es la fórmula buscada. Veamos:

$$\begin{aligned} diag_k(b) &= \gamma\beta(\bar{b}) && \text{(por definición de } diag_k) \\ &= \gamma A(\overline{diag_k}(\bar{b})) && \text{(por definición de } \beta(x_k)) \\ &= \gamma B && \text{(por definición de B)} \end{aligned}$$

como $diag_k$ es representable en AR, tenemos la siguiente derivación:

1.- $\overline{diag_k}(\bar{b})=\overline{\ulcorner B \urcorner}$	Proposición 10
2.- $\overline{diag_k}(\bar{b})=\overline{\ulcorner B \urcorner} \rightarrow (A(\overline{diag_k}(\bar{b}) \leftrightarrow A(\overline{\ulcorner B \urcorner}))$	Teo [5]
3.- $(A(\overline{diag_k}(\bar{b}) \leftrightarrow A(\overline{\ulcorner B \urcorner}))$	MP 1,2
4.- $B \leftrightarrow A(\overline{\ulcorner B \urcorner})$	por definición, $B=A(\overline{diag_k}(\bar{b}))$.

Se concluye que $\vdash B \leftrightarrow A(\overline{\ulcorner B \urcorner})$ (B es un punto fijo de $A(x_k)$). ■

La proposición 15 también es llamada *de la autorreferencia*, pues B resulta ser equivalente a una fórmula que "habla" de ella. Por ejemplo, si $A(x_k)$ es la fórmula $\overline{Ax}(x_k)$ (x_k es un axioma de AR) y $\vdash B \leftrightarrow \overline{Ax}(\ulcorner B \urcorner)$, entonces B es equivalente a una fórmula que a la luz de la codificación afirma "B es un axioma de AR". Es en este sentido que B es autorreferente.

¿Qué sucede cuando se aplica el lema diagonal a las fórmulas $TEO(x_o)$ y $\sim TEO(x_o)$? Se determinan dos enunciados D y G tales que $\vdash D \leftrightarrow TEO(\ulcorner D \urcorner)$ y $\vdash G \leftrightarrow \sim TEO(\ulcorner G \urcorner)$. El segundo de ellos corresponde al enunciado de Gödel, mientras que el primero corresponde a un enunciado que afirma ser uno de los teoremas de AR. ¿Será en realidad un teorema? Para responder a ésta y otras interrogantes vamos a demostrar un teorema debido a Löb que tiene como consecuencia la inderivabilidad de la consistencia de AR en AR.

V.3.- El teorema de Löb

<u>Proposición 16</u> (teorema de Löb).- Si $A \in L^*_a$ y $\vdash TEO(\ulcorner A \urcorner) \to A$, entonces $\vdash A$.

Demostración

Hacemos uso de la siguiente función recursiva primitiva:

$spvl(x,k)=x$ si $\forall v(v \le x \Rightarrow \neg \exists n(1 \le n \le l(x)\ \&\ LIB(v,n,x)))$

$spvl(x,k)=sb(x,h,k)$ si $h=\mu v(v \le x\ \&\ \exists n(1 \le n \le l(x)\ \&\ LIB(v,n,x)))$

$spvl(x,k)$: substituir la primer variable libre de x por k. $spvl(x,k)$ es la fórmula que se obtiene al reemplazar en x todas las ocurrencias libres de la primera variable de la lista $x_o,\ldots,x_n,\ldots$ que ocurra libre en x por k. Esta función tiene la siguiente propiedad:

$$spvl(\gamma A(x),k)=\gamma A(\bar{k}) \qquad \text{cuando } VL(A)=\{x\}.$$

Sean $p=\gamma[\,TEO(\overline{spvl}(x_o,x_o)) \to A]$
 y $B \equiv TEO(\overline{spvl}(\bar p,\bar p)) \to A$. [2]

Por el modo como se definió B, $\gamma B=spvl(p,p)$. Tenemos la siguiente prueba en AR:

1.- $\overline{spvl}(\bar p,\bar p)=\ulcorner B \urcorner$	proposición 10
2.- $\overline{spvl}(\bar p,\bar p)=\ulcorner B \urcorner \to ([\,TEO(\overline{spvl}(\bar p,\bar p)) \to A] \to [\,TEO(\ulcorner B \urcorner) \to A])$	proposición 5
3.- $[\,TEO(\overline{spvl}(\bar p,\bar p)) \to A] \to [\,TEO(\ulcorner B \urcorner) \to A]$	MP 1,2
4.- $B \to [\,TEO(\ulcorner B \urcorner) \to A]$	lo mismo que 3
5.- $TEO(\ulcorner B \to (TEO(\ulcorner B \urcorner) \to A) \urcorner)$	D_1 a 4
6.- $TEO(\ulcorner B \to (TEO(\ulcorner B \urcorner) \to A) \urcorner) \to (TEO(\ulcorner B \urcorner) \to TEO(\ulcorner TEO(\ulcorner B \urcorner) \to A \urcorner))$	D_2
7.- $TEO(\ulcorner B \urcorner) \to TEO(\ulcorner TEO(\ulcorner B \urcorner) \to A \urcorner)$	MP 5,6
8.- $TEO(\ulcorner TEO(\ulcorner B \urcorner) \to A \urcorner) \to (TEO(\ulcorner TEO(\ulcorner B \urcorner) \urcorner) \to TEO(\ulcorner A \urcorner))$	D_2
9.- $TEO(\ulcorner B \urcorner) \to (TEO(\ulcorner TEO(\ulcorner B \urcorner) \urcorner) \to TEO(\ulcorner A \urcorner))$	trans $\to$ 7,8

---

[2] B "dice": Si B es un teorema, entonces A.

10.–	$\mathrm{TEO}(\ulcorner B\urcorner)\rightarrow\mathrm{TEO}(\ulcorner\mathrm{TEO}(\ulcorner B\urcorner)\urcorner)$.	D_2
11.–	$\mathrm{TEO}(\ulcorner B\urcorner)\rightarrow\mathrm{TEO}(\ulcorner A\urcorner)$	CL 9,10: $A\rightarrow(B\rightarrow C), A\rightarrow B/A\rightarrow C$
12.–	$\mathrm{TEO}(\ulcorner A\urcorner)\rightarrow A$	TEO (por hipótesis)
13.–	$\mathrm{TEO}(\ulcorner B\urcorner)\rightarrow A$	trans $\rightarrow$ 11,12
14.–	$\mathrm{TEO}(\overline{\mathrm{spv1}(\bar{p},\bar{p})})\rightarrow A$	sub= 1,13
15.–	B	lo mismo que 14
16.–	$\mathrm{TEO}(\ulcorner B\urcorner)$	D_1 a 15
17.–	A	MP 13,16 lcqd. ∎

Corolario 1.– $\{A \mid A\in L^{\circ}_{a} \text{ y } \vdash A\}=\{A \mid A\in L^{\circ}_{a} \text{ y } \vdash\mathrm{TEO}(\ulcorner A\urcorner)\leftrightarrow A\}$.

Corolario 2 (segundo teorema de Gödel).– Si $A\in L^{\circ}_{a}$, $\vdash A$ y AR es consistente, entonces $\nvdash\sim\mathrm{TEO}(\ulcorner\sim A\urcorner)$.

Demostración

Procedemos por reducción al absurdo.

1.–	$\sim\mathrm{TEO}(\ulcorner\sim A\urcorner)$	TEO (por hipótesis)
2.–	$\sim\mathrm{TEO}(\ulcorner\sim A\urcorner)\rightarrow(\mathrm{TEO}(\ulcorner\sim A\urcorner)\rightarrow\sim A)$	TAUT.
3.–	$\mathrm{TEO}(\ulcorner\sim A\urcorner)\rightarrow\sim A$	MP 1,2
4.–	$\sim A$	Proposición 16 a 3
5.–	A	TEO (por hipótesis)

y AR es inconsistente. ∎

La fórmula $\sim\mathrm{TEO}(\ulcorner\sim A\urcorner)$ afirma, a la luz de la codificación, que AR es consistente al "decir" (*La negación de un teorema no es un teorema*). Es así que se tiene que ciertos enunciados que de un modo natural afirman la consistencia de AR no son derivables cuando el sistema es consistente.

Volveremos a este resultado en la siguiente sección, dando una segunda demostración de él en la que se pone de manifiesto su relación con el primer teorema de incompletud.

Corolario 3.– Si $D\in L^{\circ}_{a}$ y $\vdash D\leftrightarrow\mathrm{TEO}(\ulcorner D\urcorner)$, entonces $\vdash D$.

Por el lema diagonal sabemos que tal D existe. Este enunciado afirma, a la luz de la codificación, ser derivable en AR. Como sí es un teorema de AR, es verdadero. El enunciado de Gödel $G(\bar{g})$ también es verdadero (suponiendo que el sistema es consistente), pero a diferencia de éste no es derivable.

El teorema de Löb está relacionado no sólo con las pruebas de consistencia de AR, sino con las de algunas de sus extensiones. Sea $A\in L^{\circ}_{a}$ y $SF=AR\cup\{\sim A\}$. * En conexión con esta fórmula tenemos la siguiente cadena de equivalencias:

---

* SF tiene como axiomas los de AR más el enunciado $\sim A$. Las reglas de inferencia son las mismas que en AR.

(*) $\vdash TEO(\overline{A}) \rightarrow A \Leftrightarrow \vdash \sim A \rightarrow \sim TEO(\overline{A}) \Leftrightarrow \sim A \vdash \sim TEO(\overline{A}) \Leftrightarrow \vdash_{SF} \sim TEO(\overline{A})$.

$\Updownarrow$ Lob

(**) $\vdash A \Leftrightarrow AR \cup \{\sim A\}$ es inconsistente $\Leftrightarrow$ SF es inconsistente.

El enunciado $\sim TEO(\overline{A})$ afirma, a la luz de la codificación, que A no es un teorema de AR. De acuerdo a (**) ello equivale a la afirmación de que SF es consistente. Con base en lo anterior, es natural que llamemos a $\sim TEO(\overline{A})$ *la consitencia de* SF. Ahora bien, el teorema de Lob es el eslabón que une a las cadenas (*) y (**). Comparando los extremos tenemos el siguiente

<u>Corolario 4</u>.- SF es consistente $\Leftrightarrow\ \nvdash_{SF} \sim TEO(\overline{A})$.

Paráfrasis: la consistencia de SF es derivable en SF si y sólo si SF es inconsistente. En este contexto la consistencia de AR es un caso particular: basta con tomar un enunciado A cuya negación sea un teorema de AR.

V.4.- Los teoremas de Gödel

<u>Proposición 17</u>.- Si AR es ω-consistente y $\vdash TEO(\overline{A})$, entonces $\vdash A$.

Demostración

Supóngase que $\nvdash A$. En tal caso los enunciados $\neg PR(0, \overline{A}), \ldots, \neg PR(k, \overline{A})$, etc. son verdaderos. Como $\sim \overline{PR}(x_1, x_2)$ repesenta a esta relación en AR tenemos que $\vdash \sim \overline{PR}(\bar{0}, \overline{A}), \ldots, \vdash \sim \overline{PR}(\bar{k}, \overline{A})$, etc. Como por hipótesis el sistema es ω-consistente, $\nvdash \exists x_1 \overline{PR}(x_1, \overline{A})$ (es decir, $\nvdash TEO(\overline{A})$). Por contraposición en la metateoría se obtiene el resultado esperado. ■

<u>Proposición 18</u> (primer teorema de Gödel).- Sea G tal que $\vdash G \leftrightarrow \sim TEO(\overline{G})$ [4]

a) Si AR es consistente, entonces $\nvdash G$.
b) Si AR es ω-consistente, entonces $\nvdash \sim G$.

Demostración

(a) Procedemos por contraposición en la metateoría. Supóngase que $\vdash G$. Vamos a inferir de ello que AR es inconsistente.

1.- G	TEO (por hipótesis)
2.- $G \rightarrow \sim TEO(\overline{G})$	Por definición de G (lema diagonal)
3.- $\sim TEO(\overline{G})$	MP 1,2
4.- $TEO(\overline{G})$	D_1 a 1
5.- $TEO(\overline{G}) \wedge \sim TEO(\overline{G})$	adición a 3 y 4. ■

---

[4] La existencia del enunciado G está garantizada por el lema diagonal (proposición 15). G es el enunciado de Gödel.

(b) Procedemos por reducción al absurdo en la metateoría. Supongase que AR es ω-consistente y que $\vdash \sim G$.

1.– $\sim G$	TEO (por hipótesis)
2.– $\sim \mathrm{TEO}(\ulcorner G \urcorner) \rightarrow G$	TEO (por drfinición de G)
3.– $\sim G \rightarrow \mathrm{TEO}(\ulcorner G \urcorner)$	CL de 2: $\sim A \rightarrow B / \sim B \rightarrow A$
4.– $\mathrm{TEO}(\ulcorner G \urcorner)$	MP 1,3
5.– G	TEO (proposición 17 a 4)
6.– $G \wedge \sim G$	adición 1,5

Se concluye que AR es inconsistente, con lo que se contradice la hipótesis de ω-consistencia. Por lo tanto, $\nvdash \sim G$.

Sea H una fórmula cuya negación es un teorema de AR, y sea CON la fórmula $\sim \mathrm{TEO}(\ulcorner H \urcorner)$. Intuitivamente, la fórmula CON asevera la consistencia de AR. [5]

<u>Proposición 18</u>.– Si G es el enunciado de Gödel, entonces $\vdash G \leftrightarrow \mathrm{CON}$.

Demostración

$G \rightarrow \mathrm{CON}$

1.– $\sim H$	TEO (por hipótesis)
2.– $\sim H \rightarrow (H \rightarrow G)$	TAUT
3.– $H \rightarrow G$	MP 1,2
4.– $\mathrm{TEO}(\ulcorner H \rightarrow G \urcorner)$	D_1 a 3
5.– $\mathrm{TEO}(\ulcorner H \rightarrow G \urcorner) \rightarrow (\mathrm{TEO}(\ulcorner H \urcorner) \rightarrow \mathrm{TEO}(\ulcorner G \urcorner))$	D_3
6.– $\mathrm{TEO}(\ulcorner H \urcorner) \rightarrow \mathrm{TEO}(\ulcorner G \urcorner)$	MP 4,5
7.– $\sim \mathrm{TEO}(\ulcorner G \urcorner) \rightarrow \sim \mathrm{TEO}(\ulcorner H \urcorner)$	contraposición a 6
8.– $G \rightarrow \sim \mathrm{TEO}(\ulcorner G \urcorner)$	TEO (por drfinición de G)
9.– $G \rightarrow \sim \mathrm{TEO}(\ulcorner H \urcorner)$	trans→ 7,8
10.– $G \rightarrow \mathrm{CON}$	lo mismo que 9

$\mathrm{CON} \rightarrow G$

1.– $\mathrm{TEO}(\ulcorner G \urcorner) \rightarrow \mathrm{TEO}(\ulcorner \mathrm{TEO}(\ulcorner G \urcorner) \urcorner)$	D_2
2.– $G \rightarrow \sim \mathrm{TEO}(\ulcorner G \urcorner)$	TEO (por definición de G)
3.– $\mathrm{TEO}(\ulcorner G \urcorner) \rightarrow \sim G$	contraposición a 2
4.– $\mathrm{TEO}(\ulcorner \mathrm{TEO}(\ulcorner G \urcorner) \rightarrow \sim G \urcorner)$	D_1 a 3
5.– $\mathrm{TEO}(\ulcorner \mathrm{TEO}(\ulcorner G \urcorner) \rightarrow \sim G \urcorner) \rightarrow (\mathrm{TEO}(\ulcorner \mathrm{TEO}(\ulcorner G \urcorner) \urcorner) \rightarrow \mathrm{TEO}(\ulcorner \sim G \urcorner))$	D_3
6.– $\mathrm{TEO}(\ulcorner \mathrm{TEO}(\ulcorner G \urcorner) \urcorner) \rightarrow \mathrm{TEO}(\ulcorner \sim G \urcorner)$	MP 4,5
7.– $\mathrm{TEO}(\ulcorner G \urcorner) \rightarrow \mathrm{TEO}(\ulcorner \sim G \urcorner)$	trans→ 1,6

---

[5] CON se interpreta como el enunciado (H *no es un teorema de* AR). Si H es la fórmula "$\bar{1}=\bar{0}$", entonces se trata del enunciado cuya inderivabilidad Hilbert quería demostrar.

