24
2ej.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

UNA PRUEBA DE CONSISTENCIA DE LA ARITMETICA DE PEANO, DEL TIPO DE GENTZEN

T E S I S
QUE PARA OBTENER EL TITULO DE:
M A T E M A T I C O

P R E S E N T A:
FAVIO EZEQUIEL MIRANDA PEREA

DIRECTOR DE TESIS:
M. EN C. CARLOS TORRES ALCARAZ.

MEXICO, D.F. 1997

TESIS CON FALLA DE ORIGEN

UNIVERSIDAD NACIONAL
AUTÓNOMA DE
MÉXICO

M. en C. Virginia Abrín Batule
Jefe de la División de Estudios Profesionales de la
Facultad de Ciencias
P r e s e n t e

Comunicamos a usted que hemos revisado el trabajo de Tesis:

" Una Prueba de Consistencia de la Aritmética de Peano, del Tipo de Gentzen "

realizado por Favio Ezequiel Miranda Perea

con número de cuenta 8835427-9 **, pasante de la carrera de** Matemáticas

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis Propietario	M. en C. Carlos Torres Alcaraz	
Propietario	M. en C. Rafael Rojas Barbachano	RRB.
Propietario	Mat. José Matias Alvarado Mentado	
Suplente	M. en C. Maria Asunción Preisser Rodríguez	
Suplente	Mat. Fernando René Martínez Ortiz	

Virginia Abrín Batule
Consejo Departamental de Matemáticas

A mis queridos padres, Pascual Valente Miranda y Galván y
Ofelia Perea de Miranda.

Por su infinito e incondicional apoyo y cariño.

A mis maestros de Lógica Matemática y Teoría de los Conjuntos,
José Alfredo Amor Montaño, Rafael Rojas Barbachano y
Carlos Torres Alcaraz.

Por compartir sus conocimientos conmigo, pero principalmente por su invaluable amistad.

A la Palomilla de la Facultad de Ciencias, en especial a Fernando
Martínez, Diego Rojas y Francisco Ruíz.

Por los grandes momentos que hemos disfrutado juntos.

A mis Alumnos de la Facultad de Ciencias.

Por permitirme sentir la maravillosa experiencia de enseñar.

Prefacio

La Teoría de la Demostración es, junto con la teoría de modelos, una de las dos grandes ramas que conforman la Lógica Matemática. Dicha disciplina fue iniciada por *David Hilbert* en su afán de probar la consistencia de la Matemática Clásica. El trabajo de *Hilbert* fue continuado posteriormente por uno de sus asistentes en la universidad de Göttingen, el brillante matemático polaco *Gerhard Gentzen*.

El Presente trabajo cae en el marco de la teoria de la demostración tipo *Gentzen*, como se le llama en la actualidad, para distinguirla de otras escuelas, como la de *Gödel* y consiste en presentar una Prueba de Consistencia de la Aritmética de Peano (AP) basada en los artículos de *Gentzen*, de 1936, *Die Widerspruchsfreiheit der reinen Zahlentheorie (* La consistencia de la teoría de los números) y, de 1938, *Neue Fassung des Widerspruchsfreiheitbeweises für die reine Zahlentheorie (* Nueva versión de la prueba de consistencia de la teoría de los números) los cuales pueden considerarse como la simiente de la teoría de la demostración actual. Dichas pruebas, si bien no pueden ser finitistas, debido al primer teorema de incompletud de *Gödel*, estan muy cercanas al finitismo.

La prueba que presentamos, si bien esta basada en estos artículos, es mucho más accesible y clara que el original, el objetivo es que cualquier persona interesada en el tema pueda entenderla con los mínimos conocimientos necesarios, que son un curso de Lógica II en la Facultad de Ciencias o su equivalente.

Quiero agradecer profundamente al M. en C. Carlos Torres Alcaraz su apoyo en la corrección de estilo y en haberme proporcionado las obras de *Gentzen* sin las cuales hubiera sido imposible realizar este trabajo.

Pasamos ahora a describir el contenido del trabajo:

El trabajo consta de tres capítulos, en el primero se exponen el punto de vista finitista de *Hilbert* así como los conocimientos básicos necesarios para su comprensión. Se supone un conocimiento del cálculo de predicados clásico, a partir del cual se puede entender fácilmente lo que es el cálculo de secuentes, el cual utilizaremos a lo largo del trabajo. También se introducen algunos conceptos acerca de ordinales y se enuncian, de la manera más elemental, los teoremas de incompletud de *Gödel*. Si bien un conocimiento de teoría de conjuntos es deseable, no es indispensable.

En el capítulo dos se formaliza la aritmética informal en el sistema formal AP y posteriormente se prueba con detalle la consistencia de AP, dicha prueba de consistencia se sirve del concepto de accesibilidad de un ordinal, concepto que previamente explicamos en el mismo capítulo.

El tercer y último capítulo trata de la no demostrabilidad del principio de inducción transfinita hasta el ordinal ε_0 en AP, si bien tal resultado es evidente consecuencia del segundo teorema de incompletud de *Gödel*, aquí presentamos una prueba directa, basada en otro artículo de *Gentzen*, de 1943, *Beweisbarkeit und Unbeweisbarkeit von Anfangsfällen der transfiniten Induktion in der reinen Zahlentheorie* (Demostrabilidad y No Demostrabilidad del principio restringido dè inducción transfinita en la teoría elemental de los números).

Finalmente deseo que este trabajo sea de utilidad a alguien en el futuro.

Favio Ezequiel Miranda Perea.
Mayo de 1997.

Las Matemáticas son el arte del razonamiento, hasta el punto de que llegan a razonar sobre el razonamiento.

Contenido

Capítulo 1

PRELIMINARES

En este capítulo se exponen los conceptos preliminares necesarios para comprender los capítulos 2 y 3. Se supone que el lector tiene un conocimiento de la lógica clásica y la teoría de conjuntos elemental. En su mayor parte los resultados aquí expuestos no serán demostrados, por lo que el lector interesado podrá consultar las obras de referencia en la bibliografía.

1.1 ¿ Qué es la Teoría de la Demostración?

La afirmación de que una teoría matemática es consistente constituye una proposición acerca de las pruebas posibles de dicha teoría; lo que esta afirmación "dice" es: "ninguna prueba de esta teoría nos lleva a una contradicción".

Para poder llevar a cabo una prueba de consistencia de una teoría en particular, tenemos que tratar sus pruebas como objeto de nuestro estudio, formándose de esta manera una nueva teoría. La teoría matemática que tiene como objeto de estudio las pruebas matemáticas sin importar a que teoría pertenecen, es llamada Teoría de la Demostración. Una proposición perteneciente a la teoría de la demostración es, por ejemplo, el principio de dualidad de la geometría proyectiva, el cual nos dice que a partir de cualquier teorema, si reemplazamos la palabra "punto" por "recta" y viceversa obtenemos otro teorema. Este ejemplo nos muestra que la teoría de la demostración versa en gran medida sobre teorías de la matemática cotidiana.

Ordinariamente las pruebas matemáticas están expresadas en nuestro lenguaje cotidiano, en este caso el español. Dada su ambigüedad y, en gran medida, su imperfección, antes de someter las demostraciones a un examen riguroso es necesario formalizarlas, para resaltar su estructura lógica. Para ello utilizaremos la lógica matemática, reemplazando las palabras con el simbolismo lógico y las formas de razonamiento con las reglas formales de inferencia. Surge aquí la pregunta, ¿ Cómo puede llevarse a cabo una Prueba de Consistencia utilizando la Teoría de la Demostración ? la idea subyacente a la teoría de la demostración es que las pruebas formales son siempre decidibles, es decir, siempre se puede decidir de manera efectiva si una combinación de símbolos e inferencias lógicas es o no una demostración. Surge aquí las posibilidad de establecer que entre todas las posibles pruebas no existe ninguna que nos lleve a contradicciones, lo cual es una propiedad simple verificable para cualquier prueba dada.

Toda prueba de consistencia es una demostración matemática, en la cual se usan ciertos conceptos e inferencias, cuya credibilidad y consistencia debió haber sido presupuesta. *Kurt Gödel* nos enseña que la herramienta utilizada en las pruebas de consistencia de las teorías matemáticas de mayor interés (la aritmética de Peano o la teoría de conjuntos, por ejemplo) no puede ser formalizada en la teoría. Esto significa que para algunas teorías, no puede haber una prueba absoluta de consistencia. Este resultado, llamado el segundo teorema de incompletud, no es nada trivial y fue demostrado por *Gödel* en 1931, más adelante en este capitulo hablaremos un poco de dicho teorema. Así que una prueba de consistencia solamente reduce la aceptabilidad de ciertas formas de inferencia a la correctitud de otras formas de inferencia. Por lo tanto, es claro que en una prueba de consistencia no podemos utilizar solamente formas de razonamiento que parezcan considerablemente "mas seguras" que las formas de inferencia usadas en la teoría de la cual estamos demostrando la consistencia.

1.2 El Finitismo Hilbertiano

En el año 1900, en el congreso internacional de Matemáticas de París, *David Hilbert*, uno de los mas grandes matemáticos de todos los tiempos, presento una lista de 23 problemas que el creía serían el motor de la matemática en el siglo XX; el segundo de estos problemas consistía en investigar la no-contradicción o consistencia de los Axiomas de la Aritmética. En la década de los años veinte, propuso que para tal fin la herramienta matemática se limitase a lo que el llamó métodos ***finitistas***.

Si bien el concepto de método *finitista* nunca ha tenido una definición formal, trataremos de explicar, dando un par de citas, lo que se entiende por él:

1) *Carlos Torres, La Filosofía y el Programa de Hilbert*, en [To1].

Hilbert propuso el proyecto filosófico de fundamentar la matemática en la intuición pura del signo, para lo cual elaboro un programa que se puede resumir de la siguiente forma:

1) Formalizar la Matemática Clásica.
2) Demostrar que la formalización es (semanticamente) completa.[1]
3) Demostrar con métodos finitistas que la formalización es consistente.

Aquí, por finitismo o matemática finitista se entiende un razonamiento intuitivo que tiene origen en las nociones descriptivas y que procede sin presupuestos axiomaticos. Este razonamiento consiste en la reflexión directa acerca de objetos presentes en la intuición como experiencia inmediata previa a todo pensamiento.

La siguiente cita del mismo *Hilbert*, debe servir como ilustración del tipo de criterio de credibilidad que *Gentzen* adopto como el punto de vista finitista:

2) *Hilbert & Bernays, Grundlagen der Mathematik*:

"Nuestra revisión de los principios de la Teoría de los Números y del Álgebra ha permitido elucidar en su aplicación y uso el razonamiento directo e informal, libre de hipótesis axiomaticas, como se lleva a cabo en experimentos del pensamiento en términos de objetos concebidos intuitivamente.

A este tipo de razonamiento le llamaremos, para darle una expresión concisa, razonamiento finitista y también designaremos como actitud finitista o punto de vista finitista a la actitud metodológica que encierra a este razonamiento.

Igualmente hablaremos de conceptos y afirmaciones finitisticamente especificados, expresando con la palabra "finitista" en cada caso el hecho de que la deliberación, afirmación o definición cae dentro de los limites de la concepción, en principio, de objetos, así como la factibilidad, en principio, de procesos y por lo tanto cae dentro del dominio de consideraciones concretas."

[1]Semánticamente completa: que a cada enunciado verdadero de la matemática clásica le corresponda una fórmula derivable en el sistema formal.

Esta cita no intenta dar a entender que una definición formal del punto de vista finitista ha sido dada o que tal definición puede darse. *Gentzen* puntualiza que no puede ser demostrado que sus técnicas de demostración sean finitistas, puesto que este concepto no está definido formalmente y no puede ser delimitado de esta manera. Remarca que todo lo que puede lograrse en relación a esto es que las inferencias individuales sean examinadas desde el punto de vista finitista y que debe ser evaluado individualmente si las inferencias en cuestión están en armonía con las intenciones finitistas.

En las siguientes secciones definimos las herramientas necesarias de lógica y teoría de conjuntos.

1.3 Ordinales

A continuación trataremos de manera mas bien intuitiva y con un mínimo de tecnicismos algunos conceptos acerca de números ordinales los cuales se pueden tratar con todo rigor utilizando la teoría de Zermelo-Fraenkel con Axioma de Elección (ZFE). Para cualquier aclaración se recomienda consultar [End1] o [Hrb].

La teoría general de ordinales constituye una parte muy importante de la teoría de conjuntos de Cantor (ZFE). No obstante, aquí no la desarrollaremos formalmente, sino que nos limitaremos a dar ciertas definiciones intuitivas que serán necesarias.