8.— $\sim G \rightarrow (G \rightarrow H)$	TAUT
9.— $TEO(\ulcorner \sim G \rightarrow (G \rightarrow H) \urcorner)$	D_1 a 8
10.— $TEO(\ulcorner \sim G \rightarrow (G \rightarrow H) \urcorner) \rightarrow (TEO(\ulcorner \sim G \urcorner) \rightarrow TEO(\ulcorner G \rightarrow H \urcorner))$	D_3
11.— $TEO(\ulcorner \sim G \urcorner) \rightarrow TEO(\ulcorner G \rightarrow H \urcorner)$	MP 9,10
12.— $TEO(\ulcorner G \rightarrow H \urcorner) \rightarrow (TEO(\ulcorner G \urcorner) \rightarrow TEO(\ulcorner H \urcorner))$	D_3
13.— $TEO(\ulcorner \sim G \urcorner) \rightarrow (TEO(\ulcorner G \urcorner) \rightarrow TEO(\ulcorner H \urcorner))$	trans$\rightarrow$ 11,12
14.— $TEO(\ulcorner G \urcorner) \rightarrow (TEO(\ulcorner G \urcorner) \rightarrow TEO(\ulcorner H \urcorner))$	trans$\rightarrow$ 7,13
15.— $TEO(\ulcorner G \urcorner) \rightarrow TEO(\ulcorner H \urcorner)$	CL 14: $A \rightarrow (A \rightarrow B) / A \rightarrow B$
16.— $\sim TEO(\ulcorner H \urcorner) \rightarrow \sim TEO(\ulcorner G \urcorner)$	contraposición a 15
17.— $\sim TEO(\ulcorner G \urcorner) \rightarrow G$	TEO (por definición de G)
18.— $\sim TEO(\ulcorner H \urcorner) \rightarrow G$	trans$\rightarrow$ 16,17
19.— $CON \rightarrow G$	lo mismo que 18. ■

<u>Proposición 20</u> (segundo teorema de Gödel).— Si AR es consistente, entonces $\nvdash CON$.

<u>Corolario 5</u>.— $\vdash CON \rightarrow \sim TEO(\ulcorner CON \urcorner)$.

Demostración

1.— $CON \rightarrow G$	TEO (proposición 19)
2.— $G \rightarrow \sim TEO(\ulcorner G \urcorner)$	TEO (por drfinición de G)
3.— $CON \rightarrow \sim TEO(\ulcorner G \urcorner)$	trans$\rightarrow$ 1,2
4.— $TEO(\ulcorner CON \rightarrow G \urcorner)$	D_1 a 1
5.— $TEO(\ulcorner CON \rightarrow G \urcorner) \rightarrow (TEO(\ulcorner CON \urcorner) \rightarrow TEO(\ulcorner G \urcorner))$	D_3
6.— $TEO(\ulcorner CON \urcorner) \rightarrow TEO(\ulcorner G \urcorner)$	MP 4,5
7.— $\sim TEO(\ulcorner G \urcorner) \rightarrow \sim TEO(\ulcorner CON \urcorner)$	contraposición a 6
8.— $CON \rightarrow \sim TEO(\ulcorner CON \urcorner)$	trans$\rightarrow$ 3,7 ■

El corolario 5 es la formalización de la proposición 20 (segundo teorema de incompletud). Según vimos en la sección precedente, $\sim TEO(\ulcorner CON \urcorner)$ es la consistencia de $AR \cup \{\sim CON\}$. En consecuencia, en AR se prueba formalmente que <*si* AR *es consistente, entonces* $AR \cup \{\sim CON\}$ *es consistente*>.

Antes de cerrar esta sección haremos algunas observaciones en torno a las proposiciones hasta aquí expuestas:

1.— En la demostración del Primer Teorema de Gödel no se recurre a D_2 o D_3. Por lo tanto, la demostración de que $TEO(x_0)$ satisface D_1 es suficiente para estabecer la validez de la proposición 18.

2.— La demostración del Segundo Teorema de Gödel (prácticamente la proposición 19) deja ver que el enunciado de Gödel es equivalente al enunciado que asevera la consistencia de AR. Dicho enunciado es único (módulo *equivalencia formal*) y es correcto hablar de *el enunciado que afirma su inderivabilidad*.

3.— También en la metateoría son equvalentes la consistencia y la inderivabilidad de G: $\nvdash G \Leftrightarrow$ AR es consistente. Desde este punto de vista, la proposición 19 nos muestra que la formalización de éste enunciado es derivable en AR. Algunos autores confunden este hecho con el acto de transcribir la demostración de "$\nvdash G \iff$ AR *es consistente*" al interior de AR, construyendo de este modo una prueba formal del enunciado "$G \leftrightarrow CON$". Es así que J. Ladriere y E. Mendelson, entre otros, afirman:

"*...Los razonamientos que llevan a la afirmación del enunciado 3(127)* [6] *sólo hacen intervenir las proposiciones y procedimientos de demostración que pertenecen a las matemáticas clásicas. Por tanto, pueden ser formalizados el LFG. Y la proposición* $(C \rightarrow J^{*})$ [7] *puede considerarse derivable en LFG*" (J. Ladriere <u>Limitaciones internas de los formalismos</u> editorial Tecnos-Madrid 1969, pag. 179)

"*...El razonamiento metamatemático utilizado en el teorema de Gödel* [8] *puede expresarse y desarrollarse al interior de S, de modo que uno obtiene una prueba en S de* $CON_{s} \rightarrow (\dagger\dagger)$" [9] (E. mendelson <u>Introduction to Mathematical Logic</u> Van Nostrand Reinhold 1979, pag. 163).

Tales argumentos son inexactos. De hecho, la idea de *formalizar la demostración metamatemática de...* no significa nada en concreto.

Pudiera pensarse que se trata de un ejercicio de traducción: el procedimiento informal X se *traduce* en el procedimiento formal Y, el Z en el U, etc. de modo que el resultado del ejercicio fuese una prueba formal. No obstante, las cosas no son así. Lo que se hace es probar en AR fórmulas que corresponden, a través de la codificación, a enunciados metateóricos tenidos por ciertos. Empero, cada prueba sigue su propio camino, no es la calca de una demostración informal. En particular, la fórmula del segundo teorema de Gödel no se prueba *reproduciendo* en AR demostración alguna. Una exposición más precisa es ésta: A través de D_2 (que formaliza a D_1) se *imita* la demostración del Primer Teorema de Gödel en AR, creando con ello una prueba de la equivalencia formal $CON \leftrightarrow G$. De este modo, el segundo teorema se reduce al primero. En efecto, como $\vdash CON \leftrightarrow G$, el enunciado

Si AR es consistente, entonces $\nvdash CON$ (2° teorema)

se reduce a

Si AR es consistente, entonces $\nvdash G$ (1er teorema, parte (a))

Lo que no es el caso es que "*el razonamiento utilizado en el teorema de Gödel se ha expesado y desarrollado al interior de* AR". La prueba que se lleva a cabo en la proposición 19 está *sugerida* por la demostración de la proposición 18-a, pero nada más. En aquélla ciertos razonamientos específicos han cobrado *expresión* formal. Veamos algunos de ellos:

Demostración de 18-a — Prueba formal de "$CON \rightarrow G$"

$\vdash G \Rightarrow \vdash TEO(\bar{G})$ (D_1) $\xrightarrow{D_2 \text{ formaliza a } D_1}$ $TEO(\bar{G}) \rightarrow TEO(\overline{TEO(\bar{G})})$ (D_2)

...

pero $\vdash TEO(\bar{G}) \rightarrow \sim G$ $\longrightarrow$ $TEO(\overline{TEO(\bar{G}) \rightarrow \sim G})$

---

[6] El autor se refiere al enunciado $(x)\sim PR(x, diag_0(\bar{g}))$.

[7] $(C \rightarrow J^{*})$ es el análogo de la fórmula $CON \rightarrow G$

[8] El autor se refiere al Primer Teorema de incompletud.

[9] $CON_{s} \rightarrow (\dagger\dagger)$ es el análogo a $CON \rightarrow G$.

$\quad\quad\cdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \cdots$

$\therefore\ \vdash G \Rightarrow\ \vdash \sim G$ ———————————→ $TEO(\ulcorner G \urcorner) \rightarrow TEO(\ulcorner \sim G \urcorner)$

$\quad\quad\cdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \cdots$

y $\vdash G \Rightarrow\ \vdash H$ (para toda H) ———————————→ $TEO(\ulcorner G \urcorner) \rightarrow TEO(\ulcorner H \urcorner)$

Como se ve, existe un paralelismo entre la demostración del Primer Teorema de Gödel y la prueba formal que figura en el Segundo Teorema. Esta prueba se bosqueja formalizando los enunciados fundamentales que intervienen en dicha demostración. Con ello la frase "*formalizar la demostración del Primer Teorema de Gödel*" adquiere un sentido que quizá quienes la acuñaron no le quisieron dar: los pasos de la demostración al ser formalizados (es decir, traducidos en enunciados formales) indican los pasos *clave* de la prueba formal. No obstante, ésto no es lo mismo que *desarrollar el razonamiento al interior del sistema*. En la prueba formal intervienen factores y procedimientos que no provienen de nada intuitivo. No es la expresión y desarrollo de un razonamiento informal, sino que sigue sus propios cauces. Nada hay que garantice a poriori la existencia del tal prueba. En este sentido la frase antes citada ("*formalizar...*") no expresa sino el deseo de quien la profiere.

4.– La proposición 17 nos muestra que la ω–consistencia tiene como consecuencia la siguente *condición de derivación:*

D_1^*.– Si $\vdash TEO(\ulcorner A \urcorner)$, entonces $\vdash A$. (recíproco de D_1).

El hecho de que la proposición 18–b sólo requiere de D_1^* para ser demostrada deja ver que la hipótesis de ω–consistencia no es ni la óptima ni la más intuitiva. que D_1^* es más débil que la ω–consistencia se sigue hecho de que se cumple en cualquier sistema inconsistente. Esto refuerza la conjetura de que Gödel se vió forzado a asumir dicha hipótesis en su argumento al suponer que "G" no es un teorema formal.

Para evitar la hipótesis de ω–consistencia se necesita demostrar que $TEO(x_0)$ satisface D_1^*, lo cual no parece sencillo.

LLamamos *perfecto* a un predicado de prueba que satisface D_1^*. Este nombre se le otorga en virtud de que la sóla satisfación de D_1, D_2 y D_3 no es garantía de que el predicado en cuestión representa adecuadamente la noción de *teorema* en AR. Por ejemplo, el predicado $\overline{FORM}(x_0)$ satisface las condiciones D_1, D_2 y D_3 como el lector puede comprobar. Sin embargo, D_1^* no es satisfecha suponiendo que AR es consistente, pues $\vdash FORM(\ulcorner \bar{1}=\bar{0} \urcorner)$ pero $\nvdash \bar{1}=\bar{0}$. ¿Qué nos impulsa a seleccionar $TEO(x_0)$ como el predicado de prueba de AR? El hecho de que es una transcripción de la definición de *teorema* en AR.

5.– La demostración del Segundo Teorema de Gödel concluye con la demostración de que el predicado $TEO(x_0)$ satisface D_1, D_2 y D_3, cosa que haremos en el siguiente capítulo.

LAS CONDICIONES DE DERIVACION DE HILBERT Y BERNAYS

Nos proponemos demostrar las condiciones de derivación de Hilbert y Bernays. Dice *"nos proponemos"* por que la demostración se trabaja hasta cierto punto, dada la abundancia de pruebas por desarrollar.

En la literatura sobre el tema sólo se cuenta con el trabajo de Hilbert y Bernays en su libro Grundlagen der mathematic. Otros autores se limitan a dar una serie de indicaciones sobre el modo de llevarla a cabo. Dado que cubrir todos los detalles es prácticamente imposible, optamos por seguir una linea intermedia: llenar algunas lagunas al ir perfilando la demostración, aunque en forma desigual. El mayor ahínco lo ponemos en la demostración de D_3, pues ésta nos permite ahondar en la formalización de la sintaxis. En cuanto a D_2 omitimos, por larga y por no aportar nada nuevo nuestro análisis, la demostración de un lema del que se sigue en forma inmediata.

Invitamos al lector a que nos acompañe en forma activa en la tarea de *formalizar la sintaxis de* AR.[1] Trabajar sus pormenores resulta entretenido y muestra por contraste algunos elementos que intervienen desapercibidamente en los argumentos de la Aritmética Informal.

VI.1.- Preparativos

Para demostrar que $TEO(x_0)$ satisface D_2 y D_3 no es suficiente la representabilidad de las funciones recursivas en AR. Se requiere, además, expresar y probar en el sistema diversas fórmulas que corresponden a proposiciones sintácticas verdaderas. Se requiere, en otras palabras, que la representación sea correcta con variables libres, no sólo numérica. Esto incorpora la noción de *intencionalidad* en nuestro análisis.

Las *fórmulas* de AR son cadenas de signos carentes de significado, pero también son *fórmulas* aritméticas *que* expesan propiedades de los *números* y, a través de la *codificación*, definen propiedades sintácticas de los objetos de AR como *ser axioma, ser una derivación*, etc. Cuando una definición es numéricamente correcta y sólo eso, se dice que es *extensional*. Por el contrario, si de ella se derivan las propiedades generales del concepto definido se dice que es *intensional*. En este último caso lo que cuenta es que experse con plenitud la noción que define en AR. [2]

---

[1] Lo mejor es que el lector intente por cuenta propia llevar a cabo la demostración. Puede para ello confrontar sus ideas con las que aquí se exponen.

[2] *intensional* y *extensional* no son conceptos bien definidos. Más bien, son categorías que dirigen la atención hacia puntos de interes en el análisis. Aquí los incluimos por influencia del trabajo de S. Feferman Aritmetization of metamathematics in a general seting. *Fundamenta Mathematicae* 1960.

Por ejemplo, si $TEO(x_0)$ satisface D_1^M, podemos decir que es *extensionalmente* corrcta: Para todo $A\in L_0^*$, $\vdash A \Leftrightarrow \vdash TEO(\bar{A})$. Sin embargo, lo anterior no garantiza que en AR sean derivables otras características importantes de esta noción. Una de ellas es D_2, que formaliza al sguiente enunciado metateórico: Si $\vdash A \rightarrow B$ y $\vdash A$, entonces $\vdash B$. Demostrarla, en este sentido, es fortalecer la convicción de que es *intensionalmente* correcta.

Nuestro trabajo requiere demostrar que en AR son derivables fórmulas como

$$AT(x_0)\leftrightarrow\exists x_1\exists x_2(x_1, x_2<x_0\wedge TERM(x_1)\wedge TERM(x_2)\wedge x_0=\bar{2}^{\bar{1}}\bar{*}x_1\bar{*}\bar{2}^{\bar{5}}\bar{*}x_2\bar{*}\bar{2}^{\bar{1}})$$

que corresponden directamente a la proposición siguiente: A *es una fórmula atómica si y sólo si hay dos términos* t_1 *y* t_2 *tales que* $A\equiv(t_1=t_2)$.

La posibilidad de probar este tipo de fórmulas en AR tiene como base un sinnúmero de teoremas simples que *enuncian* propiedades de las operaciones y relaciones aritméticas fundamentales como son $+, \cdot, \dot{-}, \sum f$ (sumatorias), $\prod f$ (productos), $x|y$ (divisibilidad), $PRIMO(x)$ (la propiedad de ser número primo), etc. Para presentar una lista de éllos debemos hcer ciertos preparativos: demostrar algunas proposiciones útiles e introducir algunas abreviaturas que nos permitirán *captar* el sentido matemático de lo que se prueba.

VI.2.- Convenciones y abreviaturas

Letras Mayúsculas como X, Y y Z denotan sucesiones finitas de variables $x_1,\ldots,x_n$; $y_1,\ldots,y_m$ y $z_1,\ldots,z_p$.

Se utilizn como variables aritméticas las mismas variables que en AR, es decir, x_0, x_1, etc.

Al repersentar y expresar funciones y relaciones aritméticas se omite el trazo horizontal (la testa) cuando el contexto lo permite. De igual modo al escribir numerales sólo se escribe la *cifra* y se omite el trazo horizontal. Por ejemplo, se escribe

$$\vdash 2<3,\quad \vdash sg(x_0)=1\leftrightarrow x_0\geq 1 \;\text{ y }\; \vdash (x_1*x_2)*x_3=x_1*(x_2*x_3)$$

en vez de, respectivamente,

$$\vdash \bar{2}<\bar{3},\quad \vdash \overline{sg}(x_0)=\bar{1}\leftrightarrow x_0\geq \bar{1} \;\text{ y }\; \vdash (x_1\bar{*}x_2)\bar{*}x_3=x_1\bar{*}(x_2\bar{*}x_3)$$

En casos específicos se recurre a la notación que nos es familiar al escribir funciones y relaciones aritméticas, en el entendimiento de que éstas se pueden eliminar en favor de la escritura formal. Algunos ejemplos son los siguientes:

$\sum^{n} f(k) \rightsquigarrow \overline{\sigma_f}(X,n)$ (vease la definición en la página 8)

$\prod^{n} f(k) \rightsquigarrow \overline{\Psi_f}(X,n)$ (" " ")

$\mu z(z\leq f(Y)\wedge R(X,z)) \rightsquigarrow \sum_{k=0}^{fY}(\prod_{i=0}^{k}\overline{C_R}(X,i))$

$Mz(z\leq f(Y)\wedge R(X,z)) \rightsquigarrow f(Y)\dot{-}\sum_{k=0}^{fY}(\prod_{i=0}^{k}\overline{C_R}(X,f(Y)\dot{-}i))$

$fx \rightsquigarrow f(x)$.

Como primer paso demostramos una proposición que, entre otras cosas, permite derivar en AR las definiciones recursivas 25-62 del capítulo III (descripción aritmética de AR).