Intuitivamente los números ordinales son una generalización de los números naturales, al punto que los números naturales son los llamados ordinales finitos: $0, 1, 2, 3, \ldots, n, \ldots$;inmediatamente después de todos ellos introducimos el primer ordinal infinito denotado con la letra griega ω (omega) que es realmente el conjunto de los números naturales, i.e., $\omega = \mathbb{N}$. Un ordinal de gran importancia para nuestro desarrollo posterior es ε_0 (épsilon cero) el cual tiene la propiedad de ser el primer ordinal solución de la ecuación $\omega^x = x$.

Pero como pretendemos apegarnos lo más posible al punto de vista finitista, lo que haremos aquí es dar una definición recursiva de ordinales, completamente independiente de la construcción conjuntista, ya que de otra forma nos estaríamos basando en una teoría (ZFE) que esta muy lejos de los métodos finitistas, puesto que en ella se puede formalizar toda la matemática.

DEFINICIÓN. (Recursiva de ordinal)

i) 0 es ordinal.

ii) Si $\mu, \mu_1, ..., \mu_n$ son ordinales entonces ω^μ y $\mu_1 + ... + \mu_n$ son ordinales.

iii) Son todos.

Debe aclararse que esta definición solamente genera a los ordinales **menores que** ε_0.

Las relaciones $=$ y $<$ se pueden definir de manera que sean equivalentes a la igualdad y al orden usual de los ordinales construidos en la teoría de conjuntos, así que podemos desarrollar toda la teoría de ordinales menores que ε_0 mediante métodos finitistas.

NOTA: De aquí en adelante por ordinal entenderemos ordinal menor que ε_0. A los ordinales los denotaremos por letras griegas minúsculas $\alpha, \beta, \gamma, \mu, \nu$. A continuación daremos la definición formal de ε_0.

DEFINICIÓN. (Por recursión para naturales) $\omega_0 = 0, \ \ \omega_{n+1} = \omega^{\omega_n}$.

DEFINICIÓN. $\varepsilon_0 = Sup\ \{\omega_0, \omega_1, \omega_2, ..., \omega_n, ...\} = Sup\ \{0, 1, \omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, ...\}$

Con ORD denotaremos al conjunto de todos los ordinales (menores que ε_0), i.e.,

$$ORD = \{\alpha \mid \alpha \text{ es un ordinal y } \alpha < \varepsilon_0\}.$$

1.3.1 Aritmética Ordinal

Las siguientes propiedades de aritmética ordinal se emplearan a lo largo de la exposición:

OR1) La relación de orden " $<$ " es un orden total para ORD y 0 es su elemento mínimo[2].

OR2) Sean $\alpha, \beta \in ORD$, entonces $\alpha < \beta \Leftrightarrow \omega^\alpha < \omega^\beta$.

OR3) La suma y el producto de ordinales son asociativos.

OR4) Para todo $\alpha, \beta, \gamma \in ORD$, entonces $\alpha + \gamma < \beta + \gamma \Rightarrow \alpha < \beta$.

OR5) Para todo $\alpha, \beta \in ORD$, entonces, $\alpha \leq \beta \Rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma$ y $\alpha < \beta, \gamma > 0 \Rightarrow \gamma \cdot \alpha < \gamma \cdot \beta$.

OR6) (Teorema de la Forma Normal de Cantor (FNC)). Todo ordinal $\alpha \neq 0$, se puede escribir de forma única en la forma $\alpha = \omega^{\alpha_1} + \omega^{\alpha_2} + ... + \omega^{\alpha_n}$, para algunos ordinales $\alpha_1 \geq .... \geq \alpha_n$ y $n \in \mathbb{N}$. En tal caso decimos que $\omega^{\alpha_1} + \omega^{\alpha_2} + ... + \omega^{\alpha_n}$ es la Forma Normal de Cantor (FNC) de α.

OR7) Si $\alpha = \omega^{\alpha_1} + \omega^{\alpha_2} + ... + \omega^{\alpha_n}, \beta = \omega^{\beta_1} + \omega^{\beta_2} + ... + \omega^{\beta_m}$ son Formas Normales de Cantor.

[2] Nótese que no estamos pidiendo que $<$ sea un buen orden.

Entonces

$$\alpha < \beta \Leftrightarrow \begin{cases} \omega^{\alpha_i} < \omega^{\beta_i} \text{ para algúna } i \text{ y } \omega^{\alpha_j} = \omega^{\beta_j} \text{ para toda } j < i, \text{ ó} \\ \omega^{\alpha_i} = \omega^{\beta_i}, \text{para toda } i \leq n \text{ y } n < m \end{cases}$$

OR8) Si $\alpha = \omega^{\alpha_1} + \omega^{\alpha_2} + ... + \omega^{\alpha_n}$, es la FNC de α y $\nu \neq 0$, entonces $\alpha \cdot \omega^{\nu} = \omega^{\alpha_1 + \nu}$.

OR9) Si $\alpha = \omega^{\alpha_1} + \omega^{\alpha_2} + ... + \omega^{\alpha_n}, \beta = \omega^{\beta_1} + \omega^{\beta_2} + ... + \omega^{\beta_m}$ son FNC, entonces $\alpha \cdot \beta = \alpha \cdot \omega^{\beta_1} + \alpha \cdot \omega^{\beta_2} + ... + \alpha \cdot \omega^{\beta_m}$.

OR10) Si $\alpha = \omega^{\alpha_1} + \omega^{\alpha_2} + ... + \omega^{\alpha_n}$ es una FNC entonces $\alpha < \omega^{\alpha_1 + 1}$.

OR11) Si $\alpha, \beta, \gamma \in ORD$ son tales que $\alpha \leq \beta < \gamma$, entonces existe $\gamma_0 \in ORD, \gamma_0 < \gamma$ tal que $\beta = \alpha + \gamma_0$.

OR12) Si $\alpha, \beta \in ORD$ son tales que $\alpha < \beta \cdot \omega$, entonces existe $n < \omega$ tal que $\alpha < \beta \cdot n$.

OR13) Si $\alpha \in ORD$ entonces existe $n < \omega$ tal que $\alpha < \omega_n$.

A continuación definimos una operación muy especial entre ordinales llamada la suma natural, la cual denotaremos con $\oplus$ y solo sera aplicada a ordinales en FNC.

Sean $\alpha = \omega^{\alpha_1} + \omega^{\alpha_2} + ... + \omega^{\alpha_n}$ y $\beta = \omega^{\beta_1} + \omega^{\beta_2} + ... + \omega^{\beta_m}$ ordinales en FNC. Definimos la suma natural de α y β como $\alpha \oplus \beta = \omega^{\lambda_1} + \omega^{\lambda_2} + ... + \omega^{\lambda_{m+n}}$ donde $\lambda_1 \geq .... \geq \lambda_{m+n}$ y $\lambda_j = \alpha_i$ ó $\lambda_j = \beta_k$ para alguna $i \leq n$ ó $k \leq m$. Un par de propiedades de la suma natural son las siguientes:

OR14) La suma natural es conmutativa, i.e. $\alpha \oplus \beta = \beta \oplus \alpha$.

OR15) La suma natural es monótona, i.e. Si $\alpha < \beta$ entonces $\alpha \oplus \gamma < \beta \oplus \gamma$.

1.4 Lógica Matemática

Para cualquier duda de lógica elemental que no sea contestada con lo que se plantea en esta sección se recomienda consultar [End2] o [Men].

El primer paso para formular la lógica es precisar lo que entendemos por lenguaje y expresiones formales.

DEFINICIÓN. Un lenguaje formal de primer orden $\mathfrak{L}$ consta de los siguientes conjuntos de símbolos:

i) Símbolos Lógicos: Conectivos: $\neg, \vee, \wedge, \rightarrow$,

Cuantificadores: $\forall, \exists$.

ii) Símbolo de igualdad: $=$

iii) Variables: $x_0, x_1, \ldots\ldots, x_n, \ldots\ldots$

iv) Símbolos Auxiliares: Paréntesis izquierdo (, Paréntesis derecho) y Coma ,

v) Letras Predicativas: R_j^n donde $n, j \in \mathbb{N}$ y n indica la aridad de la relación.

vi) Letras funcionales: f_j^n donde $n, j \in \mathbb{N}$ y n indica la aridad de la función.

vii) Constantes Individuales: $c_0, c_1, \ldots\ldots, c_n, \ldots$

La condición ii) no es necesaria en la definición de lenguaje, si se pide entonces diremos que el lenguaje $\mathfrak{L}$ tiene igualdad.

Hasta aquí solo tenemos un conjunto de símbolos. Ahora daremos ciertas definiciones sobre cómo se combinan los símbolos, las cuales constituyen la gramática del lenguaje $\mathfrak{L}$.

DEFINICIÓN. Una expresión de $\mathfrak{L}$ es cualquier sucesión finita de símbolos de $\mathfrak{L}$.

DEFINICIÓN. (Recursiva de término)

i) Las variables y las constantes son términos.

ii) Si f^m es una letra funcional de aridad m y si $t_1, \ldots\ldots, t_m$ son términos entonces $f^m(t_1, \ldots\ldots, t_m)$ es un término.

iii) Son todos.

DEFINICIÓN. (Fórmula Atómica)Si $t_1, \ldots\ldots, t_m$ son términos entonces:

i) $t_1 = t_2$ es una fórmula atómica.

ii) Si R^m es una letra predicativa de aridad m entonces $R^m(t_1, \ldots\ldots, t_m)$ es una fórmula atómica.

iii) Son todas.

DEFINICIÓN. (Recursiva de Fórmula)

i) Las atómicas son fórmulas .

ii) Si A, B son fórmulas entonces $(\neg A), (A \wedge B), (A \vee B), (A \Rightarrow B), (\forall x_i A)$ y $(\exists x_j B)$ son fórmulas .

iii) Son Todas.

DEFINICIÓN. En las fórmulas $\forall x_i A$ y $\exists x_j B$, A y B se llaman respectivamente el alcance del cuantificador $\forall x_i$ y $\exists x_j$.

DEFINICIÓN. (Variables libres y acotadas)
Diremos que una presencia de la variable x_i en la fórmula A esta acotada syss[3]

i) x_i es la variable de un cuantificador o

ii) x_i esta dentro del alcance de un cuantificador.

En otro caso diremos que tal presencia es libre.

DEFINICIÓN. (Término Cerrado)
Un término t se dice cerrado syss en el no figuran variables. En los demás casos diremos que el término t es abierto.

Ahora lo único que falta por precisar es lo que entenderemos por una derivación o prueba formal. Para ello debemos especificar cuales son las reglas para manipular fórmulas, es decir, cuales son las reglas de inferencia. Un lenguaje junto con sus fórmulas y sus reglas de inferencia constituyen lo que se llama un Sistema Formal. El sistema formal que nosotros usaremos es el sistema LK (*Logistischer klassischer Kalkül*) de *Gentzen*. Para formular nuestro sistema LK necesitaremos el símbolo auxiliar $\rightarrow$ que no debemos confundir con el símbolo de implicación $\Rightarrow$. El símbolo $\rightarrow$ es llamado "símbolo de secuente".

NOTA: En lo que sigue las letras griegas mayúsculas $\Gamma, \Gamma_0, \Delta, \Pi, \Lambda, \Sigma$. etc..., denotaran sucesiones finitas (posiblemente vacías) de fórmulas separadas por comas.

DEFINICIÓN. Sean Γ, Δ sucesiones de fórmulas. El esquema $\Gamma \rightarrow \Delta$ se llama secuente. A Γ se le llama el antecedente del secuente, a Δ se le llama el consecuente del secuente y cada fórmula de Γ y Δ se llama fórmula del secuente.

Intuitivamente un secuente $A_0, A_1, \ldots.., A_n \rightarrow B_0, B_1, \ldots.., B_m$ (con $n, m \geq 0$) es equivalente a la formula: $A_0 \wedge A_1 \wedge \ldots.. \wedge A_n \Rightarrow B_0 \vee B_1 \vee \ldots.. \vee B_m$, es decir, a la fórmula que "afirma" que si es cierto que $A_0 \wedge A_1 \wedge \ldots.. \wedge A_n$ entonces necesariamente sera cierto que $B_0 \vee B_1 \vee \ldots.. \vee B_m$.

[3]Abreviaremos de ahora en adelante con syss a la frase "si y solo si"

Con "$A_0, A_1, ..., A_n \rightarrow$ " queremos decir que $A_0 \wedge A_1 \wedge ..... \wedge A_n$ nos lleva a una contradicción y con " $\rightarrow B_0, B_1, ..., B_m$" que $B_0 \vee B_1 \vee ..... \vee B_m$ se cumple.