<u>Proposición 21</u>.- Si $P(X)$, $S(X)$ y $T(X,z)$ son relaciones recursivas primitivas, $f(Y)$ es una función recursiva primitiva y $R(X,Y)$ es la relación

a) $\neg P(X)$

b) $P(X) \vee S(X)$

c) $P(X)\ \&\ S(X)$

d) $\exists z(z \leq f(Y)\ \&\ T(X,z))$

e) $\forall z(z \leq f(Y) \Rightarrow T(X,z))$,

entonces $\overline{R}(X,Y)$ es la fórmula

a) $\sim\overline{P}(X)$

b) $\overline{P}(x) \vee \overline{S}(X)$

c) $\overline{P}(X) \wedge \overline{S}(X)$

d) $\exists z(z \leq \overline{f}(Y) \wedge \overline{T}(X,z))$

e) $(z)(z \leq \overline{f}(Y) \rightarrow \overline{T}(X,z))$

En otras palabras, $\overline{\neg P(X)} \equiv \sim\overline{P}(X)$, $\overline{P(X) \vee S(X)} \equiv \overline{P}(x) \vee \overline{S}(X), \ldots$ y $\overline{\forall z(z \leq f(Y) \Rightarrow T(X,z))} \equiv (z)(z \leq \overline{f}(Y) \rightarrow \overline{T}(X,z))$.

Demostración

Nos ocupamos únicamente de los casos (a) y (d).

(a) Sea $K=(k_1,\ldots,k_n)$. Vamos a demostrar que si $R(K)$, entonces $\vdash \sim\overline{P}(\overline{K})$ [3] y si $\neg R(K)$, entonces $\vdash \sim\sim\overline{P}(\overline{K})$.

Supóngase que $R(K)$. En tal caso:
$\neg P(K)$ (por definición de R)
$\vdash \sim\overline{P}(\overline{K})$ (por ser expresable P) lcqd.

Ahora supóngse que $\neg R(K)$. En tal caso:
$\neg\neg P(K)$ (por definición de R)
$P(K)$ (eliminación de la doble negación)
$\vdash \overline{P}(\overline{K})$ (por ser expresable P)
y $\vdash \sim\sim\overline{P}(\overline{K})$ lcqd.

(d) Supóngase que $R(H,K)$. En tal caso:
Hay una $n \in \mathbb{N}$ tal que $n \leq f(K)$ y $T(H,n)$
Como $\leq$ y T son expresables y f repesentable en AR, entonces
$\vdash \overline{n} \leq \overline{f}(\overline{K}) \wedge \overline{T}(\overline{H},\overline{n})$
y $\vdash \exists z(z \leq \overline{f}(\overline{K}) \wedge \overline{T}(\overline{H},z))$ lcqd.

Suupóngase que $\neg R(H,K)$. Vamos a demostrar que $\vdash (z)(z \leq \overline{f}(\overline{K}) \rightarrow \sim\overline{T}(\overline{H},z))$.[4]
Como $\neg\exists z(z \leq f(K)\&T(H,z))$, entonces $\neg T(H,0),\ldots,\neg T(H,f(K))$[5]

---

[3] $\overline{K}$ denota al sucesión $(\overline{k}_1 \ldots \overline{k}_n)$ de numerales. Lo mismo se cumple para la sucesión $\overline{H}$ en el inciso (d).

[4] $(z)(z \leq \overline{f}(\overline{K}) \rightarrow \sim\overline{T}(\overline{H},z)) \equiv \sim\exists z(z \leq \overline{f}(\overline{K}) \wedge \overline{T}(\overline{H},z))$

[5] Como $C_T(X,z)$ es recursiva primitiva, en cada paso se puede hacer efectivo el cálculo de que $C_T(K,i)=0$ para cada $i \leq f(K)$.

$\vdash \sim \bar{T}(\bar{A}, \bar{0}), \ldots, \vdash \sim \bar{T}(\bar{A}, \bar{f}(\bar{R}))$ (por ser expresable T)
y $\vdash (z)(z \leq \bar{f}(\bar{R}) \rightarrow \sim \bar{T}(\bar{A}, z))$ (por la proposición [27]) lcqd. ■

Esta proposición nos permite manejar directamente en AR las definiciones de diversas nociones sintácticas. Podemos, por ejemplo, escribir

$$\vdash PR(x, y) \leftrightarrow PRUEBA(x) \wedge FORM(Y) \wedge y=(x)_{l(x)}$$

o

$$\vdash MP(x, y, z) \leftrightarrow FORM(x) \wedge FORM(y) \wedge FORM(z) \wedge (y=imp(z, x) \vee z=imp(y, x))$$

VI.3.- Las condiciones de derivación

D_1

La demostración de D_1 es asaz sencilla. Sea $A \in L_a^{\circ}$ tal que $\vdash A$. En tal caso hay una prueba $A_1, \ldots, A_n$ de A. Sea $p = \gamma^2 A_1 \ldots A_n$ el número de secuencia de la prueba. Como $PR(p, \gamma A)$, por la proposición 14 (capitulo II) $\vdash \overline{PR}(\bar{p}, \bar{A})$. En consecuencia, $\vdash \exists x_1 \overline{PR}(x_1, \bar{A})$ (es decir, $\vdash TEO(\bar{A})$) lcqd. ■

D_3

Enumeramos a continuación una lista de teoremas y proposiciones relativas a los teoremas de AR. El criterio de selección es que estén relacionados con las pruebas de D_2 y D_3. El orden en que se presentan es importante en la medida en que corresponde al de precedencia formal u orden en que se prueban. Como regla, el teorema [N] puede utilizarse en la derivación del teorema [M] si y sólo si N<M. La numeración prosigue la iniciada en el capitulo II.

Proosición 22.- Si $f(x)$ es una función recursiva, entonces las siguientes fórmulas son teoremas de AR:

a) $(x)(x \leq y \rightarrow f(x)=1) \rightarrow \sum^{y} f(k)=y+1$

b) $(x)(x \leq y \rightarrow f(x)=1) \rightarrow \prod^{y} f(k)=1$

c) $x<y \rightarrow \sum^{y} f(k)=\sum^{x} f(k) + \sum_{x+1}^{y} f(k)$

d) $x<y \rightarrow \prod^{y} f(k)=\prod^{x} f(k) \cdot \prod_{x+1}^{y} f(k)$

e) $(x)(a \leq x \leq b \rightarrow f(x)=0) \rightarrow \sum_{a}^{b} f(k)=0$

f) $(x)(a \leq x \leq b \rightarrow f(x)=1) \rightarrow \prod_{a}^{b} f(k)=1$

g) $h \leq y \rightarrow \exists z(\sum^{y} f(k)=f(h)+z)$

h) $h \leq y \rightarrow \exists z(\prod^{y} f(k)=f(h) \cdot z)$

i) $f(x)=0\to(y)(x\le y\to\prod_{x}^{y}f(k)=0)$

j) $f(x)=0\to(y)(\prod_{x}^{x+y}f(k)=0)$

k) $\sum_{x}^{x+y}f(k)=0\leftrightarrow(z)(z\le y\to f(x+z)=0)$

l) $\prod_{x}^{x+y}f(k)=0\leftrightarrow\exists z(z\le y\wedge f(x+z)=0)$

m) $x\le y\wedge\sum^{y}f(k)=0\to\sum^{x}f(k)=0$

n) $x\le y\wedge\prod^{y}f(k)=1\to\prod^{x}f(k)=1$

ñ) $(x)(f(x)=1\vee f(x)=0)\to(\sum^{y}f(k)=y+1\leftrightarrow(z)(z\le y\to f(z)=1))$

<u>Proposición 23</u>.- Si $R(X,y)$ es una relación recursiva primitiva, entonces

$$\vdash y\le z\wedge R(X,y)\to\mu u(u\le z\wedge R(X,u))\ge y$$ [6]

[100] $\vdash x|y\wedge x|z\to x|ay+bz$

[101] $\vdash\sim(x=1)\wedge x|y\to\sim(x|y+1)$

[102] $\vdash x=y+z\to x\dot{-}y=z$

[103] $\vdash(x+1)\dot{-}y=z+1\to x\dot{-}y=z$

[104] $\vdash z>0\wedge x\dot{-}y=z\to x=y+z$ [7]

[105] $\vdash x\dot{-}(y+z)=(x\dot{-}y)\dot{-}z$

[106] $\vdash x\le y\to(y\dot{-}x=z\to y=x+z)$

[107] $\vdash 0\dot{-}x=0$

[108] $\vdash(x+y)\dot{-}y=x$

[109] $\vdash z(x\dot{-}1)=zx\dot{-}z$

[110] $\vdash zx\dot{-}zy=z(x\dot{-}y)$

[111] $\vdash pd(x)\le x$

[112] $\vdash x\dot{-}y\le x$

[113] $\vdash x\dot{-}x=0$

[114] $\vdash x\dot{-}y=0\to x\le y$

[115] $\vdash x<y\le x+z\to(y\dot{-}x)+x=y\wedge(y\dot{-}x)\le z$

[116] $\vdash x\le y\to y\dot{-}(y\dot{-}x)=x$.

<u>Proposición 24</u>.- Si $f(x)$ es una función recursiva primitiva y $R(Y,z)$ es una relación recursiva primitiva, entonces son teoremas de AR las siguientes fórmulas:

a) $u=\mu z(z\le fx\wedge R(Y,z))\wedge\exists v(v\le fx\wedge R(Y,v))\leftrightarrow u\le fx\wedge R(Y,u)\wedge(v)(v\le fx\wedge R(Y,v)\to v\le u)$

b) $\sim\exists v(v\le fx\wedge R(Y,v))\leftrightarrow\sim R(Y,0)\wedge\mu z(z\le fx\wedge R(Y,z))=0$

c) $\sim\exists v(v\le fx\wedge R(Y,v))\leftrightarrow\mu z(z\le fx\wedge R(Y,z))=fx+1$

d) $u\le fx\wedge R(Y,z)\to\mu z(z\le fx\wedge R(Y,z))\le u$

e) $\mu z(z\le fx\wedge R(Y,z))\le fx\leftrightarrow\exists z(z\le fx\wedge R(Y,z))$

f) $u=\mu z(z\le fx\wedge R(Y,z))\leftrightarrow(u\le fx\wedge R(Y,u)\wedge(v)(v\le fx\wedge R(Y,v)\to u\le v)\vee\sim\exists z(z\le fx\wedge R(Y,z))$

[117] $\vdash x=yq+r\to(z|x\wedge z|y\leftrightarrow z|y\wedge z|r)$

[118] $\vdash PRIMO(x)\wedge\sim(x|y)\to(z|x\wedge z|y\to z=1)$

[119] $\vdash\sim(x|y)\to(\sim(x=y)\wedge\sim(0=y))$

[120] $\vdash x^{n}\cdot x^{m}=x^{n+m}$

[121] $\vdash x^{n}\ge 1$

[122] $\vdash 1<x\wedge x^{y}=1\to y=0$

---

[6] Sugerencia: inducción sobre "y" en AR, apoyando la demostración en las proposiciones 22-c y 22-d.

[7] Sugerencia: oprtunidad incomparable para aplicar descenso infinito a la negación de la fórmula.

[123] $\vdash 1<x \rightarrow n \leq x^n$

[124] $\vdash n<m \rightarrow p_n<p_m$

[125] $\vdash sx! = \prod_{k=1}^{sx} k$

[126] $\vdash 1 \leq x!$

[127] $\vdash x<y \rightarrow x!<y!$

[128] $\vdash n<p_n$

[129] $\vdash 1<x \wedge x^n=x^m \rightarrow n=m$

[130] $\vdash 1<x \rightarrow (n \leq m \rightarrow x^n | x^m)$

[131] $\vdash 1 \leq x \rightarrow (1 \leq m \rightarrow x | x^m)$

[132] $\vdash 0<n \rightarrow (p_n^x)_n = x.$

<u>Proposición 25</u>.– Si $f(x)$ y $g(x)$ son funciones recursivas primitivas, entonces $\vdash \sim(fx=0) \wedge \sim(gx=0) \wedge x \leq y \rightarrow fx \,|\, \prod^{y} p_k^{g(k)}$

[133] $\vdash \mathrm{PRIMO}(p_n)$

[134] $\vdash p_n>0$

[135] $\vdash \mathrm{PRIMO}(x) \leftrightarrow \exists n(x=p_n)$

[136] $\vdash p_{sn} | pm \leftrightarrow sn=m$

[137] $\vdash \sim(sn=m) \leftrightarrow \sim(p_{sn} | p_m)$

[138] $\vdash \mathrm{PRIMO}(x) \vee \exists y(1<y \wedge \mathrm{PRIMO}(y) \wedge y|x)$

[139] $\vdash \mathrm{PRIMO}(x) \rightarrow (y)(y|x \rightarrow y=x \vee y=1)$

[140] $\vdash \sim\mathrm{PRIMO}(x) \wedge \sim(x=0) \rightarrow \exists y \exists z(1<y,z<x \wedge x=yz)$

[141] $\vdash 1<x \rightarrow (y)(1<y \leq x \wedge \mathrm{PRIMO}(y) \rightarrow \sim(y|x!+1))$

[142] $\vdash \exists y(\mathrm{PRIMO}(y) \wedge p_n<y \leq p_n!+1)$

[143] $\vdash x|z \wedge y|z \rightarrow \mathrm{mcm}(x,y)|z$

[144] $\vdash \mathrm{mcm}(x,y)|xy$

[145] $\vdash xy=\mathrm{mcm}(x,y) \cdot q \rightarrow q|y$

[146] $\vdash \mathrm{PRIMO}(p) \wedge p|xy \rightarrow (p|x \vee p|y)$

[147] $\vdash x>1 \wedge \mathrm{PRIMO}(x) \wedge x|p_k^y \rightarrow x=p_k$

[148] $\vdash p_m | p_m^y \leftrightarrow y \geq 1$

[149] $\vdash \mathrm{mcd}(x,y)=1 \wedge x|yz \rightarrow x|z$

<u>Proposición 26</u>.– Si $f(x)$ y $g(x)$ son funciones recursivas primitivas, entonces $\vdash \prod^{z} p_k^{fk} \cdot \prod^{z} p_k^{gk} = \prod p_k^{fk+gk}$

[150] $\vdash \mathrm{PRIMO}(x) \wedge x \,|\, \prod^{z} p_k^{(y)_k} \rightarrow \exists k(k \leq z \wedge x=p_k)$

[151] $\vdash l(p_k)=k$

[152] $\vdash (p_k)_k=1$

[153] $\vdash x|y \rightarrow l(x) \leq l(y)$

[154] $\vdash x=\prod^{y} p_k^{(x)_k} \wedge y<z \rightarrow (x)_z=0$

[155] $\vdash 1<h<k \rightarrow (p_k)_h=0$

[156] $\vdash y \leq z \wedge x=\prod^{y} p_k^{(x)_k} \rightarrow x=\prod^{z} p_k^{(x)_k}$

[157] $\vdash (xy)_k=(x)_k+(y)_k$

[158] $\vdash \sim(x=0) \rightarrow x=\prod^{l(x)} p_k^{(x)_k}$

[159] $\vdash x>1 \rightarrow l(x) \geq 1$

[160] $\vdash p_m | x \rightarrow (x)_m \geq 1$

[161] $\vdash x=(2^x)_1$

[162] $\vdash l(2^x)=1$

<u>Proposición 27</u>.– Si $f(x)$ es una función recursiva primitiva, entonces

$$\vdash x=\prod^{z} p_k^{f(k)} \wedge fz \neq 0 \rightarrow l(x)=z$$

[163] $\vdash \prod^{z} p_{x+k}^{(y)_k} = \prod^{z+x} p_k^{(y)_{k \dot{-} x}}$

[164] $\vdash \prod_{x}^{z+x} p_k^{(y)_{k \dot{-} x}} = \prod_{0}^{z+x} p_k^{(y)_{k \dot{-} x}}$

[165] $\vdash \prod^{x} p_k^{(y)_{k \dot{-} x}}=1$

[166] $\vdash z>0 \rightarrow \prod_{sz}^{z+x} p_k^{(y)_{k \dot{-} x}} = \prod_{sz}^{z+x} p_k^{(y)_{k \dot{-} x}}$

[167] $\vdash l(x)+l(y)=l(x*y)$

[168] $\vdash l(x)=0 \rightarrow \sim\mathrm{PRUEBA}(x)$

[169] $\vdash k \leq \mathrm{l}(x) \rightarrow (x)_k = (x*y)_k$

[170] $\vdash 0 < k \leq \mathrm{l}(y) \rightarrow (y)_k = (x*y)_{\mathrm{l}(x)+k}$

[171] $\vdash \mathrm{TEO}(x) \rightarrow \mathrm{FORM}(X)$

[172] $\vdash \mathrm{TEO}(x) \wedge \mathrm{VAR}(y) \rightarrow \mathrm{TEO}(\mathrm{gen}(v, x))$

[173] $\vdash \mathrm{PRUEBA}(x) \wedge \mathrm{PRUEBA}(y) \rightarrow \mathrm{PRUEBA}(x*y)$

[174] $\vdash x = (y)_k \rightarrow x = (z*y)_{\mathrm{l}(z)+k}$

Como ejemplos presentamos las derivaciones de las fórmulas correspondientes a las proposiciones [142] (teorema de Euclides sobre la infinitud del conjunto de los números primos) y [173] (formalización de la proposición sintáctica "*si las sucesiones* $A_1, \ldots, A_n$ *y* $B_1, \ldots, B_m$ *son pruebas, entonces la sucesión* $A_1, \ldots, A_n, B_1, \ldots, B_m$ *es una prueba*"). *

[142] $\vdash \exists y(\mathrm{PRIMO}(y) \wedge p_n < y \leq p_n! + 1)$

1.— $n>0 \rightarrow p_n>0$ por [124] y $\vdash p_0=1$

2.— $\sim(n>0) \vee p_n>0$ quitando la abrviatura en 1

3.— $n=0 \vee p_n>0$ de 2 por [22] y [28]

a partir de este punto la derivación se hace por casos.

caso 1 $n=0$

4.1.— $n=0$ hipótesis

4.2.— $\mathrm{PRIMO}(2) \wedge 1<2\leq 1!+1$ expresabilidad de "PRIMO" etc.

4.3.— $\exists y(\mathrm{PRIMO}(y) \wedge 1<y\leq 1!+1)$ ($\exists$) a 4.2

4.4.— $p_0=1$ Representabildad de $p(n)$

4.5.— $\exists y(\mathrm{PRIMO}(y) \wedge p_0<y\leq p_0!+1)$ sub= 4.3 y 4.4

4.6.— $\exists y(\mathrm{PRIMO}(y) \wedge p_n<y\leq p_n!+1)$ sub= 4.1 y 4.5

Conclusión: 4.— $n=0 \rightarrow \exists y(\mathrm{PRIMO}(y) \wedge p_n<y\leq p_n!+1)$

caso 2 $p_n>1$ Aquí la derivación se divide en dos subcasos

5.1.— $p_n>1$ hipótesis

5.2.— $\exists p(\mathrm{PRIMO}(p) \wedge p \mid p_n!+1 \wedge p>1)$ hipótesis

5.3.— $\mathrm{PRIMO}(p) \wedge p \mid p_n!+1 \wedge p>1$ regla E a 5.2

5.4.— $\sim(p_n!+1=0) \wedge p \mid p_n!+1$ de [68], [126] y 5.3

---

* Al avanzar hacia las capas más profundas de la derivación formal las pruebas se hacen más complejas, más complicadas. Para hacer frente a esta situación es necesario compactar el desarrollo de cada derivación, holgando las normas que nos hemos impuesto para ello. En consecuencia, muchos pasos y algunas justificaciones se omiten. La pérdida del detalle se compensa con una mejor visión de conjunto.

5.5.— $p\le p_n!+1$	de 5.4 por [83]
5.6.— $PRIMO(p)\wedge 1<p\le p_n\to\sim(p\mid p_n!+1)$	de 5.1 y [140]
5.7.— $PRIMO(p)\wedge(p\mid p_n!+1)\to\sim(1<p\le p_n)$	L. eq. a 5.6
5.8.— $\sim(1<p\le p_n)$	CL. de 5.3 y 5.7
5.9.— $\sim(p\le p_n)$	CL. de 5.8 y $p>1$
5.10.— $p_n<p\le p_n!+1$	por [50] de 5.5 y 5.9
5.11.— $PRIMO(p)\wedge p_n<p\le p_n!+1$	CL. de 5.3 y 5.10
5.12.— $\exists y(PRIMO(y)\wedge p_n<y\le p_n!+1)$	($\exists$) a 5.11

Conclusión: 5.— $p_n>1\wedge\exists p(PRIMO(p)\wedge p\mid p_n!+1)\to\exists y(PRIMO(y)\wedge p_n<y\le p_n!+1)$

6.1.— $p_n>1$	hipótesis
6.2.— $(p)\sim(PRIMO(p)\wedge p>1\wedge p\mid p_n!+1)$	hipótesis E$\sim$(6.2)
6.3.— $(p)(p\mid p_n!+1\wedge p>1\to\sim PRIMO(p))$	L. eq. a 6.2
6.4.— $p_n!+1\mid p_n!+1\wedge p_n!+1>1\to\sim PRIMO(p_n!+1)$	(ESP) a 6.3
6.5.— $p_n!+1\mid p_n!+1\wedge p_n!+1>1$	CL. de 6.1 y [77]
6.6.— $\sim PRIMO(p_n!+1)$	MP 6.4 y 6.5
6.7.— $\exists y(PRIMO(y)\wedge 1<y\wedge y\mid p_n!+1)$	CL. de 6.6 y [138]
6.8.— $PRIMO(y)\wedge 1<y\wedge y\mid p_n!+1$	regla E a 6.7
6.9.— $PRIMO(y)\wedge 1<y\wedge y\mid p_n!+1\to\sim(y\le p_n)$	CL. de 6.1 y [141]
6.10.— $\sim(y\le p_n)$	MP 6.8 y 6.9
6.11.— $p_n<y$	CL. de 6.10 y [57]
6.12.— $PRIMO(y)\wedge p_n<y\wedge y\mid p_n!+1\wedge 0<y$	CL. de 6.8 y 6.11
6.13.— $0<y\wedge y\mid p_n!+1\to y\le p_n!+1$	CL. de 6.12 y [83]
6.14.— $PRIMO(y)\wedge p_n<y\le p_n!+1$	CL. de 6.12 y 6.13
6.15.— $\exists y(PRIMO(y)\wedge p_n<y\le p_n!+1)$	($\exists$) a 6.14

Conclusión: 6.— $p_n>1\wedge\sim\exists p(PRIMO(p)\wedge p\mid p_n!+1)\to\exists y(PRIMO(y)\wedge p_n<y\le p_n!+1)$

En resumen

1.— $n>0\to p_n>0$	
2.— $\sim(n>0)\vee p_n>0$	
3.— $n=0\vee p_n>0$	
4.— $n=0\to\exists y(PRIMO(y)\wedge p_n<y\le p_n!+1)$	conclusión 4
5.— $p_n>1\wedge(p)(PRIMO(p)\wedge p\mid p_n!+1\wedge p>1)\to\exists y(PRIMO(y)\wedge p_n<y\le p_n!+1)$	" 5
6.— $p_n>1\wedge\sim(p)(PRIMO(p)\wedge p\mid p_n!+1\wedge p>1)\to\exists y(PRIMO(y)\wedge p_n<y\le p_n!+1)$	" 6
7.— $p_n>1\to\exists y(PRIMO(y)\wedge p_n<y\le p_n!+1)$	prueba por casos a 5 y 6
8.— $\exists y(PRIMO(y)\wedge p_n<y\le p_n!+1)$	CL. de 4,7,y 3: $A\to C, B\to C, A\vee B/C$ ∎

[173] PRUEBA(x)$\wedge$PRUEBA(y)$\longrightarrow$PRUEBA(x*y)

1.- PRUEBA(x)$\wedge$PRUEBA(y)	hipótesis
2.- PRUEBA(x)	separación a 1
3.- PRUEBA(y)	separación a 1
4.- $l(x)\geq 1\wedge(h)(1\leq h\leq l(x)\longrightarrow(Ax((x)_h)\vee\exists a\exists b(1\leq a,b<h\wedge CI((x)_h,(x)_a,(x)_b))))$	de 2 por la proposición 21
5.- $l(y)\geq 1\wedge(k)(1\leq k\leq l(y)\longrightarrow(Ax((y)_k)\vee\exists c\exists d(1\leq c,d<k\wedge CI((y)_k,(y)_c,(y)_d))))$	de 3 por la proposición 21
6.- $l(x*y)=l(x)+l(y)$	Teo [167]
7.- $l(x)+l(y)\geq 1$	CL de 4,5 y [53]
8.- $l(x*y)\geq 1$	sub= 6,7
9.- $1\leq i\leq l(x*y)$	hipótesis
10.- $i\leq l(x)\vee l(x)<i$	Teo [26]
11.- $1\leq i\leq l(x)\vee l(x)<i\leq l(x*y)$	CL 9,10

En este punto la derivación se interrumpe para considerar dos casos:

<u>caso 1</u> $1\leq i\leq l(x)$

12.1.- $1\leq i\leq l(x)$	hipótesis
12.2.- $(h)(1\leq h\leq l(x)\longrightarrow(Ax((x)_h)\vee\exists a\exists b(1\leq a,b<h\wedge CI((x)_h,(x)_a,(x)_b))))$	
12.3.- $(1\leq i\leq l(x)\longrightarrow(Ax((x)_i)\vee\exists a\exists b(1\leq a,b<i\wedge CI((x)_i,(x)_a,(x)_b)))$	
12.4.- $(Ax((x)_i)\vee\exists a\exists b(1\leq a,b<i\wedge CI((x)_i,(x)_a,(x)_b)))$	
12.5.- $i\leq l(x)$	CL de 12.1
12.6.- $(x)_i=(x*y)_i$	CL de 12.5 y [169]
12.7.- $(Ax((x*y)_i)\vee\exists a\exists b(1\leq a,b<i\wedge CI((x*y)_i,(x*y)_a,(x*y)_b)))$	

El pasaje de 12.6 a 12.7 no se da aplicando tan solo la regla (sub=) Hay que considerar dos casos: $A((x)_i)$ y $\exists a\exists b(\ldots)$. En el segundo de ellos se aplican las reglas E y ($\exists$) dos veces.

<u>caso 2</u> $l(x)<i\leq l(x*y)$

13.1.- $l(x)<i\leq l(x*y)$	hipótesis
13.2.- $l(x*y)=l(x)+l(y)$	TEO [167]
13.3.- $l(x)<i\leq l(x)+l(y)$	
13.4.- $1\leq i\dot{-}l(x)\leq l(y)$	CL de 13.3 y [115]
13.5.- $(k)(1\leq k\leq l(y)\longrightarrow(Ax((y)_k)\vee\exists c\exists d(1\leq c,d<k\wedge CI((y)_k,(y)_c,(y)_d))))$	
13.6.- $(Ax((y)_k)\vee\exists c\exists d(1\leq c,d<k\wedge CI((y)_k,(y)_c,(y)_d))))$	
13.7.- $0<i\dot{-}l(x)\leq l(y)$	CL de 13.4 y [72]
13.8.- $(y)_{i\dot{-}l(x)}=(x*y)_{(i\dot{-}l(x))+l(x)}$	CL de 13.7 y [170]
13.9.- $(i\dot{-}l(x))+l(x)=i$	CL de 13.4 y [116]

| $13.10.- (y)_{i-l(x)}=(x*y)_i$
| $13.11.- Ax((x*y)_i)\vee\exists a\exists b(1\leq a, b<i\wedge CI((x*y)_i,(x*y)_a,(x*y)_b))$
|
| El pasaje de 13.10 a 13.11 es similar al del caso 1 entre 12.6 y 12.7. Además, en este caso se toma $a=c+l(x)$ y $b=d+l(x)$.

Considerados los casos precedentes podemos continuar la derivación como a continuación se indica, tomando en cuenta que los pasos 12 y 13 corresponden, respectivamente, a los casos 1 y 2:

$12.- 1\leq i\leq l(x)\rightarrow(Ax((x*y)_i)\vee\exists a\exists b(1\leq a, b<i\wedge CI((x*y)_i,(x*y)_a,(x*y)_b)))$

$13.- l(x)<i\leq l(x*y)\rightarrow(Ax((x*y)_i)\vee\exists a\exists b(1\leq a, b<i\wedge CI((x*y)_i,(x*y)_a,(x*y)_b)))$

$14.- Ax((x*y)_i)\vee\exists a\exists b(1\leq a, b<i\wedge CI((x*y)_i,(x*y)_a,(x*y)_b))$ CL 11, 12 y 13

Sea $\Gamma=\{PRUEBA(x)\wedge PRUEBA(y)\}$. Tenemos que

$$\dfrac{\dfrac{\Gamma, 1\leq i\leq l(x*y)\vdash Ax((x*y)_i)\vee\exists a\exists b(1\leq a, b<i\wedge CI((x*y)_i,(x*y)_a,(x*y)_b))}{\Gamma\vdash 1\leq i\leq l(x*y)\rightarrow Ax((x*y)_i)\vee\exists a\exists b(1\leq a, b<i\wedge CI((x*y)_i,(x*y)_a,(x*y)_b))}\text{ NTD}}{\Gamma\vdash(i)(\vdash 1\leq i\leq l(x*y)\rightarrow Ax((x*y)_i)\vee\exists a\exists b(1\leq a, b<i\wedge CI((x*y)_i,(x*y)_a,(x*y)_b)))}\text{ GEN}$$

es decir,

$PRUEBA(x)\wedge PRUEBA(y)\vdash PRUEBA(x*y)$ lcqd. ■

Pasamos ahora a la demostración de D_3.

D_3.- Si $A, B\in L^{*}_{a}$, entonces $\vdash TEO(\ulcorner A\urcorner)\wedge TEO(\ulcorner A\rightarrow B\urcorner)\rightarrow TEO(\ulcorner B\urcorner)$

$1.- TEO(\ulcorner A\urcorner)\wedge TEO(\ulcorner A\rightarrow B\urcorner)$	hipótesis
$2.- TEO(\ulcorner A\urcorner)$	
$3.- TEO(\ulcorner A\rightarrow B\urcorner)$	
$4.- \exists x_1 PR(x_1,\ulcorner A\urcorner)$	
$5.- \exists x_2 PR(x_2,\ulcorner A\rightarrow B\urcorner)$	
$6.- PR(x_1,\ulcorner A\urcorner)$	regla E a 4
$7.- PR(x_2,\ulcorner A\rightarrow B\urcorner)$	regla E a 5
$8.- PRUEBA(x_1)\wedge\ulcorner A\urcorner=(x_1)_{l(x_1)}$	por definición de PR
$9.- PRUEBA(x_2)\wedge\ulcorner A\rightarrow B\urcorner=(x_2)_{l(x_2)}$	" " "
$10.- PRUEBA(x_1*x_2)$	CL de 8 y 9 por [173]
$11.- (x_1*x_2)_{l(x_1*x_2)}=\ulcorner A\rightarrow B\urcorner$	CL de 9 por [170]
$12.- (x_1*x_2)_{l(x_1)}=\ulcorner A\urcorner$	CL de 8 por [169]
$13.- CI(\ulcorner B\urcorner,(x_1*x_2)_{l(x_1*x_2)},(x_1*x_2)_{l(x_1)})$	por ser expresable CI
$14.- \ulcorner B\urcorner=(2^{\ulcorner B\urcorner})_1$	TEO [160]
$15.- \ulcorner B\urcorner=(x_1*x_2*2^{\ulcorner B\urcorner})_{l(x_1*x_2)+1}$	CL de 14 y [170]
$16.- l(2^{\ulcorner B\urcorner})=1$	TEO [162]
$17.- \ulcorner B\urcorner=(x_1*x_2*2^{\ulcorner B\urcorner})_{l(x_1*x_2*2^{\ulcorner B\urcorner})}$	CL de 15, 16 y [167]

18.— $\mathrm{FORM}(\ulcorner B \urcorner)$ expresabilidad de FORM

19.— $l(x_1 * x_2 * 2^{\ulcorner B \urcorner}) = l(x_1 * x_2) + 1$

20.— $(k)(1 \leq k \leq l(x_1 * x_2) \rightarrow (Ax((x_1 * x_2)_k) \vee \exists a \exists b (1 \leq a, b < k \wedge$
$CI((x_1 * x_2)_k, (x_1 * x_2)_a, (x_1 * x_2)_b)))$

21.— $(k)(1 \leq k \leq l(x_1 * x_2) \rightarrow (Ax((x_1 * x_2 * 2^{\ulcorner B \urcorner})_k) \vee \exists a \exists b (1 \leq a, b < k \wedge$
$CI((x_1 * x_2 * 2^{\ulcorner B \urcorner})_k, (x_1 * x_2 * 2^{\ulcorner B \urcorner})_a, (x_1 * x_2 * 2^{\ulcorner B \urcorner})_b))$ CL de 20,[169] y [170]

22.— $Ax((x_1 * x_2 * 2^{\ulcorner B \urcorner})_{l(x_1 * x_2 * 2^{\ulcorner B \urcorner})}) \vee \exists a \exists b (1 \leq a, b < l(x_1 * x_2) + 1 \wedge$
$CI((x_1 * x_2 * 2^{\ulcorner B \urcorner})_{l(x_1 * x_2 * 2^{\ulcorner B \urcorner})}, (x_1 * x_2 * 2^{\ulcorner B \urcorner})_a, (x_1 * x_2 * 2^{\ulcorner B \urcorner})_b))$ CL de 13,15 y ($\exists$)

23.— $(k)(1 \leq k \leq l(x_1 * x_2 * 2^{\ulcorner B \urcorner}) \rightarrow (Ax((x_1 * x_2 * 2^{\ulcorner B \urcorner})_k) \vee \exists a \exists b (1 \leq a, b < k \wedge$
$CI((x_1 * x_2 * 2^{\ulcorner B \urcorner})_k, (x_1 * x_2 * 2^{\ulcorner B \urcorner})_a, (x_1 * x_2 * 2^{\ulcorner B \urcorner})_b)))$ CL de 21,22 y [30]

24.— $\mathrm{PRUEBA}(x_1 * x_2 * 2^{\ulcorner B \urcorner})$

25.— $\mathrm{PRUEBA}(x_1 * x_2 * 2^{\ulcorner B \urcorner}) \wedge \mathrm{FORM}(\ulcorner B \urcorner) \wedge \ulcorner B \urcorner = (x_1 * x_2 * 2^{\ulcorner B \urcorner})_{l(x_1 * x_2 * 2^{\ulcorner B \urcorner})}$

26.— $\mathrm{PR}(x_1 * x_2 * 2^{\ulcorner B \urcorner}, \ulcorner B \urcorner)$

27.— $\exists x_1 \mathrm{PR}(x_1, \ulcorner B \urcorner)$ ($\exists$) a 26

28.— $\mathrm{TEO}(\ulcorner B \urcorner)$ lcqd.