DEFINICIÓN. El secuente vacío $\emptyset \rightarrow \emptyset$ será denotado simplemente con el símbolo $\rightarrow$ y significa que hay una contradicción. Los secuentes se denotaran con la letra S con o sin subindices.

DEFINICIÓN. Una inferencia (regla de inferencia) es un esquema de la siguiente forma:

$$\frac{S_1}{S} \text{ ó } \frac{S_1 \quad S_2}{S}$$

donde S_1, S_2 y S son secuentes. S_1, S_2 son los secuentes superiores de la inferencia y S es el secuente inferior de la inferencia.

Intuitivamente este esquema significa que cuando S_1 y S_2 son ciertos, de ellos podemos inferir S.

1.4.1 Reglas de Inferencia del Sistema Formal LK de *Gentzen*

Nos restringiremos a las siguientes reglas de inferencia. En lo que sigue $A, B, C, D, F(a)$ denotan fórmulas .

1) Reglas Estructurales

1.1) Debilitamiento o Dilución:

$$Izquierda : \frac{\Gamma \rightarrow \Delta}{D, \Gamma \rightarrow \Delta} \text{ (DIL-I)} \qquad Derecha : \frac{\Gamma \rightarrow \Delta}{\Gamma \rightarrow \Delta, D} \text{ (DIL-D)}$$

D se llama fórmula debilitadora

1.2) Contracción o Consolidación:

$$Izquierda : \frac{D, D, \Gamma \rightarrow \Delta}{D, \Gamma \rightarrow \Delta} \text{ (CON-I)} \qquad Derecha : \frac{\Gamma \rightarrow \Delta, D, D}{\Gamma \rightarrow \Delta, D} \text{ (CON-D)}$$

1.3) Intercambio:

$$Izquierda : \frac{\Gamma, C, D, \Pi \rightarrow \Delta}{\Gamma, D, C, \Pi \rightarrow \Delta} \text{ (INT-I)} \qquad Derecha : \frac{\Gamma \rightarrow \Delta, C, D, \Lambda}{\Gamma \rightarrow \Delta, D, C, \Lambda} \text{ (INT-D)}$$

A estas tres reglas se les llama reglas débiles, mientras que las siguientes serán llamadas reglas fuertes:

1.4) Regla de Corte

$$\frac{\Gamma \to \Delta, D \quad D, \Pi \to \Lambda}{\Gamma, \Pi \to \Delta, \Lambda} \ (CTE)$$

a D se le llama la fórmula de corte.

2) Reglas Lógicas u Operacionales.

2.1) Negación

$$Izquierda : \frac{\Gamma \to \Delta, D}{\neg D, \Gamma \to \Delta} \ (NEG\text{-}I) \quad Derecha : \frac{D, \Gamma \to \Delta}{\Gamma \to \Delta, \neg D} (NEG\text{-}D)$$

D es la fórmula auxiliar de esta inferencia y $\neg D$ es la fórmula principal.

2.2) Disyunción:

$$\begin{aligned} Izquierda &: \frac{C, \Gamma \to \Delta \quad D, \Gamma \to \Delta}{C \vee D, \Gamma \to \Delta} \ (DISY\text{-}I) \\ Derecha &: \frac{\Gamma \to \Delta, C}{\Gamma \to \Delta, C \vee D} \text{ y } \frac{\Gamma \to \Delta, D}{\Gamma \to \Delta, C \vee D} \ (DISY\text{-}D) \end{aligned}$$

C y D son las fórmulas auxiliares y $C \vee D$ es la fórmula principal de esta inferencia.

2.3) Cuantificación Universal ($\forall$):

$$Izquierda : \frac{F(t), \Gamma \to \Delta}{\forall x F(x), \Gamma \to \Delta} \ (UNIV\text{-}I) \quad Derecha : \frac{\Gamma \to \Delta, F(a)}{\Gamma \to \Delta, \forall x F(x)} \ (UNIV\text{-}D)$$

donde t es un término arbitrario, a una variable y no hay presencias de a en el secuente inferior. $F(t)$ y $F(a)$ son las fórmulas auxiliares y $\forall x F(x)$ la fórmula principal de esta inferencia. La a en $UNIV\text{-}D$ es llamada la *eigenvariable* o variable propia de esta inferencia.

3) Reglas Derivadas.

Usaremos también las siguientes reglas derivadas, aunque nuestro lenguaje consta de todos los conectivos, solo consideraremos como primitivos a $\neg, \vee, \forall$, los demás conectivos, a saber $\wedge, \Rightarrow$ y $\exists$ se introducen como abreviaturas, $A \wedge B$ abrevia a $\neg(\neg A \vee \neg B)$, $\exists x F(x)$ abrevia a $\neg\forall x \neg F(x)$ y $A \Rightarrow B$ abrevia a $\neg A \vee B$

3.1) Conjunción:

$$\begin{array}{rcl} \textit{Izquierda} & : & \dfrac{C, \Gamma \to \Delta}{C \wedge D, \Gamma \to \Delta} \text{ y } \dfrac{D, \Gamma \to \Delta}{C \wedge D, \Gamma \to \Delta} \; (\textit{CONJ-I}) \\ \textit{Derecha} & : & \dfrac{\Gamma \to \Delta, C \quad \Gamma \to \Delta, D}{\Gamma \to \Delta, C \wedge D} \; (\textit{CONJ-D}) \end{array}$$

C y D son las fórmulas auxiliares y $C \wedge D$ es la fórmula principal de esta inferencia.

3.2) Implicación:

$$\begin{array}{rcl} \textit{Izquierda} & : & \dfrac{\Gamma \to \Delta, C \quad D, \Pi \to \Lambda}{C \Rightarrow D, \Gamma, \Pi \to \Delta, \Lambda} \; (\textit{IMP-I}) \\ \textit{Derecha} & : & \dfrac{C, \Gamma \to \Delta, D}{\Gamma \to \Delta, C \Rightarrow D} \; (\textit{IMP-D}) \end{array}$$

C y D son las fórmulas auxiliares y $C \Rightarrow D$ es la fórmula principal de esta inferencia.

3.3) Cuantificación Existencial ($\exists$):

$$\begin{array}{rcl} \textit{Izquierda} & : & \dfrac{F(a), \Gamma \to \Delta}{\exists x F(x), \Gamma \to \Delta} \; (\textit{EXIST-I}) \\ \textit{Derecha} & : & \dfrac{\Gamma \to \Delta, F(t)}{\Gamma \to \Delta, \exists x F(x)} \; (\textit{EXIST-D}) \end{array}$$

donde t es un término arbitrario, a es una variable y no hay presencias de a en el secuente inferior. $F(t)$ y $F(a)$ son las fórmulas auxiliares y $\exists x F(x)$ la fórmula principal de esta inferencia. La a en *EXIST-I* es llamada la *eigenvariable* o variable propia de esta inferencia.

Dichas reglas se llaman derivadas porque pueden ser obtenidas de las reglas anteriores por medio de una sencilla derivación, cómo mas adelante veremos.

Una vez definidas las reglas de inferencia, procedemos a definir los secuentes que serán considerados como axiomas del sistema, para lo cual damos la siguiente

DEFINICIÓN. (Axioma o Secuente Inicial)

Un secuente es axioma o secuente inicial syss tiene alguna de las siguientes formas:

i) $A \rightarrow A$

ii) $\rightarrow t = t$, donde t es un término cualquiera.

iii) $s_1 = t_1, ..., s_n = t_n \rightarrow f(s_1, ..., s_n) = f(t_1, ..., t_n)$, donde s_i, t_i son términos cualesquiera y f es una letra funcional cualquiera de aridad n.

iv) $s_1 = t_1, ..., s_n = t_n, R(s_1, ..., s_n) \rightarrow R(t_1, ..., t_n)$, donde s_i, t_i son términos cualesquiera y R es una letra predicativa cualquiera de aridad n.

A los axiomas de la forma ii),iii) o iv) se les llama axiomas de igualdad.

Por ultimo definiremos lo que es una derivación o prueba formal en el sistema LK, lo cual se conoce brevemente como LK-derivación.

DEFINICIÓN. Una derivación P es un árbol de secuentes que satisface las siguientes condiciones:

i) Los secuentes en el ultimo nivel del árbol son axiomas.

ii) En el primer nivel del árbol solo hay un secuente llamado el secuente final.

iii) Cada secuente del árbol excepto el secuente final es secuente superior de alguna inferencia, cuyo secuente inferior también pertenece a P.

Una derivación que tiene a S como secuente final es una derivación o prueba de S; un secuente S se dice derivable o demostrable syss existe una derivación de S. Una fórmula A se dice derivable o demostrable syss el secuente $\rightarrow A$ es demostrable.

La notación

$$P : \begin{array}{c} \ddots \vdots \cdot^{\cdot^{\cdot}} \\ \Gamma \rightarrow \Delta \end{array}$$

denota a una derivación P del secuente $\Gamma \rightarrow \Delta$.

Como ejemplo de una derivación, obtendremos la demostración de que las fórmulas A y $\neg\neg A$ son equivalentes (lo cual se denota $A \equiv \neg\neg A$) i.e., que los secuentes $A \rightarrow \neg\neg A$ y $\neg\neg A \rightarrow A$ son derivables:

i) $A \rightarrow \neg\neg A$

$$\frac{A \rightarrow A}{A, \neg A \rightarrow} \ (NEG\text{-}I)$$

$$\frac{A, \neg A \rightarrow}{A \rightarrow \neg\neg A} \ (NEG\text{-}D)$$

i) $\neg\neg A \rightarrow A$

$$\frac{A \rightarrow A}{\rightarrow A, \neg A} \ (NEG\text{-}D)$$

$$\frac{\rightarrow A, \neg A}{\neg\neg A \rightarrow A} \ (NEG\text{-}I)$$

De i) y ii) concluimos que $A \equiv \neg\neg A$. Como se puede observar, hemos repetido algunos secuentes por dos razones: para que sea más clara la comprensión de la derivación presentando inferencias completas y por razones tipográficas, esto lo seguiremos haciendo la mayoría de las veces puesto que no representa problema alguno.

Como segundo ejemplo demostraremos una de las reglas derivadas, digamos *IMP-I*. Al quitar la abreviatura *IMP-I* se obtiene de *DIL*, *INT*[4], *DISY-I* y de *NEG-I*:

$$\frac{\Gamma \rightarrow \Delta, C}{\neg C, \Gamma \rightarrow \Delta} \ (NEG\text{-}I)$$

$$\frac{\neg C, \Gamma \rightarrow \Delta}{\neg C, \Gamma, \Pi \rightarrow \Delta, \Lambda} \ (DIL \ e \ INT) \quad \frac{D, \Pi \rightarrow \Lambda}{D, \Gamma, \Pi \rightarrow \Delta, \Lambda} \ (DIL \ e \ INT)$$

$$\frac{\neg C, \Gamma, \Pi \rightarrow \Delta, \Lambda \qquad D, \Gamma, \Pi \rightarrow \Delta, \Lambda}{\neg C \vee D, \Gamma, \Pi \rightarrow \Delta, \Lambda} \ (DISY\text{-}I)$$

Y este ultimo secuente es, utilizando la abreviatura: $C \Rightarrow D, \Gamma, \Pi \rightarrow \Delta, \Lambda$, por lo que la regla *IMP-I* es válida.

Para terminar esta sección mencionaremos (sin demostrarlo) un resultado que relaciona los sistemas de deducción H del tipo de Hilbert con los sistemas de secuentes de *Gentzen*.

[4] Aquí las reglas DIL e INT se utilizan tantas veces como sea necesario para igualar las formulas en ambos secuentes y poder aplicar la regla DISY-I.

PROPOSICIÓN. Sea A una fórmula cualquiera en un lenguaje de primer orden, entonces:

$$\vdash_H A \text{ syss } \vdash_{LK} \rightarrow A$$

Cualquier duda posterior sobre el cálculo de secuentes se puede consultar en [Tak] o en [Kle].

1.5 Definiciones Relativas a Fórmulas y Secuentes dentro de una Derivación

Cuando consideremos una fórmula o un símbolo lógico junto con el lugar que ocupa en una derivación, un secuente o una fórmula, hablaremos de la fórmula o el símbolo lógico de la derivación en el secuente o en la fórmula, respectivamente. Una fórmula en un secuente es llamada **fórmula-secuente.**

Sucesor de una Fórmula. Si una fórmula A pertenece a un secuente superior de alguna inferencia, entonces el sucesor de A se define como sigue:

1) Si A es una fórmula de corte, entonces A no tiene sucesor. Esta definición es intuitivamente obvia, pues en tal caso A desaparece.