Por el teorema de la deducción, $\vdash \mathrm{TEO}(\ulcorner A \urcorner) \wedge \mathrm{TEO}(\ulcorner A \rightarrow B \urcorner) \rightarrow \mathrm{TEO}(\ulcorner B \urcorner)$. ■

$\boxed{D_2}$

Para demostrar D_2 es *necesario* "describir" en $\mathcal{AR}$ el modo en que los signos y las expresiones de L_a se combinan para formar términos, fórmulas y deducciones. Es por eso que introducimos las siguientes funciones aritméticas:

63.— $con_k(x_1, \ldots, x_k) = x_1 * \ldots * x_k$ concatenar las expresiones $x_1, \ldots, x_k$

Si $a_1 = \gamma e_1$, $a_2 = \gamma e_2, \ldots$ y $a_k = \gamma e_k$, entonces $con_k(a_1, \ldots, a_k) = \gamma e_1 \ldots e_k$.

64.— $coni_{n+1}(x_1, \ldots, x_n, y) = 2^7 * con_n(x_1, \ldots, x_n) * 2^{15} * y * 2^9$

Si $a_1 = \gamma e_1, \ldots,$ $a_n = \gamma e_n$ y $a = \gamma e$, entonces $coni_{n+1}(a_1, \ldots, a_n, a) = \gamma(e_1 \ldots e_n \bar{=} e)$.

65.— $=^{\prime}(x, y) = coni_2(x, y)$

Si r y t son términos, entonces $=^{\prime}(\gamma r, \gamma t)$ es el número de Gödel de la fórmula $(r = t)$.

66.— $\exists^{\prime}(n, x) = con_6(2^8, 2^7, 2^{23+4n}, 2^9, 2^8, x)$

Si $a = \gamma A$, entonces $\exists^{\prime}(n, a) = \gamma \exists x_n A$ (es decir, $\gamma \sim (x_n) \sim A$).

A continuación enumeramos algunos teoremas que intervienen en la derivación de D_2. No son todos los requeridos, como se desprende de los comentarios en torno a la proposición 28.

---

[175] $\vdash nml(0) = 2^{17}$ [176] $\vdash nml(sx) = 2^{19} * nml(x)$

[177] $\vdash TERM(nml(x))$ [178] $\vdash x=y \rightarrow nml(x)=nml(y)$

[179] $\vdash nml(sx)=\ulcorner s\urcorner * nml(x)$ [180] $\vdash nml(sx)=con_2(\ulcorner s\urcorner, nml(x))$

[181] $\vdash con_3(\ulcorner +\urcorner, nml(x), nml(y))=nml(+xy)$ [P]

[182] $\vdash TERM(x) \rightarrow TEO(=^{\prime}(x, x))$

[183] $\vdash con_4(\ulcorner s\urcorner, \ulcorner +\urcorner, nml(x), nml(y))=\ulcorner s\urcorner * con_3(\ulcorner +\urcorner, nml(x), nml(y))$

[184] $\vdash TERM(x) \rightarrow TEO(=^{\prime}(con_3(\ulcorner +\urcorner, x, nml(0)), x))$ [10]

[185] $\vdash TERM(x) \wedge TERM(y) \rightarrow TEO(=^{\prime}(con_3(\ulcorner +\urcorner, x, \ulcorner s\urcorner * y), con_4(\ulcorner s\urcorner, \ulcorner +\urcorner, x, y))$ [10]

[186] $\vdash =^{\prime}(\ulcorner e_1\urcorner, \ulcorner e_2\urcorner)=\ulcorner e_1 = e_2\urcorner$ (e_1 y e_2 expresiones de L_a)

[187] $\vdash =^{\prime}(con_3(x, y, z), w)=coni_4(x, y, z, w)$

[188] $\vdash TEO(x) \rightarrow TEO(\exists^{\prime}(n, x))$

[189] $\vdash \exists^{\prime}(1, coni_4(\ulcorner C_{rs}\urcorner, nml(x_1), \ulcorner A\urcorner, nml(0)))\dot{=}^{\prime} TEO(\ulcorner A\urcorner)$

<u>Proposición 28</u>.— Si f es una función recursiva primitiva de grado n, entonces $\vdash TEO(=^{\prime}(con_{n+1}(\ulcorner f\urcorner, nml(x_1), \ldots, nml(x_n)), nml(fx_1 \ldots x_n)))$.

La demostración se hace por inducción sobre $N(f)$ (el nivel de f). En el caso de las funciones definidas por recursión se aplica inducción en AR a la variable de la recursión. Mostramos el procedimiento con dos casos: cuando f es la función *sucesor* y cuando f es la función *suma*.

Primer caso.— f es la función *sucesor*.
Por demostrar: $\vdash TEO(=^{\prime}(con_2(\ulcorner s\urcorner, nml(x_1)), nml(sx_1)))$

1.— $TERM(nml(sx_1)) \rightarrow TEO(=^{\prime}(nml(sx_1), nml(sx_1)))$	TEO [182]
2.— $TERM(nml(sx_1))$	TEO [177]
3.— $TEO(=^{\prime}(nml(sx_1), nml(sx_1)))$	MP 1,2
4.— $nml(sx_1)=con_2(\ulcorner s\urcorner, nml(x_1))$	TEO [180]
5.— $TEO(=^{\prime}(con_2(\ulcorner s\urcorner, nml(x_1)), nml(sx_1)))$	sub= 3,4

Segundo caso.— f es la función *suma*.
Por demostrar: $\vdash TEO(=^{\prime}(con_3(\ulcorner +\urcorner, nml(x_1), nml(x_2)), nml(+x_1x_2)))$. La prueba se hace por inducción sobre "x_2" en AR.

$$A(0):\ TEO(=^{\prime}(con_3(\ulcorner +\urcorner, nml(x_1), nml(0)), nml(+x_1 0)))$$

1.— $TERM(nml(x_1)) \rightarrow TEO(=^{\prime}(con_3(\ulcorner s\urcorner, nml(x_1), nml(0), nml(x_1)))$	TEO [184]
2.— $TERM(nml(x_1))$	TEO [177]
3.— $TEO(=^{\prime}(con_3(\ulcorner s\urcorner, nml(x_1), nml(0), nml(x_1)))$	MP 1,2
4.— $+x_1 0=x_1$	Ax 12
5.— $+x_1 0=x_1 \rightarrow nml(+x_1 0)=nml(x_1)$	TEO [178]
6.— $nml(+x_1 0)=nml(x_1)$	MP 4,5
7.— $TEO(=^{\prime}(con_3(\ulcorner +\urcorner, nml(x_1), nml(0)), nml(+x_1 0)))$	sub= 3,6

[P] Algunos teoremas tienen una heurística interesante. La de [181] es ésta: $con_3(\gamma\bar{+}, nml(k_1), nml(k_2))=\gamma\bar{+}\bar{k}_1\bar{k}_2$, mientras que $nml(k_1 \oplus k_2)=\gamma\overline{k_1 \oplus k_2}=\gamma\bar{+}\bar{k}_1\bar{k}_2$ como se desprende de la proposición 7.
[10] La heurística es en estos casos la siguiente: "*Si t es un término, entonces* $\vdash t+0=t$" y "*Si r y t son términos, entonces* $\vdash r+st=s(r+t)$".

$A(sx_2)$: $TEO(\ulcorner=\urcorner(con_3(\ulcorner+\urcorner, nml(x_1), nml(sx_2)), nml(+x_1sx_2)))$

1.–	$+x_1sx_2=s+x_1x_2$	Ax 13
2.–	$nml(sx_2)=\ulcorner s\urcorner * nml(x_2)$	TEO [179]
3.–	$TERM(nml(x_1))\wedge TERM(nml(x_2))\rightarrow TEO(\ulcorner=\urcorner(con_3(\ulcorner+\urcorner, nml(x_1), \ulcorner s\urcorner * nml(x_2)), con_4(\ulcorner s\urcorner, \ulcorner+\urcorner, nml(x_1), nml(x_2))))$	TEO [185]
4.–	$TERM(nml(x_1))\wedge TERM(nml(x_2))$	CL de [177]
5.–	$TEO(\ulcorner=\urcorner(con_3(\ulcorner+\urcorner, nml(x_1), \ulcorner s\urcorner * nml(x_2)), con_4(\ulcorner s\urcorner, \ulcorner+\urcorner, nml(x_1), nml(x_2))))$	
6.–	$nml(sx_2)=\ulcorner s\urcorner * nml(x_2)$	TEO [179]
7.–	$con_4(\ulcorner s\urcorner, \ulcorner+\urcorner, nml(x_1), nml(x_2))=\ulcorner s\urcorner * con_3(\ulcorner+\urcorner, nml(x_1), nml(x_2))$	TEO [183]
8.–	$con_3(\ulcorner+\urcorner, nml(x_1), nml(x_2))=nml(+x_1x_2)$	TEO [181]
9.–	$TEO(\ulcorner=\urcorner(con_3(\ulcorner+\urcorner, nml(x_1), nml(sx_2)), \ulcorner s\urcorner * nml(+x_1x_2)))$	CL de 5,6,7 y 8
10.–	$\ulcorner s\urcorner * nml(+x_1x_2)=nml(s+x_1x_2)$	TEO [179]
11.–	$TEO(\ulcorner=\urcorner(con_3(\ulcorner+\urcorner, nml(x_1), nml(sx_2)), nml(+x_1sx_2)))$	sub= 9,10

Hemos demostrado que $\vdash A(sx_2)$. En consecuencia, $\vdash A(x_2)\rightarrow A(sx_2)$. lcqd. ■

En el caso de las funciones definidas por recursión la idea es demostrar que $\vdash TERM(x_1)\wedge\ldots\wedge TERM(x_n)\rightarrow TEO(\ulcorner=\urcorner(con_{n+2}(\ulcorner f\urcorner, x_1, \ldots, x_n, \ulcorner s\urcorner * y), con_{2n+4}(\ulcorner h\urcorner, x_1, \ldots, x_n, y, \ulcorner f\urcorner, x_1, \ldots x_n, y))$. El lector imaginará los pasos correspondientes a los números 1,7,8, y 10 de nuestro segundo ejemplo.

Por último la demostración de D_2.

D_2.– Si $A\in L^{\circ}_{a}$, entonces $\vdash TEO(\ulcorner A\urcorner)\rightarrow TEO(\ulcorner TEO(\ulcorner A\urcorner)\urcorner)$

1.–	$PR(x_1, \ulcorner A\urcorner)\rightarrow C_{PR}(x_1, \ulcorner A\urcorner)=0$	TAUT $A\rightarrow A$
2.–	$TEO(\ulcorner=\urcorner(con_3(\ulcorner C_{PR}\urcorner, nml(x_1), \ulcorner A\urcorner), nml(C_{PR}x_1\ulcorner A\urcorner)))$	prop. 28
3.–	$C_{PR}(x_1, \ulcorner A\urcorner)=0\rightarrow nml(C_{PR}x_1\ulcorner A\urcorner)=nml(0)$	TEO [178]
4.–	$PR(x_1, \ulcorner A\urcorner)\rightarrow nml(C_{PR}x_1\ulcorner A\urcorner)=nml(0)$	trans $\rightarrow$ 1,3
5.–	$PR(x_1, \ulcorner A\urcorner)\rightarrow TEO(\ulcorner=\urcorner(con_3(\ulcorner C_{PR}\urcorner, nml(x_1), \ulcorner A\urcorner), nml(0)))$	CL de 2 y 4
6.–	$\ulcorner=\urcorner(con_3(\ulcorner C_{PR}\urcorner, nml(x_1), \ulcorner A\urcorner), nml(0))=coni_4(\ulcorner C_{PR}\urcorner, nml(x_1), \ulcorner A\urcorner, nml(0))$	TEO [187]
7.–	$PR(x_1, \ulcorner A\urcorner)\rightarrow TEO(coni_4(\ulcorner C_{PR}\urcorner, nml(x_1), \ulcorner A\urcorner, nml(0)))$	sub= 5,6
8.–	$TEO(coni_4(\ulcorner C_{PR}\urcorner, nml(x_1), \ulcorner A\urcorner, nml(0)))\rightarrow TEO(\ulcorner\exists\urcorner(1, coni_4(\ulcorner C_{PR}\urcorner, nml(x_1), \ulcorner A\urcorner, nml(0))))$	TEO [188]
9.–	$PR(x_1, \ulcorner A\urcorner)\rightarrow TEO(\ulcorner\exists\urcorner(1, coni_4(\ulcorner C_{PR}\urcorner, nml(x_1), \ulcorner A\urcorner, nml(0))))$	trans $\rightarrow$ 7,8
10.–	$\ulcorner\exists\urcorner(1, coni_4(\ulcorner C_{PR}\urcorner, nml(x_1), \ulcorner A\urcorner, nml(0)))=\ulcorner TEO(\ulcorner A\urcorner)\urcorner$	TEO [189]
11.–	$PR(x_1, \ulcorner A\urcorner)\rightarrow TEO(\ulcorner TEO(\ulcorner A\urcorner)\urcorner)$	sub= 9,10
12.–	$(x_1)(PR(x_1, \ulcorner A\urcorner)\rightarrow TEO(\ulcorner TEO(\ulcorner A\urcorner)\urcorner))$	(GEN) a 11
13.–	$\exists x_1 PR(x_1, \ulcorner A\urcorner)\rightarrow TEO(\ulcorner TEO(\ulcorner A\urcorner)\urcorner)$	CL de 12
14.–	$TEO(\ulcorner A\urcorner)\rightarrow TEO(\ulcorner TEO(\ulcorner A\urcorner)\urcorner)$	lcqd. ■

FIN

RECURSIVIDAD Y ENUMERABILIDAD RECURSIVA

Al considerar conjuntos de números naturales a la luz de las funciones recursivas aparecen diversas nociones relacionadas con los Teoremas de Gödel y la investigación de los sistemas formales.

1) Un conjunto A de números naturales es *recursivo* si y sólo si su función característica es recursiva. Cuando un conjunto es recursivo es posible decidir de un modo efectivo si un número natural arbitrario le pertenece o no le pertence. Basta para ello efectuar un cálculo. En tal caso la función característica representa un algoritmo que permite decidir *mecánicamente* la pertenencia al conjunto A.

2) Un conjunto A es *recursivamente enumerable* si y sólo si existe una función recursiva $f:\mathbb{N}\longrightarrow\mathbb{N}$ tal que $f(\mathbb{N})=A$. La importancia de esta noción radica en que la función f proporciona un método para generar en forma mecáanica y sistemática una lista f(0),f(1),... etc. de los elementos de A.

3) Sea K un conjunto y sea ϕ una función de K en $\mathbb{N}$. ϕ es una *codificación* si y sólo si satisface las condiciones siguientes:

i) ϕ es 1-1 (inyectiva).
ii) Hay un algorítmo para calcular ϕ en todos sus argumentos.
iii) $\phi(K)$ es un conjunto recursivo.
iv) Hay un algorítmo para calcular ϕ^{-1} en todos sus argumentos.[1]

Si $\phi:K\longrightarrow\mathbb{N}$ es una codificación y $k\in K$, entonces se dice que $\phi(k)$ es un código (o número de código) de k. Identificando a los elementos de K con sus números de código los problemas relativos a K se transforman en problemas relativos al conjunto de números $\phi(K)$. Un ejemplo es el siguiente. En Lógica son de interés los problemas de la *decisión* y la *axiomatizabilidad*. Al investigar tales cuestiones se toma como base una codificación que asocia a cada expresión de un lenguaje formal $\mathbb{L}$ un único número natural. Tales codificaciones son fáciles de describir.

4) Sea $\mathbb{L}$ un lenguaje de primer orden y ϕ una codificación de $\mathbb{L}$. Un conjunto $\Gamma\subseteq\mathbb{L}$ es una *teoría* si y sólo si Γ es cerrado bajo noción de consecuencia lógica, es decir, $\Gamma=\{\varphi\in\mathbb{L} \mid \Gamma\models\varphi\}$. Por el teorema de completud de Gödel para el Cálculo de Predicados tenemos que Γ es una teoría si y sólo si $\Gamma=\{\varphi\in\mathbb{L} \mid \Gamma\vdash\varphi\}$.

Si $\mathbb{A}$ es una estructura del mismo tipo que $\mathbb{L}$, denotamos $T(\mathbb{A})$ al conjunto $\{\varphi\in\mathbb{L} \mid \mathbb{A}\models\varphi\}$ y le llamamos *teoría de* $\mathbb{A}$. $T(\mathbb{A})$ es una teoría en el sentido del párrafo anterior.

5) Un conjunto $A\subseteq\mathbb{L}$ es *decidible* si y sólo si hay una codificación $\phi:\mathbb{L}\longrightarrow\mathbb{N}$ tal que la función característica de $\phi(A)$ es recursiva. En particular, una teoría $T\subseteq\mathbb{L}$ es *decidible* si y sólo si hay una codificación $\phi:\mathbb{L}\longrightarrow\mathbb{N}$ tal que el conjunto $\phi(T)$ es recursivo.

---

[1] Recuérdese que $\mathrm{Dom}\phi^{-1}=\phi(K)$.

6) Un conjunto $A \subseteq L$ es *recursivamente enumerable* si y sólo si hay una codificación $\phi: L \longrightarrow \mathbb{N}$ tal que $\phi(A)$ es recursivamente enumerable.

7) Una teoría $T \subseteq L$ es *axiomatizable* si y sólo si existe un conjunto decidible de fórmulas A tal que $T = \{p \in L \mid A \models p\}$.

Algunos resultados de interés son los siguientes:

—El conjunto $\{p \in L \mid \models p\}$ es axiomatizable.
—El conjunto $\{p \in L \mid \models p\}$ es indecidible.
—El conjunto $\{p \in L \mid \models p\}$ es recursivamente enumerable.
—$T(N)$ no es axiomatizable. $N = \langle \mathbb{N}, +, \cdot, s, \leq, 0, 1 \rangle$.
—$T(N)$ no es decidible.
—La Teoría Elemental de los Grupos es indecidible.
—La Teoría Elemental de la Geometría Euclideana es decidible.
—La Teoría Elemental de la Grupos Abelianos es decidible.

TEOREMA DE GÖDEL Y TEMAS AFINES

Problemas para el capítulo II

Sea $\mathbb{A}$ la siguiente estructura:

$A(\emptyset)=\mathbb{N}$

$A(c_o)=0$

$A(I_o)=K_{00}$

$A(I_{nk})=P_{nk}$ para cada $(n,k)\in\mathbb{N}^2$ tal que $1\leq k\leq n$

$A(s)$ es la función sucesor

$A(Rgh)$ es la función $f:\mathbb{N}^{n+1}\longrightarrow\mathbb{N}$ definida por las ecuaciones

$$f(\mathbb{X},0)=A(g)(\mathbb{X});\ \ f(\mathbb{X},sy)=A(h)(\mathbb{X},y,f(\mathbb{X},y))$$

$A(Cgh_1\ldots h_m)$ es la función $f:\mathbb{N}^n\longrightarrow\mathbb{N}$ definida por la ecuación

$$F(\mathbb{X})=A(g)(A(h_1)(\mathbb{X}),\ldots,A(h_m)(\mathbb{X}))$$

Una relación aritmética $R\subseteq\mathbb{N}^n$ es *definible* en L_a $\Leftrightarrow$ existe una fórmula $\bar{R}(x_1,\ldots,x_n)\in L_a$ tal que:

a) $VL(\bar{R})=\{x_1,\ldots,x_n\}$

b) Para todo $K=(k_1,\ldots,k_n)\in\mathbb{N}^n$, $K\in R \Leftrightarrow \mathbb{A}\models\bar{R}(\bar{k}_1,\ldots,\bar{k}_n)$.

Estos conceptos están relacionados con los problemas que siguen.

1.- Demostrar que la noción sintáctica ‹*x es un axioma de grupo k*› para $k\in\{2,3,5,6,8,9,10,11,13,14\}$ es recursiva primitiva.

2.- La siguiente es una variación de la prueba heurística que Gödel expone en su disertación de 1931. En ella se muestra la manera en que la paradoja del mentiroso, la paradoja de Richard y el procedimiento diagonal de Cantor pueden utilizarse para determinar la existencia de enunciados indecidibles.

Sea $\mathbb{SF}$ un sistema formal en cuyo lenguaje son definibles propiedades de los Números Naturales. Supóngase que las fórmulas de $L_{\mathbb{SF}}$ que tienen una sóla variable libre se han ordenado en forma secuencial de algún modo: $A_1(x),\ldots,A_n(y)$, etc.

Se define la propiedad $\mathbb{G}$ de números naturales como sigue:

$$\mathbb{G}=\{k\in\mathbb{N}\ |\ \nvdash A_k(\bar{k})\}.^1$$

---

[1] "$x\in\mathbb{G}$" se lee "x es Gödeliano". Esta definición guarda un enorme parecido con la definición de *número Richardiano*.

Supóngase que la propiedad G es definible en L_{ar}.[2] De acuerdo a nuestra suposición hay una fórmula con una variable libre que define a G en L_{ar}. Se g el lugar que le corresponde en el orden secuencial.

$$k \in G \Leftrightarrow A \models A_g(k) \Leftrightarrow \vdash A_k(\bar{k})$$

Supóngase, por último, que $A_g(x)$ *expresa* a G en SF. Si A es un *modelo* de SF, entonces el enunciado $A_g(\bar{g})$ es indecidible en SF.

$\vdash A_g(\bar{g}) \Leftrightarrow g \notin G$		por definición de G
	$\Leftrightarrow A \models A_g(\bar{g})$	por que $A_g(x)$ define a G
	$\Leftrightarrow A \models \sim A_g(\bar{g})$	por definición de *verdad y satifacción*
	$\Leftrightarrow \vdash \sim A_g(\bar{g})$	por *expresabilidad*, por ser A *modelo* de SF.

conclusión: $\vdash A_g(\bar{g}) \Leftrightarrow \vdash \sim A_g(\bar{g})$

Como A esun modelo de SF, el sistema es consistente y $A_g(\bar{g})$ indecidible.

El objeto de este problema es definir la propiedad G en L_a y demostrar con ello una variante del primer teorema de Gödel.

a) Demuéstrese que las siguientes nociones sintácticas son recursivas:

(a_1) spvl(x, k)

Si x es una fórmula, entonces spvl(x, k) es la fórmula que se obtiene al substituir la primera variable de la lista $x_0, \ldots, x_n$ etc. que ocurra libre en x por el numeral de k (Es decir, si z es la primera variable de la lista que ocurre libre en A(z) y $x = \gamma A(z)$, entonces $spvl(x,k) = \gamma A(\bar{k})$). Si x no tiene variables libres, entonces spvl(x, k)=x.

(a_2) $F_1VL(x)$

El predicado $F_1VL(x)$ es verdadero $\Leftrightarrow$ x es el número de Gödel de una fórmula con una sola variable libre.

(a_3) $f_1(n)$

$f_1(n)$ es la n-esima fórmula con una variable libre de acuerdo al orden inducido por la numeración de Gödel entre las fórmulas de L_a. Notese que $f_1(0) = \gamma(x_0 = c_0)$. Este hecho se puede utilizar en la definición de f_1.

b) Con las nociones previas demuéstrese que la siguiente relación es recursiva: <x *es una prueba de la fórmula que se obtiene al substituir en* $f_1(k)$ *la variable libre por* $\bar{k}$>. Encuéntrese la fórmula que la expresa en AR.

---

[2] (para que esto suceda es suficiente con que las nociones que ocurren en el <u>definendis</u> sean definibles. Dichas nociones son las siguientes:

1.- La relación de orden entre las fórmulas con una varible libre.
2.- La noción de *ser una fórmula con una variable libre*.
3.- La relación φ *es el resultado de substituir en* Ψ *la única variable libre por el numeral* $\bar{k}$.
4.- La noción de *ser un teorema de* SF.

Negando la fórmula y generalizando respecto a "x_1" se llega a una fórmula $GD(x_2)$ cuya única variable libre es "x_2". Nótese que bajo interpretación $GD(x_2)$ corresponde a la propiedad <x_2 *es Gödeliano*>.

c) Como $GD(x_2)$ es una fórmula con una sola variable libre (¿por qué?), $\gamma GD(x_2)\in f_1(\mathbb{N})$. Sea $g\in\mathbb{N}$ tal que $f_1(g)=\gamma GD(x_2)$. Demuéstrense los incisos siguientes en el orden en que aparecen:

(c_1) Si AR es consistente, entonces $\not\vdash GD(\bar{g})$.

(c_2) Si AR es ω-consistente, entonces $\not\vdash \sim GD(\bar{g})$.

Conclúyase que si AR es ω-consistente, entonces $GD(\bar{g})$ es indecidible. Compárese esta demostración con el argumento heurístico dado al principio.

×××

3.- El teorema de Gödel establece una propiedad *sintáctica* del sistema AR al fijar un límite a su capacidad deductiva. En su momento, los Teoremas *limitativos* de esta clase llevaron a explorar las propiedaes de los sistemas formales en otros niveles, no sólo el sintáctico. Fue así que en 1936 Tarski demuestró un teorema que limita la capacidad que ciertos formalismos tienen para *representar* su semántica. Tarski consideró en particular de la noción de *verdad* o, más bien, la noción de <*ser una fórmula verdadera en una interpretación dada*>. Presentamos su teorema en el caso específico del sistema AR.

Teorema de Tarski.- Si $V=\{\gamma\Psi \mid A\models\Psi\}$, entonces V no es definible en L_α.

a) Supóngase que V es definible a través de una fórmula $V(x_1)\in L_\alpha$. Con ayuda de la función $sb(x,v,t)$ construyase una fórmula $W(x_1)$ que corresponda intuitivamente al enunciado metamatemático <*el enunciado* $W(\bar{a})$ *es falso en* A> siendo $a=\gamma W(x_1)$.

b) Demuéstrese que $A\models W(\bar{a}) \Leftrightarrow A\models\sim W(\bar{a})$, contradicción que refuta la supuesta definibilidad de V.

c) Demuéstrese que si A es un *modelo* de AR, entonces V no es recursivo.

d) conclúyase que no sólo es imposible *demostrar* en AR el que una fórmula sea verdadera en A bajo la interpretación estándar, sino que es imposible encontrar una fórmula de AR que defina dicha noción.

×××

4.- El *problema de la decisión* para un sistema SF consiste en determinar un procedimiento *efectivo* para decidir, dada cualquier fórmula de L_{SF}, si ésta es o no es un teorema de SF.

El problema se resuelve favorablemente en el caso del Cálculo Proposicional y negativamente (al menos parcialmente) en los casos del Cálculo de Predicados y el sistema AR (Para entender el sentido de la frase "*al menos parcialmente*" léanse los comentarios al final de este problema).

Teorema de Church.- Si $T=\{\gamma\Psi \mid \Psi\in L_\alpha \ \&\ \vdash\Psi\}$ y AR es consistente, entonces T no es recursivo.

a) Si T es recursivo, entonces hay una fórmula $T(x_1)$ que lo *expresa* en AR.

Con la función $sb(x,v,t)$ y la fórmula $T(x_1)$ constrúyase una fórmula $U(x_1)$ tal que $U(\bar{c})$ corresponda intuitivamente al enunciado metamatemático <*el enunciado* $U(\bar{c})$ *no es un teorema de* AR>, siendo $c=\gamma U(x_1)$.

b) Demuéstrense los siguientes incisos en el orden en que aparecen:

(b_1) Si $\vdash U(\bar{c})$, entonces $\vdash \sim U(\bar{c})$ y, por consistencia, $\nvdash U(\bar{c})$

sugerencia: úsese la expresabilidad de $T(x_1)$.

(b_2) Por el inciso anterior, $\nvdash U(\bar{c})$. Demuéstrese que en tal caso $\vdash U(\bar{c})$

sugerencia: úsese de nuevo la expresabilidad de $T(x_1)$.

c) conclúyase lo siguiente: Si AR es consistente, entonces $\vdash U(\bar{c}) \Leftrightarrow \nvdash U(\bar{c})$. Por reducción al absurdo en la metateoría se infiere que T no es recursivo.

Las nociones de *calculabilidad efectiva y procedimiento efectivo* [9] tienen un sentido intuitivo y, por lo mismo, impreciso. No obstante, Church propuso identificar la noción de *función efectivamente calculble* con el concepto de *función recursiva*. Esta identificación no puede ser objeto de una demostración rigurosa (aunque puede ser refutada), ya que en ella intervienen una noción imprecisa y un concepto bien definido. Se le conoce como la *Tesis de Church*. En su favor se argumenta que toda función calculable conocida a la fecha (Enero de 1988) es recursiva.

Aceptando la Tesis de Church, el teorema que lleva su nombre se puede expesar como sigue: El conjunto de teoremas de AR no es decidible.

d) Demuéstrese que la fórmula $\exists x_1 \overline{PR}(x_1,x_2)$ define en L_a al conjunto T.

>>>

5.- Sea $R(x_1,\ldots,x_n)$ una relación aritmética axpresable en AR. Demuéstrese la siguiente proposición:

AR es consistente $\Leftrightarrow$ Si $\vdash \bar{R}(\bar{k}_1,\ldots,\bar{k}_n)$, entonces $R(k_1,\ldots,k_n)$.

>>>

6.- En su monografía de 1931 Gödel afirma en un pie de página que cualquier antinomia epistemológica es útil para demostrar la existencia de enunciados indecidibles. Gödel en particular se vale de la paradoja de Epiménides (también llamada "*del mentiroso*") que se puede enunciar así: *Este enuncaido es falso.* Cambiando la noción de *falsedad* por la de *inderivabilidad* construye el enunciado <*este enunciado es inderivble*>.

Considerese la versión dual de la paradoja de Epiménides:

Sócrates dice: *"Lo que dice Platón es verdad".*
Platón dice: *"Lo que dice Sócrates es falso".*

Con base en estos enunciados y cambiando las nociones referidas, es posible construir enunciados que son verdaderos en la Aritmética si y

---

[9] Esta segunda noción se reduce a la primera a través de un artificio que aquí no veremos.

sólo si son inderivables en AR, quedando demostrada con ello la incompletud *semántica* de AR en caso de que sea consistente u ω-consistente.

a) Considérese la relación aritmética

$$PR(x, sb(sb(y, 31, nml(z)), 35, nml(y)))$$ [4]

y sea $P(x_1, x_2, x_3)$ la fórmula de L_α que la expresa en AR:

$$P(x_1, x_2, x_3) \equiv \overline{PR}(x_1, \overline{sb}(\overline{sb}(x_2, \overline{31}, \overline{nml}(x_3)), \overline{35}, \overline{nml}(x_2)))$$

Obsérvese que en $P(x_1, x_2, x_3)$ se hace *referencia* a una operación cruzada con las variables "x_2" y "x_3". En el primer caso "x_2" se substituye por "$nml(x_3)$", mienteras que en el segundo caso "x_3" se substituye por "$nml(x_2)$". Esto corresponde a la referencia en cruz de la paradoja dual de Epiménides.

Considérense ahora las fórmulas $\exists x_1 P(x_1, x_2, x_3)$ y $(x_1)\sim P(x_1, x_2, x_3)$ y sean $s = \gamma \exists x_1 P(x_1, x_2, x_3)$ y $p = \gamma (x_1)\sim P(x_1, x_2, x_3)$ sus *números* de Gödel ("p" por Platón y "s" por *Sócrates*).

Sean $S \equiv \exists x_1 P(x_1, \bar{p}, \bar{s})$ y $P \equiv (x_1)\sim P(x_1, \bar{s}, \bar{p})$.

b) Muéstrese que bajo su interpretación usual:

S afirma: "*El enunciado* P *es derivable en* AR".

P afirma: "*el enunciado* S *es inderivable en* AR".

c) Demuéstrese que si AR es consistente, entonces $\nvdash P$.

sugerencia: $\vdash P \Rightarrow \vdash S \Rightarrow \vdash \sim P$.

d) Demuéstrese que si AR es ω-consistente, entonces $\nvdash S$.

sugerencia: por el inciso (c), $\nvdash P$.

e) conclúyase que si AR es consistente, entonces $A \models P$ y $\nvdash P$.

---

[4] $31 = \partial x_2$ y $35 = \partial x_3$.

PROPOSICIONES RELATIVAS A LA ARITMETICA Y LOS TEOREMAS DE AR.