2) Si A es la fórmula denotada por C (D respectivamente) en el secuente superior de un intercambio ($\frac{\Gamma,C,D,\Pi\rightarrow\Delta}{\Gamma,D,C,\Pi\rightarrow\Delta}$), entonces la C (D respectivamente) en el secuente inferior es el sucesor de A.

3) Si A es la k-esima fórmula en la lista Γ (respectivamente Π, Δ, Λ) de un secuente superior de una inferencia, entonces el sucesor de A es la k-esima fórmula en la lista Γ (respectivamente Π, Δ, Λ) del secuente inferior de la misma inferencia.

4) Si A no cae en ninguno de los casos anteriores, entonces A es una fórmula auxiliar en el secuente superior de una inferencia y su sucesor será la fórmula principal de dicha inferencia.

Predecesor: Si A es el sucesor de B entonces decimos que B es el predecesor de A. Nótese que algunas fórmulas pueden tener dos predecesores (por ejemplo la fórmula principal de una inferencia *CONJ-D)* en cuyo caso al de la izquierda se le llama primer predecesor y al de la derecha segundo predecesor.

Ejemplo:

$$\frac{\Gamma \to \Delta, \mathbf{A}}{\underbrace{\neg\mathbf{A}}_{\text{Sucesor de } A}, \Gamma \to \Delta} \qquad \frac{\mathbf{C}, \Gamma \to \Delta \quad D, \Gamma \to \Delta}{\underbrace{\mathbf{C} \vee \mathbf{D}}_{\text{Sucesor de } C}, \Gamma \to \Delta}$$

$$\frac{\overbrace{\mathbf{A}}^{\text{Predecesor de } A\wedge B}, \Gamma \to \Delta}{\mathbf{A} \wedge \mathbf{B}, \Gamma \to \Delta}$$

Rama de secuentes: Una sucesión de secuentes dentro de una derivación se dice que es una **rama** syss:

i) La sucesión empieza con un axioma y termina con el secuente final.

ii) Cada secuente en la sucesión (excepto el secuente final) es un secuente superior de alguna inferencia y esta inmediatamente seguido por su secuente inferior.

Ejemplo:

$$\frac{\dfrac{\dfrac{\dfrac{\mathbf{B} \to \mathbf{B}}{\mathbf{A}, \mathbf{B} \to \mathbf{B}}}{\mathbf{A}, \mathbf{B} \to \mathbf{B}, \mathbf{C}}}{\mathbf{B}, \mathbf{A} \to \mathbf{C}, \mathbf{B}} \qquad \dfrac{\dfrac{\dfrac{C \to C}{A, C \to C}}{B, A, C \to C}}{C, B, A \to C}}{\mathbf{B} \Rightarrow \mathbf{C}, \mathbf{B}, \mathbf{A} \to \mathbf{C}}$$

los secuentes en negritas constituyen una rama.

Los conceptos Arriba,Abajo y En Medio: Dados dos secuentes S_1 y S_2 en una derivación P, decimos que S_1 esta arriba de S_2 o que S_2 esta abajo de S_1 syss hay una rama a la cual pertenecen ambos secuentes de tal manera que S_1 aparece antes que S_2. Cabe señalar que nunca hay secuentes arriba de los axiomas, ni abajo del secuente final.

Si un secuente S esta abajo de S_1 y arriba de S_2 decimos que S esta en medio de S_1 y S_2.

Una inferencia esta abajo de un secuente S syss su secuente inferior esta bajo S. En particular cualquier inferencia esta bajo su secuente superior. En el ejemplo anterior el secuente

$A, B \to B, C$ esta abajo de $A, B \to B$, el secuente $A, B \to B, C$ esta arriba de $B, A \to C, B$ y el secuente $B, A \to C, B$ esta entre los secuentes $A, B \to B$ y $B \Rightarrow C, B, A \to C$.

Fórmula Inicial y Fórmula Final: una fórmula A dentro de una derivación se llama fórmula inicial (final) syss pertenece a un axioma o secuente inicial (secuente final).

Haz de Fórmulas y los conceptos Explícito e Implícito: Una sucesión de fórmulas dentro de una derivación se llama un haz syss cumple las siguientes propiedades:

i) La sucesión empieza con una fórmula inicial o una fórmula debilitadora.

ii) La sucesión termina con una fórmula final o fórmula de corte.

iii) Cada fórmula de la sucesión, excepto la última es seguida inmediatamente por su sucesor.

Un **haz** se llama **explícito (implícito)** syss termina en una fórmula final (fórmula de corte); una fórmula dentro de una derivación se llama **explícita (implícita)** syss los haces que la contienen son explícitos (implícitos); Un **secuente** dentro de una derivación se llama **explícito (implícito)** syss contiene una fórmula explícita (implícita); una **inferencia lógica** se llama **explícita (implícita)** syss su fórmula principal es explícita (implícita).

Ejemplo:

$$\begin{array}{c}
\begin{array}{cc}
\begin{array}{c}
\underline{A} \to A \\ \hline
\underline{A}, \neg A \to \\
\underline{A}, \neg A \to \\ \hline
\underline{A \wedge B}, \neg A \to \\
\underline{A \wedge B}, \neg A \to \\ \hline
\neg A \to \underline{\neg(A \wedge B)} \\
\neg A \to \underline{\neg(A \wedge B)}
\end{array}
&
\begin{array}{c}
B \to \mathbf{B} \\ \hline
B, \neg\mathbf{B} \to \\
B, \neg\mathbf{B} \to \\ \hline
A \wedge B, \neg\mathbf{B} \to \\
A \wedge B, \neg\mathbf{B} \to \\ \hline
\neg\mathbf{B} \to \neg(A \wedge B) \\
\neg\mathbf{B} \to \neg(A \wedge B)
\end{array}
\end{array} \\ \hline
\neg\mathbf{A} \vee \neg\mathbf{B} \to \underline{\neg(A \wedge B)}
\end{array}$$

Aquí las fórmulas subrayadas y las fórmulas en negritas constituyen dos haces, ambos explícitos.

Ancestro y Descendiente: Sean A, B fórmulas. Decimos que A es un ancestro de B y que B es un descendiente de A syss hay un haz al que pertenecen A y B, en el cual A aparece arriba de B.

Segmento Final de una Derivación: El segmento final o parte final de una derivación P se define de la siguiente manera:

i) El secuente final de P pertenece al segmento final.

ii) El secuente superior de una inferencia que **no** sea una inferencia lógica implícita pertenece al segmento final de P syss el secuente inferior también pertenece.

iii) El secuente superior de una inferencia lógica implícita **no** pertenece al segmento final de P.

Esta definición se puede mostrar equivalente a la siguiente, que es la que usaremos con mas frecuencia: Un secuente S pertenece al segmento final de P syss **no** hay una inferencia lógica implícita bajo S. Por otra parte decimos que una inferencia lógica pertenece al segmento final de P syss su secuente inferior pertenece al segmento final de P. Con la notación segfin(P) denotamos al segmento final de la derivación P.

Frontera de una Derivación: decimos que una inferencia J pertenece a la frontera de la derivación P o que J es una **inferencia frontera** de P syss el secuente inferior de J pertenece a segfin(P) y el secuente superior no. Nótese que si J pertenece a la frontera de P entonces es una inferencia lógica implícita (¿ Por qué ?). Con ∂P denotamos a la frontera de P.

Corte Adecuado: Un corte que pertenece a segfin(P) es adecuado syss cada una de sus fórmulas de corte tiene un ancestro el cual es fórmula principal de una inferencia frontera.

Cortes Prescindibles e Imprescindibles: Un corte se dice prescindible syss su fórmula de corte no tiene símbolos lógicos, en otro caso el corte se llama imprescindible. Los cortes prescindibles son aquellos cuyas fórmulas de corte son atómicas.

Ejemplo:

$$
\dfrac{
  \dfrac{
    \dfrac{\vdots}{\Gamma' \to \Theta', A} \quad \dfrac{\vdots}{\Gamma' \to \Theta', B}
  }{\Gamma' \to \Theta', A \wedge B}\, I_1
  \;\; \vdots \;\;
  \Gamma \to \Theta, A \wedge B
  \qquad\qquad
  \dfrac{\dfrac{\vdots}{A, \Pi' \to \Lambda'}}{A \wedge B, \Pi' \to \Lambda'}\, I_2
  \;\; \vdots \;\;
  A \wedge B, \Pi \to \Lambda
}{\Gamma, \Pi \to \Theta, \Lambda}\, I
$$

$$\vdots$$

$$\Delta \to \Xi$$

en esta derivación, las inferencias I_1 e I_2 son inferencias frontera, el corte I es un corte adecuado e imprescindible y el segmento final de la derivación consta de todos los secuentes bajo I_1 e I_2.

1.6 Algunos Resultados acerca de Derivaciones

En esta sección desarrollaremos algunos resultados útiles para simplificar derivaciones que ya tenemos previamente dadas.

DEFINICIÓN. (Prueba Regular)

Una LK-Derivación se dice regular syss satisface las siguientes condiciones:

i) Todas sus variables propias o eigenvariables son distintas entre si.

ii) Si una variable x figura como variable propia en un secuente S de la derivación, entonces x figura solamente en secuentes arriba de S.

Un resultado importante que enunciamos en la siguiente proposición es que toda derivación puede transformarse de una forma sencilla en una derivación regular.

PROPOSICIÓN. Si P es una LK-Derivación con secuente final S, entonces existe una derivación regular Q de S. Mas aún, Q se obtiene de P simplemente reemplazando variables libres de una manera adecuada.

<u>**Dem**</u>: Puesto que el concepto de variable propia solo aparece en las inferencias del tipo *UNIV-D* y *EXIST-I*, y siendo *EXIST-I* una regla derivada a partir de *UNIV-D*, nuestra prueba

será por inducción sobre el número de aplicaciones de *UNIV-D*. Sea l tal número.

i) si $l = 0$, entonces en P no figuran inferencias del tipo *UNIV-D*, por lo que P ya es regular.

ii) $l > 0$, en tal caso P es S.P.G. de la siguiente forma:

$$\begin{array}{cc} & P_1 \quad P_2 \ldots\ldots P_k \\ (*)\{ & \ddots \vdots \ddots \\ & S \end{array}$$

donde para cada $1 \leq i \leq k$, P_i es una subprueba de la siguiente forma:

$$\begin{array}{ccc} & & \ddots \vdots \ddots \\ I_i & : & \dfrac{\Gamma_i \longrightarrow \Delta_i,\ F_i(b_i)}{\Gamma_i \longrightarrow \Delta_i,\ \forall y_i F_i(y_i)} \end{array}$$

y cada I_i es una inferencia *UNIV-D* minimal i.e. no hay dentro de P ninguna otra inferencia *UNIV-D* bajo I_i (es decir, en la parte de P denotada por $(*)$).

Claramente P_i tiene una aplicación menos de *UNIV-D* que P, por lo que por hipótesis de inducción existe una prueba regular del secuente $\Gamma_i \longrightarrow \Delta_i,\ F_i(b_i)$. Denotemos tal derivación con Q_i. Nótese que ninguna variable libre en $\Gamma_i \longrightarrow \Delta_i,\ F_i(b_i)$ aparece como variable propia en Q_i, pues en caso contrario sólo podría aparecer en secuentes arriba de aquél en el que aparece como variable propia (digamos S_1). No obstante, tal variable figura en el secuente final $\Gamma_i \longrightarrow \Delta_i$, $F_i(b_i)$ que obviamente esta abajo de S_1.

Sean $c_1, ..., c_m$ las variables propias que aparecen en todas las Q_i y que, dentro de P, figuran arriba de $\Gamma_i \longrightarrow \Delta_i,\ F_i(b_i)$ para toda $1 \leq i \leq k$.

Cambiemos en toda la derivación las variables $c_1, ..., c_m$ por $d_1, ..., d_m$ donde las d_i son las primeras variables que no figuran ni en P ni en ninguna Q_i. Pos su parte, si b_i figura en P bajo $\Gamma_i \longrightarrow \Delta_i, \forall y_i F_i(y_i)$, entonces la cambiamos por la variable d_{m+i} (puesto que estamos construyendo una prueba regular).

Ahora bien, si Q_i^r es la derivación obtenida de Q_i aplicando este reemplazo, es claro que para cualquier $1 \leq i \leq k$, Q_i^r es regular.