Proposición 1.— Si $f(X,y)$ es una función recursiva primitiva, entonces las funciones

$$\sigma f(X,z)=\sum_{k=0}^{z} f(X,k) \quad y \quad \Pi f=\prod_{k=0}^{z} f(X,k) \text{ son recursivas primitivas. } \blacksquare$$

Proposición 2 (cerradura).— Sean $R(X)$ y $S(Y)$ relaciones recursivas (recursivas primitivas). En tal caso:

i) $\neg R(X)$ es recursiva (recursiva primitiva).
ii) $R(X)\&S(Y)$ es recursiva (recursiva primitiva).
iii) $R(X)\vee S(Y)$ es recursiva (recursiva primitiva). ■

Proposición 3.— Sea $R(X,z)$ una relación recursiva (rp) de grado n+1 y sea $f(Y)$ una función recursiva (rp). En tal caso:

i) $S(X,Y)\equiv\exists z(z\leq f(Y)\ \&\ R(X,z))$ es una relación recusiva (rp) en las variables $\{x_1,\ldots,x_n\}\cup\{y_1,\ldots,y_m\}$.
ii) $T(X,Y)\equiv\forall z(z\leq f(Y)\ \Rightarrow\ R(X,z))$ es una relación recursiva (rp) en las variables $\{x_1,\ldots,x_n\}\cup\{y_1,\ldots,y_m\}$. ■

Proposición 4.— Si $R(X,z)$ y $f(Y)$ son recursivas (rp), la función

$$g(X,Y)=\begin{cases} \min RF & \text{si } RF\neq\emptyset \\ f(Y)+1 & \text{si } RF=\emptyset \end{cases}$$

es recursiva (rp). ■

Proposición 5.— Sean $R_1(X),\ldots,R_k(X)$ relaciones recursivas (rp) ajenas entre sí y sean $g_1(X),\ldots,g_k(X)$, $h(X)$ funciones recursivas (rp). La función f definida por las ecuaciones

$f(X)=g_1(X)$.....si $R_1(X)$
$f(X)=g_2(X)$.....si $R_2(X)$
.....
$f(X)=g_k(X)$.....si $R_k(X)$
$f(X)=h(X)$......en el caso restante
es recursiva (rp). ■

Proposición 6.— Sea f la función definida por curso de valores como sigue:

$$f(X,0)=k \quad ; \quad f(X,sy)=\prod_{i=0}^{y}(f(X,i)+g(X,i))$$

Se afirma que si g es recursiva (rp), entonces f es recursiva (rp). ■

[1] $\vdash x=y\rightarrow y=x$

[2] $\vdash x=y\rightarrow(y=z\rightarrow x=z)$

[3] $\vdash x_i=x_k\rightarrow f(x_1\ldots x_i\ldots x_n)=f(x_1\ldots x_k\ldots x_n)$

[4] $\vdash r=t\rightarrow sr=st$

[5] $\vdash r=t\rightarrow(A(r,r)\rightarrow A(r,t))$

[6] $\vdash r_0=r_1\rightarrow t(r_0,r_0)=t(r_0,r_1)$

[7] $\vdash x+\overline{1}=sx$

[8] $\vdash x+(y+z)=(x+y)+z$

[9] $\vdash sx+y=x+sy$

[10] $\vdash 0+x=x$

[11] $\vdash x+y=y+x$

[12] $\vdash y+x=z+x\rightarrow y=z$

[13] $\vdash x=0\vee\exists y(x=sy)$

[14] $\vdash x\leq x$

[15] $\vdash 0\leq x$

[16] $\vdash x\leq sx$

[17] $\vdash x\leq y\wedge y\leq z\rightarrow x\leq z$

[18] $\vdash x\leq y\vee sy\leq x$

[19] $\vdash x+y=0\rightarrow x=0$

[20] $\vdash x\leq y\wedge y\leq x\rightarrow x=y$

[21] $\vdash x\leq sy\rightarrow(x\leq y\vee x=sy)$

[22] $\vdash x\leq 0\rightarrow x=0$

[23] $\vdash sx\leq y\leftrightarrow x<y$

[24] $\vdash x<sy\rightarrow x\leq y$

[25] $\vdash x<y\rightarrow sx<sy$

[26] $\vdash y\leq x\vee x<y$

[27] a) $\vdash A(\overline{0})\wedge\ldots\wedge A(\overline{k})\rightarrow(x)(x\leq\overline{k}\rightarrow A(x))$

b) $\vdash(x)(x\leq y\rightarrow A(x))\wedge A(y+\overline{1})\rightarrow(x)(x\leq y=\overline{1}\rightarrow A(x))$

c) $\vdash(x)(x\leq y\rightarrow A(x))\wedge z\leq y\rightarrow(x)(x\leq z\rightarrow A(x))$

[28] $\vdash A(\overline{k})\rightarrow(x)(\overline{k}\leq x\rightarrow\exists y(y\leq x\wedge A(y)))$

[29] $\vdash(x)(x\leq y\rightarrow A(x))\wedge(x)(y<x\rightarrow B(x))\rightarrow(x)(A(x)\vee B(x))$

[30] a) $\vdash(z)(x\leq z\leq y\rightarrow A(z))\wedge A(y+\overline{1})\rightarrow(z)(x\leq z\leq y+\overline{1}\rightarrow A(z))$

b) $\vdash A(\overline{0})\wedge\ldots\wedge A(\overline{k-1})\rightarrow(x)(x<\overline{k}\rightarrow A(x))$ con $k\in\mathbb{N}^+$

c) $\vdash A(\overline{k})\wedge\ldots\wedge A(\overline{k}+\overline{h})\rightarrow(x)(\overline{k}\leq x\leq\overline{k}+\overline{h}\rightarrow A(x))$

[31] $\vdash x+y=\overline{1}\rightarrow(x=\overline{1}\vee y=\overline{1})$

[32] $\vdash x+y=x+z\rightarrow y=z$

[33] $\vdash\overline{2}+\overline{1}=\overline{3}$, $\vdash\overline{2}+\overline{2}=\overline{4}$, etc.

[34] $\vdash x\cdot y=y\cdot x$

[35] $\vdash x\cdot(y\cdot z)=(x\cdot y)\cdot z$

[36] $\vdash x\cdot\overline{1}=x$

[37] $\vdash\sim(x=0)\rightarrow(x\cdot y=0\leftrightarrow y=0)$

[38] $\vdash\sim(x=0)\wedge\sim(y=0)\leftrightarrow\sim(x\cdot y=0)$

[39] $\vdash y=0 \leftrightarrow (x\cdot y=0)$

[40] $\vdash x=0 \rightarrow (y)(x\cdot y=0)$

[41] $\vdash x<y \rightarrow \sim(x=y)$

[42] $\vdash x\cdot y=0 \leftrightarrow (x=0 \vee y=0)$

[43] $\vdash x\cdot y=\bar{1} \leftrightarrow (x=\bar{1} \wedge y=\bar{1})$

[44] $\vdash \sim(x=0) \rightarrow (x\cdot y=x\cdot z \rightarrow y=z)$

[45] $\vdash \bar{2}\cdot\bar{1}=\bar{2}$, $\vdash \bar{2}\cdot\bar{2}=\bar{4}$, etc

[46] $\vdash x\cdot\bar{2}=x+x$

[47] $\vdash x\cdot(y+z)=x\cdot y+x\cdot z$

[48] $\vdash \sim(x=0) \rightarrow (x=\bar{1} \vee \exists y(x=ssy))$

[49] $\vdash \sim(x=sx)$

[50] $\vdash x\leq y \rightarrow (y<z \rightarrow x<z)$

[51] $\vdash \sim(\bar{1}\leq x\leq y) \wedge \sim(x\leq\bar{1}) \rightarrow \sim(x\leq y)$

[52] $\vdash \sim(x\leq y) \wedge x\leq z \rightarrow y<x\leq z$

[53] a) $\vdash x<y \leftrightarrow x+z<y+z$

b) $\vdash x\leq y \rightarrow x+z\leq y+z$

[54] $\vdash x\leq y \leftrightarrow (x=y \vee x<y)$

[55] $\vdash x<y \vee x=y \vee y<x$

[56] $\vdash x\leq y \rightarrow z\cdot x\leq z\cdot y$

[57] a) $\vdash x<u \wedge y<w \rightarrow x\cdot y<u\cdot w$

b) $\vdash x\leq u \wedge y\leq w \rightarrow x\cdot y\leq u\cdot w$

c) $\vdash 0<x\leq u \wedge y\leq w \rightarrow x\cdot y<u\cdot w$

d) $\vdash \sim(x=0) \rightarrow (y<z \rightarrow x\cdot y<x\cdot z)$

[58] a) $\vdash x\leq y \rightarrow x\leq sy$

b) $\vdash x<y \rightarrow sx\leq y$

[59] $\vdash \sim(x<x)$

[60] $\vdash x<y \leftrightarrow \sim(y\leq x)$

[61] $\vdash x\leq y \rightarrow (y<z \rightarrow x<z)$

[62] a) $\vdash 0<sx$

b) $\vdash x<sx$

[63] $\vdash \sim(x<0)$

[64] $\vdash x\leq y \vee y\leq x$

[65] a) $\vdash x\leq x+y$

b) $\vdash \sim(y=0) \rightarrow x<x+y$

[66] a) $\vdash x<\bar{1} \rightarrow x=0$

b) $\vdash x\leq\bar{1} \rightarrow (x=0 \vee x=\bar{1})$

[67] $\vdash x<y \leftrightarrow (x\leq y \wedge \sim(x=y))$

[68] a) $\vdash \sim(x=0) \rightarrow y \leq y \cdot x$

b) $\vdash \sim(x=0) \leftrightarrow 0 < x$

[69] $\vdash 0 < x \rightarrow (0 < y \rightarrow 0 < x \cdot y)$

[70] $\vdash \sim(x=0) \rightarrow (\bar{1} < y \rightarrow x < x \cdot y)$

[71] $\vdash \sim(x=0) \rightarrow (x \cdot y = x \cdot z \rightarrow y = z)$

[72] $\vdash \bar{0} < \bar{1}$, $\vdash \bar{1} < \bar{2}$, etc.

[73] a) $\vdash \sim(x=0) \wedge \sim(y=0) \rightarrow (x \cdot y = z \rightarrow x \leq z \wedge y \leq z)$

b) $\vdash \sim(x=0) \rightarrow (x \cdot y \leq z \rightarrow y \leq z)$

[74] a) $\vdash x+y=z \wedge \sim(x+u=z) \rightarrow \sim(y=u)$

b) $\vdash x \leq y+z \rightarrow (x \leq y \vee y < x \leq x+z)$

[75] $\vdash \sim(y=0) \rightarrow \exists q \exists r (x = y \cdot q + r \wedge r < y)$

[76] a) $\vdash x=\bar{0} \vee \ldots \vee x=\bar{k} \rightarrow x \leq \bar{k}$

b) $\vdash x=\bar{0} \vee \ldots \vee x=\overline{k-1} \rightarrow x < \bar{k}$ con $k \in \mathbb{N}^+$

[77] $\vdash x | x$

[78] $\vdash x | y \rightarrow (y | z \rightarrow x | z)$

[79] a) $\vdash x | 0$

b) $\vdash \bar{1} | x$

[80] $\vdash x | x \cdot y$

[81] $\vdash 0 | x \rightarrow x = 0$

[82] $\vdash x | y \wedge y | x \rightarrow x = y$

[83] $\vdash \sim(x=0) \rightarrow (y | x \rightarrow y \leq x)$

[84] $\vdash x | z \leftrightarrow \exists y (y \leq z \wedge x \cdot y = z)$

[85] $\vdash x | y \rightarrow x | y \cdot z$

[86] $\vdash x | y \wedge x | z \rightarrow x | u \cdot y + w \cdot z$

[87] $\vdash \bar{1} < x \rightarrow (x | sy \rightarrow \sim(x | y))$

[88] $\vdash x | \bar{1} \rightarrow x = \bar{1}$

[89] $\vdash x | y \wedge \sim(z | y) \rightarrow \sim(x = z)$

[90] $\vdash x | y \wedge x | sy \rightarrow x = \bar{1}$

[91] $\vdash \bar{1} < x \wedge (y)(\bar{1} < y \wedge y | x \rightarrow x \leq y) \rightarrow (z)(z | x \rightarrow z = \bar{1} \vee z = x)$

[92] $\vdash P(\bar{2})$ [1]

[93] $\vdash P(\bar{3})$

[94] $\vdash \sim P(\bar{4})$

[95] $\vdash \exists x (x < y \wedge x | y \wedge P(x)) \rightarrow \sim P(y)$

[96] $\vdash ((x)(x < y \rightarrow A(x)) \rightarrow A(y)) \rightarrow A(y)$ inducción completa

[97] $\vdash \exists y A(y) \rightarrow \exists y (A(y) \wedge (x)(A(x) \rightarrow y \leq x))$ buen orden

[98] $\vdash (A(y) \rightarrow \exists x (x < y \wedge A(x))) \rightarrow \sim A(y)$ descenso infinito

---

1 $P(x)$ es abreviatura de la fórmula $(z)(z | x \rightarrow z = \bar{1} \vee z = x)$.

[99] $\vdash A(\bar{k})\wedge(x)(A(x)\rightarrow A(sx))\rightarrow(x)(\bar{k}\leq x\rightarrow A(x))$.

Proposición 7.– Si $h,k\in\mathbb{N}$, entonces $\vdash\overline{h\oplus k}=\bar{h}\bar{+}\bar{k}$. ■

Proposición 8.– Si $h,k\in\mathbb{N}$ y $h\neq k$, entonces $\vdash\sim(\bar{h}=\bar{k})$. ■

Proposición 9.– Si f es una función recursiva primitiva de grado n y $k_1,\ldots,k_n\in\mathbb{N}$, entonces $\vdash\overline{f(k_1\ldots k_n)}=\bar{f}(\bar{k}_1\ldots\bar{k}_n)$. ■

Proposición 10.– Si f es una función recursiva primitiva de grado n, entonces la fórmula $\bar{f}(x_1\ldots x_n)=x_{n+1}$ la representa fuertemente en AR. ■

Proposición 11.– Sea $g(x_1,\ldots,x_n,y)$ una función aritmética y sea $G(x_1\ldots x_n,y,z)$ una fórmula que la representa fuertemente en AR. Si $g(k_1\ldots k_n,k)=a$ y $a\neq b$, entonces $\vdash\sim G(\bar{k}_1\ldots\bar{k}_n,\bar{k},\bar{b})$. ■

Proposición 12.– Sea $g(x_1,\ldots,x_n,y)$ una función aritmética tal que:

(1) Para todo $(k_1,\ldots,k_n)\in\mathbb{N}^n$ existe $k\in\mathbb{N}$ tal que $g(k_1,\ldots,k_n,k)=0$
(2) La fórmula $G(x_1,\ldots,x_n,y,z)$ la representa fuertemente en AR.

En tal caso la función $f(x_1,\ldots,x_n)=\mu y(g(x_1,\ldots,x_n,y)=0)$ está fuertemente representada en AR por la fórmula

$F(x_1\ldots x_n,y)\equiv G(x_1\ldots x_n,y,\bar{0})\wedge(z)(z<y\rightarrow\sim G(x_1\ldots x_n,z,\bar{0}))$. ■

Proposición 13.– Si $f:\mathbb{N}^n\longrightarrow\mathbb{N}$ es una función recursiva, entonces f es fuertemente representable en AR. ■

Proposición 14.– Toda relación recursiva es expresable en AR. ■

Proposición 15 (lema diagonal).– Si $A(x_k)\in L_a$ y $VL(A)=\{x_k\}$, entonces existe un enunciado (fórmula sin variables libres) $B\in L_a^0$ tal que $\vdash B\leftrightarrow A(\ulcorner B\urcorner)$. ■

Proposición 16 (teorema de Lob).– Si $A\in L_a^0$ y $\vdash TEO(\ulcorner A\urcorner)\rightarrow A$, entonces $\vdash A$. ■

Corolario 1.– $\{A \mid A\in L_a^0$ y $\vdash A\}=\{A \mid A\in L_a^0$ y $\vdash TEO(\ulcorner A\urcorner)\leftrightarrow A\}$. ■

Corolario 2 (segundo teorema de Gödel).– Si $A\in L_a^0$, $\vdash A$ y AR es consistente, entonces $\nvdash\sim TEO(\ulcorner\sim A\urcorner)$. ■

Corolario 3.– Si $D\in L_a^0$ y $\vdash D\leftrightarrow TEO(\ulcorner D\urcorner)$, entonces $\vdash D$. ■

Corolario 4.– SF es consistente $\Leftrightarrow$ $\nvdash_{SF}\sim TEO(\ulcorner A\urcorner)$. ■

Proposición 17.– Si AR es ω-consistente y $\vdash TEO(\ulcorner A\urcorner)$, entonces $\vdash A$. ■

Proposición 18 (primer teorema de Gödel).– Sea G tal que $\vdash G\leftrightarrow\sim TEO(\ulcorner G\urcorner)$

a) Si AR es consistente, entonces $\nvdash G$.
b) Si AR es ω-consistente, entonces $\nvdash\sim G$. ■

Proposición 19.– Si G es el enunciado de Gödel, entonces $\vdash G\leftrightarrow CON$. ■

Proposición 20 (segundo teorema de Gödel).– Si AR es consistente, entonces $\nvdash$CON. ∎