Así la prueba regular deseada es:

$$(*')\left\{\begin{array}{c} \underbrace{\dfrac{Q_1^r}{\Gamma_1 \to \Delta_1, \forall y_1 F_1(y_1)} \cdots\cdots\cdots \dfrac{Q_i^r}{\Gamma_i \to \Delta_i, \forall y_i F_i(y_i)} \cdots\cdots \dfrac{Q_k^r}{\Gamma_k \to \Delta_k, \forall y_k F_k(y_k)}} \\ \ddots \vdots \ddots \\ S \end{array}\right.$$

donde $(*')$ es igual que $(*)$ excepto por la sustitución de b_i por d_{m+i}.□

Supongamos ahora que ya tenemos dada una derivación del secuente $\Gamma(a) \to \Delta(a)$ donde la notación $\Gamma(a)$ indica que en las fórmulas de Γ hay presencias de la variable a. Sea b una variable que no figura en tal derivación. En tal caso podemos reemplazar todas las presencias de a por b, obteniendo como resultado una derivación del secuente $\Gamma(b) \to \Delta(b)$. Metafóricamente, si yo tenia un árbol de peras, en el que no había ninguna manzana, si en él cambio todas las peras por manzanas, obtendré un árbol de manzanas idéntico al de peras que ya tenia. Tal resultado lo enunciamos formalmente como sigue:

PROPOSICIÓN. Si $\Gamma(a) \to \Delta(a)$ es un secuente demostrable, $P(a)$ una derivación de $\Gamma(a) \to \Delta(a)$ y b es una variable que no figura en $P(a)$, entonces el árbol $P(b)$, que se obtiene reemplazando en $P(a)$ todas las presencias de a por b es una derivación del secuente $\Gamma(b) \to \Delta(b)$.

Dem: La prueba es por inducción sobre el numero k de inferencias en $P(a)$.

$[k = 0]$ En este caso no hay inferencias, así que la prueba $P(a)$ consta únicamente del secuente $\Gamma(a) \to \Delta(a)$ que es necesariamente un axioma y, sin importar el tipo de axioma, la prueba es trivial. Por ejemplo, si $\Gamma(a) \to \Delta(a)$ es de la forma $a = 3 \to sa = s3$, entonces $P(b)$ es $b = 3 \to sb = s3$ y es obvio que esto es un axioma.

Hipótesis de inducción: La proposición vale para cualquier derivación que tiene a lo mas n inferencias.

$[k = n+1]$ Digamos que $P(a)$ es de la siguiente forma:

$$Q(a)\left\{\begin{array}{c} \ddots\vdots\;\ddots \\ \underline{S_1(a)} \end{array}\right.$$
$$S(a)$$

donde $J : \frac{S_1(a)}{S(a)}$ es la última inferencia de la derivación.
Analizaremos varios casos segun el tipo de inferencia que sea J.

i) J es una inferencia débil.

En este caso la prueba es muy simple Como ejemplo haremos el caso en que J es una dilución, digamos $J : \frac{\Lambda(a)\rightarrow\Pi(a)}{D(a),\Lambda(a)\rightarrow\Pi(a)}$. En este caso $P(a)$ es:

$$\frac{Q(a)\left\{\begin{array}{c} \ddots\vdots\;\ddots \\ \Lambda(a) \rightarrow \Pi(a) \end{array}\right.}{D(a), \Lambda(a) \rightarrow \Pi(a)}$$

y como $Q(a)$ tiene n inferencias, entonces por hipótesis de inducción $Q(b)$ es una derivación del secuente $\Lambda(b) \rightarrow \Pi(b)$. Así que aplicando otra vez una dilución, obtenemos $D(b), \Lambda(b) \rightarrow \Pi(b)$, Esquemáticamente:

$$\frac{Q(b)\left\{\begin{array}{c} \ddots\vdots\;\ddots \\ \Lambda(b) \rightarrow \Pi(b) \end{array}\right.}{D(b), \Lambda(b) \rightarrow \Pi(b)}$$

los otros casos son análogos.
El caso en el que J es un corte, digamos $J : \frac{\Lambda(a)\rightarrow\Pi(a),D(a)\quad D(a),\Sigma(a)\rightarrow\Omega(a)}{\Lambda(a),\Sigma(a)\rightarrow\Pi(a),\Omega(a)}$, también es muy sencillo; sólo que ahora tenemos 2 subpruebas, (una por cada secuente superior del corte) así que $P(a)$ es:

$$\frac{Q_1(a)\left\{\begin{array}{cc} \ddots\vdots\;\ddots & \ddots\vdots\;\ddots \\ \Lambda(a) \rightarrow \Pi(a), D(a) & D(a), \Sigma(a) \rightarrow \Omega(a) \end{array}\right\} Q_2(a)}{\Lambda(a), \Sigma(a) \rightarrow \Pi(a), \Omega(a)}$$

y por hipótesis de inducción , $Q_1(b)$ y $Q_2(b)$ son derivaciones. De lo anterior concluimos, aplicando de nuevo un corte, que $P(b)$ es una derivación:

$$Q_1(b)\left\{\begin{array}{c}\ddots\vdots\cdot\cdot\\ \Lambda(b)\rightarrow\Pi(b),D(b)\end{array}\right.\quad\begin{array}{c}\ddots\vdots\cdot\cdot\\ D(b),\Sigma(b)\rightarrow\Omega(b)\end{array}\Big\}Q_2(b)$$
$$\overline{\Lambda(b),\Sigma(b)\rightarrow\Pi(b),\Omega(b)}$$

El caso en el que J es una inferencia lógica proposicional es también obvio. Por lo que procederemos al caso en el que J es una inferencia con cuantificadores.
Veamos el caso en el que J es una *UNIV-D* digamos $J:\frac{\Lambda(a)\rightarrow\Pi(a),A(a)}{\Lambda(a)\rightarrow\Pi(a),\forall xA(x)}$. En este caso $P(a)$ es:

$$Q(a)\left\{\begin{array}{c}\ddots\vdots\cdot\cdot\\ \Lambda(a)\rightarrow\Pi(a),A(a)\end{array}\right.$$
$$\overline{\Lambda(a)\rightarrow\Pi(a),\forall xA(x)}$$

Hay 2 subcasos:

i) La variable propia de J es precisamente a, en cuyo caso a no figura en Λ,Π ni en $A(x)$. Por hipótesis de inducción, reemplazar todas las presencias de a en $Q(a)$ por b nos produce una derivación $Q(b)$ cuyo secuente final es $\Lambda\rightarrow\Pi,A(b)$, donde ni en Λ ni en Π figura b, así que podemos aplicar de nuevo una *UNIV-D* con b como variable propia, con lo cual tenemos que $P(b)$ es una derivación de $\Lambda\rightarrow\Pi,\forall xA(x)$:

$$Q(b)\left\{\begin{array}{c}\ddots\vdots\cdot\cdot\\ \Lambda\rightarrow\Pi,A(b)\end{array}\right.$$
$$\overline{\Lambda\rightarrow\Pi,\forall xA(x)}$$

ii)a no es la variable propia de J. En este caso a podría figurar en Λ y en Π. Si c es la variable propia de J, en la fórmula A también puede figurar a, por lo que la denotamos $A(a,c)$.

$P(a)$ es:

$$\cfrac{Q(a)\left\{\begin{array}{c} \cdot\,\cdot\,\vdots\,\cdot\,\cdot \\ \Lambda(a) \rightarrow \Pi(a), A(a,c) \end{array}\right.}{\Lambda(a) \rightarrow \Pi(a), \forall x A(a,x)}$$

Ahora, por hipótesis de inducción, reemplazar todas las presencias de a por b en $Q(a)$ nos produce una derivación $Q(b)$ cuyo secuente final es $\Lambda(b) \longrightarrow \Pi(b), A(b,c)$. Puesto que b no figura en $P(a)$, por hipótesis tenemos que $b \neq c$ y por lo tanto podemos aplicar de nuevo una *UNIV-D* con c como variable propia, obteniendo la derivación $P(b)$ con secuente final $\Lambda(a) \longrightarrow \Pi(a), \forall x A(a,x)$. El caso en el que J es una *UNIV-I* es también muy simple y se deja como ejercicio al lector.□

El resultado que acabamos de demostrar tiene una extensión a todos los términos bastante útil. La enunciamos en la siguiente

PROPOSICIÓN. Sea t un término cualquiera y $\Gamma(a) \longrightarrow \Delta(a)$ un secuente derivable en LK. Sea $P(a)$ una derivación de $\Gamma(a) \longrightarrow \Delta(a)$ en la que toda variable propia es diferente de a y no figura en t. Al Reemplazar todas las presencias de a por t en $P(a)$ se obtiene una derivación $P(t)$ del secuente $\Gamma(t) \longrightarrow \Delta(t)$.

Dem: La demostración es por inducción sobre términos y se omite.□

COROLARIO. Si t es un término cualquiera y $S(a)$ un secuente demostrable en LK, entonces $S(t)$ también es demostrable.

A continuación probamos algunos resultados relacionados con la igualdad.

PROPOSICIÓN. Para cualesquiera términos s, t, el secuente $s = t \rightarrow t = s$ es derivable.

Dem: De los axiomas $\rightarrow s = s$ y $s = t, s = s \rightarrow t = s$ es inmediato que mediante un corte[5]:

$$\frac{\rightarrow s = s \quad s = t, s = s \rightarrow t = s}{s = t \rightarrow t = s}$$

[5]En este caso el segundo es un axioma de igualdad del tipo iv) donde la formula original $R(a)$ es $s = a$.

□

PROPOSICIÓN. Si $A(a_1, ..., a_n)$ es una fórmula cualquiera, entonces el secuente

$$s_1 = t_1, ..., s_n = t_n,\ A(s_1, ..., s_n) \rightarrow A(t_1, ..., t_n)$$

es derivable para cualesquiera términos $s_1, ..., s_n, t_1, ..., t_n$.

<u>**Dem**</u>: Inducción sobre fórmulas.

i) Si A es atómica, entonces el secuente es un axioma.

ii) Supongamos que A es de la forma $\neg B$, donde por hipótesis de inducción el secuente $t_1 = s_1, ..., t_n = s_n,\ B(t_1, ..., t_n) \rightarrow B(s_1, ..., s_n)$ es derivable. En tal caso tenemos la siguiente derivación:

$$\frac{t_1 = s_1, ..., t_n = s_n,\ B(t_1, ..., t_n) \rightarrow B(s_1, ..., s_n)}{t_1 = s_1, ..., t_n = s_n,\ B(t_1, ..., t_n), \neg B(s_1, ..., s_n) \rightarrow}\ (NEG\text{-}I)$$

$$\frac{t_1 = s_1, ..., t_n = s_n,\ B(t_1, ..., t_n), \neg B(s_1, ..., s_n) \rightarrow}{t_1 = s_1, ..., t_n = s_n,\ \neg B(s_1, ..., s_n) \rightarrow \neg B(t_1, ..., t_n)}\ (NEG\text{-}D)$$

por lo que el secuente $s_1 = t_1, ..., s_n = t_n,\ A(s_1, ..., s_n) \rightarrow A(t_1, ..., t_n)$ es derivable[6].

iii) Si A es de la forma $B \vee C$ donde por hipótesis de inducción los secuentes $s_1 = t_1, ..., s_n = t_n,\ B(s_1, ..., s_n) \rightarrow B(t_1, ..., t_n)$ y $s_1 = t_1, ..., s_n = t_n,\ C(s_1, ..., s_n) \rightarrow C(t_1, ..., t_n)$ son derivables, tenemos la siguiente derivación donde $\vec{s}$ y $\vec{t}$ representan respectivamente a las n-adas, $s_1, ..., s_n$ y $t_1, ..., t_n$:

$$\frac{s_i = t_i, B(\vec{s}) \rightarrow B(\vec{t})}{s_i = t_i, B(\vec{s}) \rightarrow B(\vec{t}), C(\vec{t})} \quad \frac{s_i = t_i, C(\vec{s}) \rightarrow C(\vec{t})}{s_i = t_i, C(\vec{s}) \rightarrow B(\vec{t}), C(\vec{t})}\,(DIL\text{-}D)$$

$$\frac{s_i = t_i, B(\vec{s}) \rightarrow B(\vec{t}), C(\vec{t}) \quad s_i = t_i, C(\vec{s}) \rightarrow B(\vec{t}), C(\vec{t})}{s_i = t_i, B(\vec{s}) \vee C(\vec{s}) \rightarrow B(\vec{t}), C(\vec{t})}\,(DISY\text{-}I)$$

$$\frac{s_i = t_i, B(\vec{s}) \vee C(\vec{s}) \rightarrow B(\vec{t}), C(\vec{t})}{s_i = t_i, B(\vec{s}) \vee C(\vec{s}) \rightarrow B(\vec{t}), B(\vec{t}) \vee C(\vec{t})}\,(DISY\text{-}D)$$

$$\frac{s_i = t_i, B(\vec{s}) \vee C(\vec{s}) \rightarrow B(\vec{t}), B(\vec{t}) \vee C(\vec{t})}{s_i = t_i, B(\vec{s}) \vee C(\vec{s}) \rightarrow B(\vec{t}) \vee C(\vec{t}), B(\vec{t}) \vee C(\vec{t})}\,(DISY\text{-}D)$$