Corolario 5.– $\vdash$CON$\rightarrow\sim$TEO(⌜CON⌝). ∎

Proposición 21.– Si $P(X), S(X)$ y $T(X, z)$ son relaciones recursivas primitivas, $f(Y)$ es una función recursiva primitiva y $R(X, Y)$ es la relación

a) $\neg P(X)$

b) $P(X) \vee S(X)$

c) $P(X)$ & $S(X)$

d) $\exists z(z \leq f(Y)$ & $T(X, z))$

e) $\forall z(z \leq f(Y) \Rightarrow T(X, z))$,

entonces $\overline{R}(X, Y)$ es la fórmula

a) $\sim\overline{P}(X)$

b) $\overline{P}(x) \vee \overline{S}(X)$

c) $\overline{P}(X) \wedge \overline{S}(X)$

d) $\exists z(z \leq \overline{f}(Y) \wedge \overline{T}(X, z))$

e) $(z)(z \leq \overline{f}(Y) \rightarrow \overline{T}(X, z))$ ∎

Proosición 22.– Si $f(x)$ es una función recursiva, entonces las siguientes fórmulas son teoremas de AR:

a) $(x)(x \leq y \rightarrow f(x)=1) \rightarrow \sum^{y} f(k)=y+1$

b) $(x)(x \leq y \rightarrow f(x)=1) \rightarrow \prod^{y} f(k)=1$

c) $x<y \rightarrow \sum^{y} f(k)=\sum^{x} f(k) + \sum_{x+1}^{y} f(k)$

d) $x<y \rightarrow \prod^{y} f(k)=\prod^{x} f(k) \cdot \prod_{+1}^{y} f(k)$

e) $(x)(a \leq x \leq b \rightarrow f(x)=0) \rightarrow \sum_{a}^{b} f(k)=0$

f) $(x)(a \leq x \leq b \rightarrow f(x)=1) \rightarrow \prod_{a}^{b} f(k)=1$

g) $h \leq y \rightarrow \exists z(\sum^{y} f(k)=f(h)+z)$

h) $h \leq y \rightarrow \exists z(\prod^{y} f(k)=f(h) \cdot z)$

i) $f(x)=0 \rightarrow (y)(x \leq y \rightarrow \prod_{x}^{y} f(k)=0)$

j) $f(x)=0 \rightarrow (y)(\prod_{x}^{x+y} f(k)=0)$

k) $\sum_{x}^{x+y} f(k)=0 \leftrightarrow (z)(z \leq y \rightarrow f(x+z)=0)$

l) $\prod_{x}^{x+y} f(k)=0 \leftrightarrow \exists z(z \leq y \wedge f(x+z)=0)$

m) $x \leq y \wedge \sum^{y} f(k)=0 \rightarrow \sum^{x} f(k)=0$

n) $x \leq y \wedge \prod^{y} f(k)=1 \rightarrow \prod^{x} f(k)=1$

ñ) $(x)(f(x)=1 \vee f(x)=0) \rightarrow (\sum^{y} f(k)=y+1 \leftrightarrow (z)(z \leq y \rightarrow f(z)=1)$

Proposición 23.– Si $R(X, y)$ es una relación recursiva primitiva, entonces

$$\vdash y \leq z \wedge R(X, y) \rightarrow Mu(u \leq z \wedge R(X, u)) \geq y \ \blacksquare$$

[100] $\vdash x|y \wedge x|z \rightarrow x|ay+bz$

[101] $\vdash \sim(x=1) \wedge x|y \rightarrow \sim(x|y+1)$

[102] $\vdash x=y+z \rightarrow x \dot{-} y=z$

[103] $\vdash (x+1) \dot{-} y=z+1 \rightarrow x \dot{-} y=z$

[104] $\vdash z>0 \wedge x \dot{-} y=z \rightarrow x=y+z$

[105] $\vdash x \dot{-} (y+z)=(x \dot{-} y) \dot{-} z$

[106] $\vdash x \leq y \rightarrow (y \dot{-} x=z \rightarrow y=x+z)$

[107] $\vdash 0 \dot{-} x=0$

[108] $\vdash (x+y) \dot{-} y=x$

[109] $\vdash z(x \dot{-} 1)=zx \dot{-} z$

[110] $\vdash zx \dot{-} zy=z(x \dot{-} y)$

[111] $\vdash pd(x) \leq x$

[112] $\vdash x \dot{-} y \leq x$

[113] $\vdash x \dot{-} x=0$

[114] $\vdash x \dot{-} y=0 \rightarrow x \leq y$

[115] $\vdash x<y \leq x+z \rightarrow (y \dot{-} x)+x=y \wedge (y \dot{-} x) \leq z$

[116] $\vdash x \leq y \rightarrow y \dot{-} (y \dot{-} x)=x$.

<u>Proposición 24</u>.– Si $f(x)$ es una función recursiva primitiva y $R(Y,z)$ es una relación recursiva primitiva, entonces son teoremas de AR las siguientes fórmulas:

a) $u=\mu z(z \leq fx \wedge R(Y,z)) \wedge \exists v(v \leq fx \wedge R(Y,v)) \leftrightarrow u \leq fx \wedge R(Y,u) \wedge (v)(v \leq fx \wedge R(Y,v) \rightarrow v \leq u)$

b) $\sim \exists v(v \leq fx \wedge R(Y,v)) \leftrightarrow \sim R(Y,0) \wedge \mu z(z \leq fx \wedge R(Y,z))=0$

c) $\sim \exists v(v \leq fx \wedge R(Y,v)) \leftrightarrow \mu z(z \leq fx \wedge R(Y,z))=fx+1$

d) $u \leq fx \wedge R(Y,z) \rightarrow \mu z(z \leq fx \wedge R(Y,z)) \leq u$

e) $\mu z(z \leq fx \wedge R(Y,z)) \leq fx \leftrightarrow \exists z(z \leq fx \wedge R(Y,z))$

f) $u=\mu z(z \leq fx \wedge R(Y,z)) \leftrightarrow (u \leq fx \wedge R(Y,u) \wedge (v)(v \leq fx \wedge R(Y,v) \rightarrow u \leq v) \vee \sim \exists z(z \leq fx \wedge R(Y,z))$

[117] $\vdash x=yq+r \rightarrow (z|x \wedge z|y \leftrightarrow z|y \wedge z|r)$

[118] $\vdash PRIMO(x) \wedge \sim(x|y) \rightarrow (z|x \wedge z|y \rightarrow z=1)$

[119] $\vdash \sim(x|y) \rightarrow (\sim(x=y) \wedge \sim(0=y))$

[120] $\vdash x^n \cdot x^m=x^{n+m}$

[121] $\vdash x^n \geq 1$

[122] $\vdash 1<x \wedge x^y=1 \rightarrow y=0$

[123] $\vdash 1<x \rightarrow n \leq x^n$

[124] $\vdash n<m \rightarrow p_n<p_m$

[125] $\vdash sx! = \prod_{k=1}^{sx} k$

[126] $\vdash 1 \leq x!$

[127] $\vdash x<y \rightarrow x!<y!$

[128] $\vdash n<p_n$

[129] $\vdash 1<x \wedge x^n=x^m \rightarrow n=m$

[130] $\vdash 1<x \rightarrow (n \leq m \rightarrow x^n|x^m)$

[131] $\vdash 1 \leq x \rightarrow (1 \leq m \rightarrow x|x^m)$

[132] $\vdash 0<n \rightarrow (p_n^x)_n=x$.

<u>Proposición 25</u>.– Si $f(x)$ y $g(x)$ son funciones recursivas primitivas, entonces $\vdash \sim(fx=0) \wedge \sim(gx=0) \wedge x \leq y \rightarrow fx|\prod^{y} p_k^{g(k)}$ ■

[133] $\vdash PRIMO(p_n)$

[134] $\vdash p_n>0$

[135] $\vdash PRIMO(x) \leftrightarrow \exists n(x=p_n)$

[136] $\vdash p_{sn}|pm \leftrightarrow sn=m$

[137] $\vdash \sim(sn=m) \leftrightarrow \sim(p_{sn}|p_m)$

[138] $\vdash PRIMO(x) \vee \exists y(1<y \wedge PRIMO(y) \wedge y|x)$

[139] $\vdash PRIMO(x) \rightarrow (y)(y|x \rightarrow y=x \vee y=1)$

[140] $\vdash \sim PRIMO(x) \wedge \sim(x=0) \rightarrow \exists y \exists z(1<y, z<x \wedge x=yz)$

[141] $\vdash 1<x \rightarrow (y)(1<y \leq x \wedge PRIMO(y) \rightarrow \sim(y|x!+1))$

[142] $\vdash \exists y(PRIMO(y) \wedge p_n<y \leq p_n!+1)$

[143] $\vdash x|z \wedge y|z \rightarrow mcm(x,y)|z$

[144] $\vdash mcm(x,y)|xy$

[145] $\vdash xy=mcm(x,y) \cdot q \rightarrow q|y$

[146] $\vdash \mathrm{PRIMO}(p) \wedge p \mid xy \rightarrow (p \mid x \vee p \mid y)$

[147] $\vdash x > 1 \wedge \mathrm{PRIMO}(x) \wedge x \mid p_k \rightarrow x = p_k$

[148] $\vdash p_{sn} \mid p_{sn}^{y} \leftrightarrow y \geq 1$

[149] $\vdash \mathrm{mcd}(x,y) = 1 \wedge x \mid yz \rightarrow x \mid z$

<u>Proposición 26</u>.— Si f(x) y g(x) son funciones recursivas primitivas, entonces $\vdash \prod^{z} p_k^{fk} \cdot \prod^{z} p_k^{gk} = \prod p_k^{fk+gk}$ ∎

[150] $\vdash \mathrm{PRIMO}(x) \wedge x \mid \prod^{z} p_k^{(y)_k} \rightarrow \exists k (k \leq z \wedge x = p_k)$

[151] $\vdash l(p_k) = k$

[152] $\vdash (p_k)_k = 1$

[153] $\vdash x \mid y \rightarrow l(x) \leq l(y)$

[154] $\vdash x = \prod^{y} p_k^{(x)_k} \wedge y < z \rightarrow (x)_z = 0$

[155] $\vdash 1 < h < k \rightarrow (p_k)_h = 0$

[156] $\vdash y \leq z \wedge x = \prod^{y} p_k^{(x)_k} \rightarrow x = \prod^{z} p_k^{(x)_k}$

[157] $\vdash (xy)_k = (x)_k + (y)_k$

[158] $\vdash \sim(x = 0) \rightarrow x = \prod^{l(x)} p_k^{(x)_k}$

[159] $\vdash x > 1 \rightarrow l(x) \geq 1$

[160] $\vdash p_{sn} \mid x \rightarrow (x)_{sn} \geq 1$

[161] $\vdash x = (2^x)_1$

[162] $\vdash l(2^x) = 1$

<u>Proposición 27</u>.— Si f(x) es una función recursiva primitiva, entonces

$$\vdash x = \prod^{z} p_k^{f(x(} \wedge fz \neq 0 \rightarrow l(x) = z \;\blacksquare$$

[163] $\vdash \prod^{z} p_{x+k}^{(y)_k} = \prod^{z+x} p_k^{l(y)_{k \dot- x}}$

[164] $\vdash \prod_{x}^{z+x} p_k^{(y)_{k \dot- x}} = \prod_{0}^{z+x} p_k^{(y)_{k \dot- x}}$

[165] $\vdash \prod^{x} p_k^{(y)_{k \dot- x}} = 1$

[166] $\vdash z > 0 \rightarrow \prod_{sz}^{z+x} p_k^{(y)_{k \dot- x}} = \prod_{sz}^{z+x} p_k^{(y)_{k \dot- x}}$

[167] $\vdash l(x) + l(y) = l(x * y)$

[168] $\vdash l(x) = 0 \rightarrow \sim \mathrm{PRUEBA}(x)$

[169] $\vdash k \leq l(x) \rightarrow (x)_k = (x * y)_k$

[170] $\vdash 0 < k \leq l(y) \rightarrow (y)_k = (x * y)_{l(x)+k}$

[171] $\vdash \mathrm{TEO}(x) \rightarrow \mathrm{FORM}(x)$

[172] $\vdash \mathrm{TEO}(x) \wedge \mathrm{VAR}(y) \rightarrow \mathrm{TEO}(\mathrm{gen}(v,x))$

[173] $\vdash \mathrm{PRUEBA}(x) \wedge \mathrm{PRUEBA}(y) \rightarrow \mathrm{PRUEBA}(x * y)$

[174] $\vdash x = (y)_k \rightarrow x = (z * y)_{l(z)+k}$

[175] $\vdash \mathrm{nml}(0) = 2^{17}$

[176] $\vdash \mathrm{nml}(sx) = 2^{19} * \mathrm{nml}(x)$

[177] $\vdash \mathrm{TERM}(\mathrm{nml}(x))$

[178] $\vdash x = y \rightarrow \mathrm{nml}(x) = \mathrm{nml}(y)$

[179] $\vdash \mathrm{nml}(sx) = \ulcorner s \urcorner * \mathrm{nml}(x)$

[180] $\vdash \mathrm{nml}(sx) = \mathrm{con}_2(\ulcorner s \urcorner, \mathrm{nml}(x))$

[181] $\vdash \mathrm{con}_3(\ulcorner + \urcorner, \mathrm{nml}(x), \mathrm{nml}(y)) = \mathrm{nml}(+xy)$

[182] $\vdash \mathrm{TERM}(x) \rightarrow \mathrm{TEO}(=^{\cdot}(x,x))$

[183] $\vdash \mathrm{con}_4(\ulcorner s \urcorner, \ulcorner + \urcorner, \mathrm{nml}(x), \mathrm{nml}(y)) = \ulcorner s \urcorner * \mathrm{con}_3(\ulcorner + \urcorner, \mathrm{nml}(x), \mathrm{nml}(y))$

[184] $\vdash \mathrm{TERM}(x) \rightarrow \mathrm{TEO}(=^{\cdot}(\mathrm{con}_3(\ulcorner + \urcorner, x, \mathrm{nml}(0)), x))$ [10]

[185] $\vdash \mathrm{TERM}(x) \wedge \mathrm{TERM}(y) \rightarrow \mathrm{TEO}(=^{\cdot}(\mathrm{con}_3(\ulcorner + \urcorner, x, \ulcorner s \urcorner * y), \mathrm{con}_4(\ulcorner s \urcorner, \ulcorner + \urcorner, x, y))$

[186] $\vdash =^{\cdot}(\ulcorner e_1 \urcorner, \ulcorner e_2 \urcorner) = \ulcorner e_1 = e_2 \urcorner$ (e_1 y e_2 expresiones de L_a)

[187] $\vdash =^{\cdot}(\mathrm{con}_3(x,y,z), w) = \mathrm{coni}_4(x,y,z,w)$

[188] $\vdash \mathrm{TEO}(x) \rightarrow \mathrm{TEO}(\exists^{\cdot}(n,x))$

[189] $\vdash \exists^{\cdot}(1, \mathrm{coni}_4(\ulcorner \subset \urcorner, \mathrm{nml}(x_1), \ulcorner A \urcorner, \mathrm{nml}(0))) = \ulcorner \mathrm{TEO}(A) \urcorner$

<u>Proposición 28</u>.— Si f es una función recursiva primitiva de grado n, entonces $\vdash \mathrm{TEO}(=^{\cdot}(\mathrm{con}_{n+1}(\ulcorner f \urcorner, \mathrm{nml}(x_1), \ldots, \mathrm{nml}(x_n)), \mathrm{nml}(fx_1 \ldots x_n)))$. ∎

BIBLIOGRAFIA

Barwise, J. (editor)

Handbook of Mathematical Logic. Springer, 1977.

Boolos, George y Jeffrey, Richard.

Computability and Logic. Cambridge University Press, USA, 1974.

Delong, Howard.

A profile of Mathematical Logic. Addison-Wesley, USA, 1970.

Feferman, Salomon.

Aritmetization of Metamathematics in a general seting. *Fundamenta Mathematicae*, 1960.

Gödel, Kurt.

Obras Completas. Alianza Universidad, Madrid, 1981.

Hilbert, David y Bernays, Paul.

Grundlagen der Mathematik. Vol. I (1934), Vol. II (1939), Springer.

Kleene, Stephen C.

Introducción a la Metamatemática. Editorial Tecnos, Madrid, 1974.

Ladriere, Jean.

Limitaciones internas de los formalismos. Editorial Tecnos, Madrid, 1969.

Malitz, Jerome.

Introduction to Mathematical Logic. Springer-Verlag, Nueva York, 1979.

Margaris, Angelo.

First Order Mathematical Logic. Blaisdel Publishing Co. USA, 1967.

Mendelson, Elliot.

Introduction to Mathematical Logic. Van Nostrand Reinhold, Nueva York, 1964.

Monk, J. Donald.

Mathematical Logic. Springer-Verlag, Nueva York, 1976.

Robbin, Joel W.

Mathematical logic: a first course. W. A. Benjamin Inc. Nueva York, 1969.

Smorynski, C.

The Incompleteness Theorems. Artículo publicado en Barwise, J.

Torres Alcaraz, Carlos.

La Filosofía Formalista de la Matemática: el punto de vista de Hilbert. Tesis profesional para obtener el título de Matemático, Facultad de Ciencias, UNAM, 1978.

Curso de Lógica. Notas de clase reproducidas en *DITTO* para la materia de Lógica Matamática III, Departamento de Matemáticas, Facultad de Ciencias, UNAM.