[6] Aquí utilizamos la proposición anterior para deducir que de $t_i = s_i$ obtenemos $s_i = t_i$.

$$\frac{s_i = t_i, B(\bar{s}) \vee C(\bar{s}) \rightarrow B(\bar{t}) \vee C(\bar{t}), B(\bar{t}) \vee C(\bar{t})}{s_i = t_i, B(\bar{s}) \vee C(\bar{s}) \rightarrow B(\bar{t}) \vee C(\bar{t})} (CON\text{-}D)$$

de esta manera queda demostrado el secuente $s_1 = t_1, ..., s_n = t_n,\ A(s_1, ..., s_n) \rightarrow A(t_1, ..., t_n)$.

iv) Si A es de la forma $\forall x B(x, a_1, ..., a_n)$, donde por hipótesis de inducción el secuente $s_1 = t_1, ..., s_n = t_n,\ B(b, s_1, ..., s_n) \rightarrow B(b, t_1, ..., t_n)$ es derivable (no siendo b ninguna de las a_i ¿ Por qué?), tenemos la siguiente derivación[7]:

$$\frac{s_1 = t_1, ..., s_n = t_n,\ B(b, s_1, ..., s_n) \rightarrow B(b, t_1, ..., t_n)}{s_1 = t_1, ..., s_n = t_n,\ B(b, s_1, ..., s_n) \rightarrow \forall x B(x, t_1, ..., t_n)} (UNIV\text{-}D)$$

$$\frac{s_1 = t_1, ..., s_n = t_n,\ B(b, s_1, ..., s_n) \rightarrow \forall x B(x, t_1, ..., t_n)}{s_1 = t_1, ..., s_n = t_n,\ \forall x B(x, s_1, ..., s_n) \rightarrow \forall x B(x, t_1, ..., t_n)} (UNIV\text{-}I)$$

Con este último caso queda demostrada nuestra proposición para cualquier fórmula.□

1.7 Definición de Consistencia

El objetivo principal de este trabajo es exhibir una prueba de consistencia de un sistema muy particular: el de la aritmética o teoría de los números. Para ello debemos definir el concepto de consistencia.

El término consistencia, derivado del latín *consistens*, significa solidez. En nuestro caso tiene el siguiente sentido: el sistema está libre de contradicciones. De hecho, la palabra correspondiente en alemán es *widerspruchsfreiheit*, que es una composición de las palabras *freiheit*, libertad y *widerspruch*, contradicción, es decir libre de contradicciones. A continuación precisamos dicho concepto de consistencia.

DEFINICIÓN. Decimos que un sistema formal es consistente syss no hay una fórmula A tal que tanto A como su negación $\neg A$ son demostrables. Decimos que el sistema es inconsistente cuando no es consistente.

OBSERVACIÓN: Esta definición tiene sentido solamente en el caso en que el sistema cuente con un símbolo para la negación, como el nuestro. En los otros casos se dice que el sistema es

[7] Con b actuando como la variable propia.

consistente cuando hay una fórmula que no es demostrable en él, lo cual resulta equivalente. A continuación demostraremos un resultado que nos proporciona una segunda caracterización de esta noción, el cual utilizaremos en la prueba de consistencia.

PROPOSICIÓN. Un sistema formal es consistente syss en el no es demostrable el secuente vacío $\rightarrow$.

<u>Dem</u>:

$\Rightarrow$) (Contrapositiva) Si el secuente vacío $\rightarrow$ es demostrable, entonces por dillución para cualquier fórmula A tenemos que:

$$\frac{\rightarrow}{\rightarrow A} \quad \text{y} \quad \frac{\rightarrow}{\rightarrow \neg A}$$

y el sistema es inconsistente.□

$\Leftarrow$) (Contrapositiva) Si el sistema es inconsistente, entonces existe una fórmula A tal que los secuentes $\rightarrow A$ y $\rightarrow \neg A$ son demostrables. Por lo tanto, utilizando *NEG-I* y el hecho de que $A \equiv \neg\neg A$, tenemos que:

$$\frac{\rightarrow \neg A}{A \rightarrow}$$

y ahora utilizando esto y un corte tenemos:

$$\frac{\rightarrow A \quad A \rightarrow}{\rightarrow}$$

Por lo que el secuente vacío $\rightarrow$ es demostrable.□

En la última sección del capítulo enunciamos los trascendentales teoremas de Gödel.

1.8 Los Teoremas de Gödel

Como paso preliminar a la demostración de consistencia de la matemática clásica, Hilbert y sus seguidores pusieron a prueba su herramienta aplicando sus métodos a la lógica misma y a algunos fragmentos de la Aritmética. Lo primero fue formalizar la lógica de primer orden y demostrar su consistencia con métodos finitistas. Realizada esta tarea dirigieron su atención

a la teoría de los números. En este caso la formalización se realizó por etapas, considerando fragmentos sucesivos de la Aritmética de Peano. En cada situación una prueba de consistencia finitista fue elaborada para el fragmento. En 1930 había razones para esperar que en poco tiempo el programa se vería coronado con éxito.
Esta etapa, caracterizada por el trabajo constructivo de Hilbert en la Teoría de la Demostración, llegó a su fin en 1931 cuando las investigaciones tomaron un curso inesperado: Kurt Gödel, entonces un joven matemático vienés de 25 años, dio a conocer un trabajo que habría de dejar una huella indeleble en la lógica moderna. Utilizando tan solo métodos finitistas, Gödel demostró que la consistencia de la aritmética formal no se puede probar mediante herramientas que a su vez sean representables dentro del formalismo. Esto significa, entre otras cosas, que los recursos y métodos de razonamiento incorporados en un formalismo aritmético no muy restringido son insuficientes para probar su consistencia, es decir, que hay que recurrir necesariamente a una teoría más fuerte que esta para tal fin. Lo anterior constituyo un fuerte golpe a la pretensión de Hilbert de eliminar para siempre los problemas de fundamentación de las matemáticas: Ahora resultaba que la justificación de cualquier teoría con cierto poder expresivo habría de encontrarse en otra teoría que en cierto sentido la desbordaba, quedando pendiente el problema de la consistencia de esta última. Lo anterior no hacía mas que poner en entredicho la posibilidad de justificar la validez del análisis con una prueba finitista de consistencia. (Ver [To3]).
A continuación enunciaremos de la manera más elemental, los dos Teoremas de Incompletud de Gödel, también conocidos como teoremas limitativos.

Primer Teorema de Incompletud de Gödel

Si la Aritmética es Consistente entonces es Incompleta.[8]

Ahora bien, dado que demostraremos que la aritmética es consistente, por el primer teorema de incompletud de Gödel quedara demostrado que la aritmética es incompleta, es decir, que hay verdades aritméticas que jamás seremos capaces de demostrar en el sistema formal. Las consecuencias filosóficas de este resultado (así como su exposición y análisis) van más allá de los objetivos de este trabajo.

[8]Aquí por aritmética entendemos cualquier sistema formal que represente a nuestra aritmética informal, como el sistema AP que desarrollaremos en el capítulo 2.
Una teoría es incompleta si en ella existen enunciados indecidibles, es decir afirmaciones que no se pueden ni probar ni refutar dentro del sistema.

El segundo teorema de incompletud de Gödel tiene que ver con la cuestión de la consistencia y es el que realmente derrumba al Programa de Hilbert:

Segundo Teorema de Incompletud de Gödel

Si la Aritmética es Consistente, entonces es incapaz de probar su propia Consistencia.

Esto es: No es posible probar la consistencia de la aritmética (o de cualquier otra teoría que la contenga) mediante las técnicas propias de la misma teoría, a menos que la misma aritmética sea inconsistente.

Una exposición detallada de las demostraciones y consecuencias de estos teoremas se puede hallar en [To2] y en [Roj].

Después de la aparición de los teoremas limitativos, solo había dos alternativas: olvidarse del programa completamente, lo cual resultaba frustrante, o tratar de debilitar el programa, es decir, investigar hasta donde se tiene que llegar para conseguir una prueba de consistencia. Esto fue precisamente lo que hizo *Gentzen* en sus pruebas de consistencia.

En 1933 *Gentzen* consiguió obtener una prueba de consistencia de la aritmética clásica relativa a la aritmética intuicionista, resultado que junto con los Teoremas de Gödel, tuvo un enorme impacto. Al respecto, *Paul Bernays* comenta:

"Así que se ha vuelto aparente el hecho de que el punto de vista finitista no es la única alternativa a las formas de razonamiento y no es necesariamente implicado por la idea de la Teoría de la Demostración. Una extensión de los métodos de la teoría de la demostración estaba sugerida[9]: En lugar de una restricción a los métodos finitistas de razonamiento, se requería solamente que los argumentos fueran de un carácter constructivo, permitiéndose así tratar con formas más generales de inferencia."

Una extensión de tal tipo es la utilizada por *Gentzen* en sus pruebas de consistencia de la Aritmética de 1936 y 1938, ver [Gen1] y [Gen2].

[9] Aquí se entiende por Teoría de la Demostración, a la parte de la teoría de la demostración que unicamente utiliza metodos finitistas, como Hilbert la utilizo.

Capítulo 2

AP ES CONSISTENTE

La meta principal de este capítulo es dar una demostración de la Consistencia de la Aritmética de Peano. No obstante, antes de proceder a tal prueba necesitamos formalizar en un sistema lógico la Aritmética informal, cosa que haremos enseguida.

2.1 El Sistema Formal AP para la Aritmética

El sistema formal que usaremos es básicamente el sistema LK con ciertos agregados. En primer lugar, es necesario definir el lenguaje del sistema, un lenguaje de primer orden con igualdad denotado por $\mathfrak{L}_{AP}$ y que consta de los siguientes símbolos:

Constante: 0

Letras Funcionales: $+, \cdot, s$

donde los símbolos $+, \cdot$ denotaran a las operaciones binarias de suma y producto respectivamente y el símbolo s a la función sucesor unaria. Con estos símbolos utilizaremos notación infija. Obsérvese también que nuestro lenguaje carece de letras predicativa, aunque algunas otras formulaciones de la aritmética utilizan el símbolo binario $<$ para denotar el orden usual de los números naturales. El uso de este símbolo se puede evitar definiendo en términos de la igualdad y la suma de la siguiente manera:

$$x < y \underset{def.}{\Leftrightarrow} \exists\, z \neq 0 (y = x + z)$$

Aparte de los axiomas lógicos del sistema, distinguimos los siguientes secuentes llamados **Axiomas Matemáticos.**

DEFINICIÓN. Un secuente S es un axioma matemático syss tiene alguna de las siguientes formas, donde t, r denotan términos cualesquiera.

i) $s(r) = s(t) \rightarrow r = t$

ii) $s(t) = 0 \rightarrow$

iii) $\rightarrow t + 0 = t$

iv) $\rightarrow t + s(r) = s(t + r)$

v) $\rightarrow t \cdot 0 = 0$

vi) $\rightarrow t \cdot s(r) = t \cdot r + t$

Analicemos lo que dicen estos axiomas. El grupo i) dice que la función sucesor es inyectiva; el grupo ii) que el cero no pertenece a la imagen de la función sucesor; los grupos iii) y iv), y v) y vi) definen recursivamente las operaciones de suma y producto. Así, intuitivamente es muy clara la validez de dichos axiomas.

Además de las reglas de inferencia ya conocidas de LK, el sistema AP tiene la siguiente regla adicional, llamada Inducción:

$$\frac{F(a), \Gamma \rightarrow \Delta, F(sa)}{F(0), \Gamma \rightarrow \Delta, F(t)} \ (IND)$$

con las siguientes restricciones: la variable a no figura en $F(0), \Gamma$ o Δ; t es un término arbitrario (en el cual podría figurar a) y $F(a)$ es una fórmula arbitraria de $\mathfrak{L}_{AP}$. A $F(a)$ se le llama **la fórmula de inducción** y a es la variable propia de la inferencia; además, $F(a)$ y $F(sa)$ se llaman las fórmulas auxiliares izquierda y derecha respectivamente, y $F(0)$ y $F(t)$ las fórmulas principales izquierda y derecha respectivamente. Definimos el sucesor de $F(a)$, $(F(sa))$ como $F(0)$, $(F(t))$.

Este sistema formal suele denotarse PA (*Peano Arithmetik*), nosotros lo denotaremos con sus siglas en español AP (Aritmética de Peano).

En lo que sigue demostraremos algunos resultados que usaremos más adelante. Empezamos con el siguiente

LEMA 1. Para todo término cerrado s, existe un único número natural n tal que la fórmula

$s = \overline{n}$ es demostrable sin cortes imprescindibles y sin inducción, donde $\bar{n}$ denota al término $s^n(0)$ y es llamado el numeral de n.

<u>Dem</u>: Inducción sobre el término cerrado s

Caso i) Si $s = 0$, el resultado es inmediato pues el secuente $\rightarrow 0 = 0$ es un axioma[1].

Caso ii) Si $s = st$, donde t es un término cerrado y por hipótesis de inducción existe n tal que la fórmula $t = \overline{n}$ es demostrable, entonces utilizando un corte y el axioma de igualdad $t = \overline{n} \rightarrow st = s\overline{n}$, obtenemos:

$$\frac{\rightarrow t = \overline{n} \quad t = \overline{n} \rightarrow st = s\overline{n}}{\rightarrow st = s\overline{n}}$$

esto es, la fórmula $s = \overline{n+1}$ es demostrable.

Caso iii) Si $s = t_1 + t_2$ y por hipótesis de inducción existen n_1 y n_2 tales que los secuentes $\rightarrow t_1 = \bar{n}_1$ y $\rightarrow t_2 = \bar{n}_2$ son demostrables; entonces tenemos la siguiente derivación:

$$\frac{\rightarrow t_1 = \bar{n}_1 \qquad t_1 = \bar{n}_1, t_2 = \bar{n}_2 \rightarrow t_1 + t_2 = \overline{n}_1 + \overline{n}_2}{t_2 = \bar{n}_2 \rightarrow t_1 + t_2 = \overline{n}_1 + \overline{n}_2}$$

$$\frac{\rightarrow t_2 = \overline{n}_2 \quad t_2 = \overline{n}_2 \rightarrow t_1 + t_2 = \overline{n}_1 + \overline{n}_2}{\rightarrow t_1 + t_2 = \overline{n}_1 + \overline{n}_2}$$

Además, es claro que $\overline{n}_1 + \overline{n}_2 = \overline{n_1 + n_2}$. Por lo tanto, la fórmula $s = \overline{n_1 + n_2}$ queda demostrada.

Caso iv) Cuando $s = t_1 \cdot t_2$, se procede analogamente al caso iii), por lo que lo omitimos.

LEMA 2. Si s y t son términos cerrados, entonces alguno de los secuentes $\rightarrow s = t$ o $s = t \rightarrow$ es derivable sin un corte imprescindible ni inducción.

<u>Dem</u>: Utilizando el lema 1, es suficiente con demostrar lo siguiente: Para cualesquiera números naturales n y m, alguno de los secuentes $\rightarrow \overline{n} = \overline{m}$ o $\overline{n} = \overline{m} \rightarrow$ es derivable. Tenemos dos casos:

i) $n = m$. En este caso el secuente $\rightarrow \overline{n} = \overline{m}$ es un axioma.

ii) $n \neq m$. Podemos suponer, sin perder generalidad, que $n < m$, i.e., que hay un natural k

[1] Aqui 0 denota al simbolo para la constante que representa al número cero, no al número en si.

tal que $n + k = m$. Tenemos la siguiente derivación:

$$\dfrac{s^{k+1}(0) = s(0) \rightarrow s^k(0) = 0 \qquad\qquad s^k(0) = 0 \rightarrow}{s^{k+1}(0) = s(0) \rightarrow}$$

$$\dfrac{s^{k+2}(0) = s^2(0) \rightarrow s^{k+1}(0) = s(0) \qquad s^{k+1}(0) = s(0) \rightarrow}{s^{k+2}(0) = s^2(0) \rightarrow}$$

$$\dfrac{s^{k+3}(0) = s^3(0) \rightarrow s^{k+2}(0) = s^2(0) \qquad s^{k+2}(0) = s^2(0) \rightarrow}{s^{k+3}(0) = s^3(0) \rightarrow}$$

$$\dfrac{\ddots \vdots \ddots}{s^{k+n}(0) = s^n(0) \rightarrow}$$

pero $k + n = m$, así que en este caso queda demostrado el secuente $\overline{m} = \overline{n} \rightarrow$.□

LEMA 3. Si s y t términos cerrados tales que la fórmula $s = t$ es derivable sin un corte imprescindible ni inducción, y si $q(a)$ y $r(a)$ son dos términos con algunas presencias de a (posiblemente ninguna), entonces el secuente $q(s) = r(s) \rightarrow q(t) = r(t)$ es derivable sin cortes imprescindibles ni inducción.

Dem: En este caso toda la derivación se reduce al siguiente corte prescindible:

$$\dfrac{\rightarrow s = t \quad s = t, q(s) = r(s) \rightarrow q(t) = r(t)}{q(s) = r(s) \rightarrow q(t) = r(t)}$$

puesto que por una proposición anterior (capitulo 1) el secuente $s = t, q(s) = r(s) \rightarrow q(t) = r(t)$ es derivable.□

LEMA 4. Si s y t son como en el lema 3 y si $F(a)$ es una fórmula cualquiera, entonces el secuente $F(s) \rightarrow F(t)$ es derivable sin un corte imprescindible ni inducción.

Dem: Análoga a la del lema 3:

$$\dfrac{\rightarrow s = t \quad s = t, F(s) \rightarrow F(t)}{F(s) \rightarrow F(t)}$$

por lo que el secuente $F(s) \rightarrow F(t)$ es derivable sin cortes imprescindibles ni inducción.□

2.2 Accesibilidad

El concepto de accesibilidad de un ordinal es una manera de justificar el carácter casi finitista de la prueba de consistencia de *Gentzen*, que suele demostrarse con base en la inducción transfinita hasta ε_0. Mientras que para quienes aceptan el razonamiento transfinito no es necesaria alguna otra justificación, para los finitistas ésta es una justificación basada en un concepto completamente constructivo como lo es el de accesibilidad, el cual en su desarrollo no utiliza nada mas que la simple inducción para naturales.

DEFINICIÓN. Sea $(\alpha_n)\searrow$ una sucesión estrictamente decreciente de ordinales (i.e. $\alpha_n \in ORD$ p.t. $n \in \mathbb{N}$ y $n < m \Rightarrow \alpha_n > \alpha_m$) y $\mu \in ORD$. En tal caso decimos que (α_n) es μ-dominada syss $\mu > \alpha_0$ y, por lo tanto, $\mu > \alpha_n$ p.t. $n \in \mathbb{N}$.

DEFINICIÓN. Sea $\beta \in ORD$. Decimos que β es accesible syss cualquier sucesión $(\alpha_n)\searrow$ β-dominada es finita.

PROPOSICIÓN. Para toda $m < \omega$, m es accesible.

<u>**Dem**</u>: Si $(\alpha_n)\searrow$ es una sucesión m-dominada, entonces $m > \alpha_0 \Rightarrow \alpha_0 \in \{0, 1, ..., m-1\}$ y como nuestra sucesión es estrictamente decreciente, es obvio que tiene a lo mas $m-1$ elementos distintos. Por lo tanto, es finita.$\square$

COROLARIO. ω es accesible

<u>**Dem**</u>: Trivial.$\square$

Debe quedar muy claro que el concepto de accesibilidad de un ordinal tiene significado solamente cuando se ha demostrado mediante un método constructivo que dicho ordinal cumple la propiedad de accesibilidad. El método que aquí presentamos nos parece más claro y no tan complicado en su exposición, (en comparación con el método de los eliminadores) aunque tiene la desventaja de no ser completamente constructivo, pues utiliza la inducción para naturales. El lector interesado en dicho método debe consultar [Tak].

PROPOSICIÓN. Si μ y ν son accesibles, entonces $\mu + \nu$ es accesible.

Dem: Sea $(\alpha_n)\searrow$ una sucesión $(\mu+\nu)$-dominada. La demostración se divide en dos partes:
i) Existe un $n \in \mathbb{N}$ tal que $\alpha_n \leq \mu$
Supongamos que no. En tal caso tenemos que para cualquier $n \in \mathbb{N}$, $\alpha_n > \mu$. Como $\mu < \alpha_n < \mu + \nu$ entonces, por $OR11$, existe $\beta_n < \mu + \nu$ tal que $\alpha_n = \mu + \beta_n$ y como $\alpha_n = \mu + \beta_n < \mu + \nu$ entonces, por $OR4$, $\beta_n < \nu$. Consideremos ahora la sucesión (β_n) la cual es ν-dominada Si $n < m$, $\mu + \beta_n = \alpha_n > \alpha_m = \mu + \beta_m \underset{OR4}{\Rightarrow} \beta_n > \beta_m$ y $(\beta_n)\searrow$. De esta forma hemos construido una sucesión estrictamente decreciente, ν-dominada e infinita, lo cual contradice el hecho de que ν es accesible. Por lo tanto, existe $n \in \mathbb{N}$ tal que $\alpha_n \leq \mu$.□
ii) (α_n) es finita.
Si n_0 es tal que $\mu \geq \alpha_{n_0}$, entonces la sucesión $(\alpha_m)_{m=n_0}^{\infty}$ es μ-dominada y, además, es finita, pues μ es accesible. Por lo tanto, la sucesión completa (α_n) es finita.□

COROLARIO. Para cualesquiera $\alpha \in ORD$ y $n \in \mathbb{N}$, si α es accesible, entonces $\alpha \cdot n$ es accesible.

Dem: Es inmediata pues $\alpha \cdot n = \alpha + \alpha + ... + \alpha$ (n veces).□

PROPOSICIÓN. Sea $\alpha \in ORD$. Si α es accesible entonces $\alpha \cdot \omega$ es accesible.

Dem: Sea $(\beta_n)\searrow$ una sucesión $\alpha \cdot \omega$-dominada. Como $\beta_0 < \alpha \cdot \omega$ entonces, por $OR12$, $\beta_0 < \alpha \cdot n$ para algún $n \in \mathbb{N}$, y, por lo tanto, (β_n) es $\alpha \cdot n$-dominada, así que por el corolario anterior (β_n) es finita.□

DEFINICIÓN. (Recursiva de n-accesibilidad)
Sea $\alpha \in ORD$, decimos que α es 1-accesible syss α es accesible. Decimos que α es $(n+1)$-accesible syss para cualquier $\beta \in ORD$, si β es n-accesible entonces $\beta \cdot \omega^\alpha$ es n-accesible.

PROPOSICIÓN. Sean $\mu, \nu \in ORD$ y $n \in \mathbb{N}$. Si μ es n-accesible y $\nu < \mu$, entonces ν es n-accesible.

Dem: Inducción sobre n.

$n = 1$) Supongamos que μ es accesible. Si $(\alpha_n)\searrow$ es una sucesión ν-dominada, como $\nu < \mu$ y $\alpha_0 < \nu$, concluimos que $(\alpha_n)\searrow$ es μ-dominada. Por lo tanto, $(\alpha_n)\searrow$ es finita ya que μ es accesible.

Hipótesis de Inducción: Si μ es n-accesible y $\nu < \mu$ entonces ν es n-accesible.

Ahora supongamos que μ es $(n+1)$-accesible y $\nu < \mu$. Sea $\alpha \in ORD$, tal que α es n-accesible. Queremos demostrar que $\alpha \cdot \omega^\nu$ es n-accesible. Como $\nu < \mu$ entonces, por $OR2$, $\omega^\nu < \omega^\mu$ y, por $OR5, \alpha \cdot \omega^\nu < \alpha \cdot \omega^\mu$. Puesto que μ es $(n+1)$-accesible y α es n-accesible. Concluimos que $\alpha \cdot \omega^\mu$ es n-accesible. Por lo tanto como $\alpha \cdot \omega^\nu < \alpha \cdot \omega^\mu$ aplicando la hipótesis de inducción tenemos que $\alpha \cdot \omega^\nu$ es n-accesible.$\square$

PROPOSICIÓN. Sea $(\mu_m)\nearrow \mu$ una sucesión arbitraria estrictamente creciente con limite μ y sea $n \in \mathbb{N}$. Si para toda m, μ_m es n-accesible entonces μ es n-accesible; en otras palabras, el limite de sucesiones de n-accesibles es n-accesible.

__Dem__: Inducción sobre n.

$n = 1$) Sea $(\alpha_n)\searrow$ una sucesión μ-dominada. Como $\mu > \alpha_0$, entonces $\mu_m > \alpha_0$ para algún m y, por lo tanto, la sucesión (α_n) es μ_m-dominada y en consecuencia es finita.

Hip. de Ind.: Para cualquier sucesión $(\mu_m)\nearrow \mu$,si para toda m, μ_m es n-accesible entonces μ es n-accesible.

Supongamos que para toda m, μ_m es $(n+1)$-accesible. Queremos demostrar que μ es $(n+1)$-accesible. Tomemos un ordinal α n-accesible y demostremos que $\alpha \cdot \omega^\mu$ es n-accesible. Tenemos las siguientes relaciones entre sucesiones: Si $(\mu_m)\nearrow \mu$ entonces, por $OR2$, $(\omega^{\mu_m})\nearrow \omega^\mu$ de donde se sigue, por $OR5$, que $(\alpha \cdot \omega^{\mu_m})\nearrow \alpha \cdot \omega^\mu$, de modo que basta ver que para toda m, $\alpha \cdot \omega^{\mu_m}$ es n-accesible pues, utilizando la hipótesis de inducción, obtenemos que $\alpha \cdot \omega^\mu$ es n-accesible. Sin embargo, $\alpha \cdot \omega^{\mu_m}$ es n-accesible, pues por hipótesis μ_m es n-accesible. Concluimos que μ es $(n+1)$-accesible.$\square$

PROPOSICIÓN. Sea $\nu \in ORD$. Si ν es $(n+1)$-accesible, $\nu \cdot \omega$ también lo es.

__Dem__: Supongamos que ν es $(n+1)$-accesible. Queremos ver que $\nu \cdot \omega$ es $(n+1)$-accesible, tomemos α n-accesible y demostremos que $\alpha \cdot \omega^{\nu \cdot \omega}$ es n-accesible. Por la proposición anterior, basta ver que $\alpha \cdot \omega^{\nu \cdot m}$ es n-accesible para cada m, pues $(\alpha \cdot \omega^{\nu \cdot m})\nearrow \alpha \cdot \omega^{\nu \cdot \omega}$; pero tenemos que

$\alpha \cdot \omega^{\nu \cdot m} = \alpha \cdot (\omega^{\nu})^m = \alpha \cdot \underbrace{\omega^{\nu} \cdot \omega^{\nu} \cdot \ldots \cdot \omega^{\nu}}_{m \text{ veces}}$ así que, por la $(n+1)$-accesibilidad de ν, tenemos que si $\alpha \cdot \omega^{\nu}$ n-accesible entonces, como ν es $(n+1)$-accesible, $(\alpha \cdot \omega^{\nu}) \cdot \omega^{\nu}$ es n-accesible y, de nuevo, como ν es $(n+1)$-accesible, $(\alpha \cdot \omega^{\nu} \cdot \omega^{\nu}) \cdot \omega^{\nu}$ es n-accesible y, así sucesivamente, hasta llegar a la conclusión de que $\alpha \cdot \omega^{\nu \cdot m}$ es n-accesible (este procedimiento se puede justificar mediante inducción sobre m). Por lo tanto, concluimos que $\alpha \cdot \omega^{\nu \cdot \omega}$ es n-accesible y por ende $\nu \cdot \omega$ es $(n+1)$-accesible.□

PROPOSICIÓN. Para cualquier $n \in \mathbb{N}$, 1 es $(n+1)$-accesible.

__Dem__: El caso para $n = 0$ es trivial. Supongamos que $n \geq 1$. Queremos demostrar que si α es n-accesible, entonces $\alpha \cdot \omega^1 = \alpha \cdot \omega$ es n-accesible. Como $n \geq 1$ entonces $n = m + 1$ para algún $m \in \mathbb{N}$. Por lo tanto, debemos demostrar que si α es $(m+1)$-accesible entonces $\alpha \cdot \omega$ es $(m+1)$-accesible. Mas este es el resultado de la proposición anterior.□

PROPOSICIÓN. Para cualquier k y para toda $n > k$, ω_k es $(n-k)$-accesible.

__Dem__: Inducción sobre k,

$k = 0$) P.D. Para toda $n > 0$, $\omega_0 = 1$ es n accesible. Esto equivale a demostrar que 1 es $(m+1)$-accesible para toda $m \geq 0$, que es la proposición anterior.

Hipótesis de inducción: ω_k es $(n-k)$-accesible para toda $n > k$.

P.D. Para toda $n > k+1$, ω_{k+1} es $(n-(k+1))$-accesible.

Sea $n > k+1$,como $n > k$ y $n - k = (n-(k+1)) + 1$, tenemos que, por hipótesis de inducción, ω_k es $((n-(k+1)) + 1)$-accesible. Por lo tanto, como 1 es $(n-(k+1))$-accesible, entonces, puesto que ω_k es $((n-(k+1)) + 1)$-accesible, $1 \cdot \omega^{\omega_k} = \omega^{\omega_k} = \omega_{k+1}$ es $(n-(k+1))$-accesible.□

COROLARIO. ω_k es accesible para cualquier $k \in \mathbb{N}$.

__Dem__: Trivial.

Tomemos ahora cualquier sucesión $(\alpha_n)\searrow$ que sea ε_0-dominada. Como $\alpha_0 < \varepsilon_0$ implica $\alpha_0 < \omega_k$ para algún $k \in \mathbb{N}$, tenemos que (α_n) es ω_k-dominada, y, por el corolario anterior, (α_n) es finita. De esta manera hemos demostrado la siguiente

PROPOSICIÓN. ε_0 es accesible

Este último resultado es crucial, ya que la inconsistencia de la aritmética implicaría que ε_0 no es accesible. De lo anterior se sigue que AP no puede ser inconsistente, si bien nos falta mucho camino por andar para llegar a tal resultado.

2.3 La Relación entre Ordinales y Derivaciones

Nuestra herramienta principal para la prueba de consistencia es el concepto de accesibilidad, para cuya comprensión necesitamos dar una relación entre los números ordinales[2] y las derivaciones, lo cual explicamos en esta sección.

Antes de dar la asignación de ordinales necesitamos un par de definiciones.

DEFINICIÓN. Sea A una fórmula. El *grado* de A es el número de símbolos lógicos que figuran en ella y es denotado $grd(A)$. El grado de un corte es el grado de la fórmula de corte y el grado de una inducción es el grado de la fórmula de inducción. Abusando de la notación, si J es un corte o inducción, denotamos a su grado con $grd(J)$.

DEFINICIÓN. Sea S un secuente. La *altura* de S en la derivación P es el máximo de los grados de los cortes e inducciones que figuran en P bajo S. Tal numero se denota con $h_P(S)$; esto es

$$h_P(S) = \max\{\ grd(J) \mid J \text{ es un corte o } IND, \text{ que figura en } P \text{ bajo } S\ \}$$

A continuación enunciamos algunos resultados útiles acerca de la altura.

PROPOSICIÓN.

a) La altura del secuente final de una derivación es cero.

b) Si S_1 figura arriba de S_2 en una derivación, entonces $h_P(S_2) \leq h_P(S_1)$.

c) Si S_1 y S_2 son los secuentes superiores de una inferencia, entonces $h_P(S_1) = h_P(S_2)$.

<u>Dem</u>: Trivial.□

DEFINICIÓN. (Por recursión para naturales).

Dado cualquier ordinal α, definimos:

$$\omega_0(\alpha) = \alpha, \quad \omega_{n+1}(\alpha) = \omega^{\omega_n(\alpha)}$$

[2] Recordemos que por ordinales entendemos solamente ordinales menores que ε_0.

Lo que sigue es asignar a cada secuente de una derivación un número ordinal.

DEFINICIÓN. Sea $SEC(P) = \{S \mid S$ es un secuente de AP, que figura en P $\}$ Definimos recursivamente la función de asignación de ordinales $o_P : SEC(P) \to ORD$ de la siguiente manera:

i) Si S es un axioma, entonces $o_P(S) = 1$.

ii) Si $J : \frac{S_1}{S}$ es una inferencia débil, entonces $o_P(S) = o_P(S_1)$.

iii) Si $J : \frac{S_1}{S}$ es una inferencia del tipo *CONJ-I, DISY-D, IMP-D, NEG-D, NEG-I* o una inferencia con cuantificadores, entonces $o_P(S) = o_P(S_1) + 1$.

iv) Si $J : \frac{S_1 \quad S_2}{S}$ es una inferencia del tipo *CONJ-D* , *DISY-I o IMP-I*, entonces $o_P(S) = o_P(S_1) \oplus o_P(S_2)$.

v) Si $J : \frac{S_1 \quad S_2}{S}$ es un corte, entonces $o_P(S) = \omega_{k-l}(o_P(S_1) \oplus o_P(S_2))$ donde $k = h_P(S_1)$ y $l = h_P(S)$.

vi) Si $J : \frac{S_1}{S}$ es una *IND*, entonces $o_P(S) = \omega_{k-l+1}(\mu_1 \oplus 1)$ donde $o_P(S_1) = \omega^{\mu_1} + ... + \omega^{\mu_n}$ está en FNC, $k = h_P(S_1)$ y $l = h_P(S)$.

El ordinal de una derivación P, denotado con $o(P)$, por abuso de notación, es el ordinal de su secuente final. Con la notación:

$$P : \begin{array}{c} \ddots \vdots \ddots \\ \Gamma \xrightarrow{\mu} \Delta \end{array}$$

denotamos una derivación P de $\Gamma \to \Delta$ tal que $o(P) = o_P(\Gamma \to \Delta) = \mu$

OBSERVACIÓN: Cuando en el contexto de una discusión sólo nos estemos refiriendo a una derivación en particular escribiremos $o(S)$ en lugar de $o_P(S)$.

2.4 Derivaciones Simples

Aunque este trabajo cae en su totalidad en la rama de la lógica llamada Teoría de la Demostración, la cual es un tratamiento formal de la sintaxis de un lenguaje, para la prueba de consistencia necesitamos el concepto de derivación simple, que se sirve del concepto semántico de verdad y que trataremos de manera intuitiva.

DEFINICIÓN. Una AP-Derivación P se dice simple syss cumple las siguientes dos condiciones:

i) En P no hay presencias libres de variables.

ii) En P figuran solamente axiomas matemáticos, inferencias débiles y cortes prescindibles.

El resultado que utilizaremos es el siguiente: No hay una derivación simple del secuente vacío. no obstante, antes de proceder a la demostración, necesitamos hablar de cierta noción de verdad, la cual no es ni pretende ser una noción formal como la de *Tarski* de 1936. Mas bien, se trata de una noción intuitiva que se referirá **única y exclusivamente** a los secuentes que figuren en una derivación simple, sobre los cuales no tiene sentido preguntarse acerca de su valor de verdad sin especificar una derivación simple en la que éstos figuren.

Consideremos una fórmula de la forma $s = t$ con s y t términos cerrados cualesquiera, utilizando la interpretación natural de la constante 0 como el numero natural cero, podemos decidir inmediatamente si la fórmula es verdadera o falsa (sera verdadera si cuando al interpretarla en los números naturales, s denota al mismo número que t y falsa en el caso contrario). Por ejemplo, la fórmula $s0 = ss0$ se interpreta como $1 = 2$ y por lo tanto es falsa. En cambio, la fórmula $sss0 = s0 + ss0$ se interpreta como $3 = 1 + 2$ y, obviamente, es verdadera. Hechas estas observaciones pasamos a definir lo que entendemos como un secuente verdadero.

DEFINICIÓN. Sea $S = A_1, ..., A_n \rightarrow B_1, ..., B_m$ un secuente considerado dentro de una derivación simple Decimos que S es verdadero syss A_i es falsa para alguna $1 \leq i \leq n$ o B_j es verdadera para alguna $1 \leq j \leq m$.

La definición anterior es equivalente a decir que S es verdadero syss siempre que $A_1, ..., A_n$ son todas verdaderas, al menos una de $B_1, ..., B_m$ es verdadera. Nótese la semejanza con la definición de verdad de la implicación.

Dos consecuencias inmediatas de la definición son que el secuente vacío $\rightarrow$ es falso y que el secuente S sera falso syss $A_1, ..., A_n$ son todas verdaderas y $B_1, ..., B_m$ son todas falsas; para demostrar nuestro resultado necesitamos antes de dos lemas.

LEMA 1. Los Axiomas Matemáticos cerrados son verdaderos

<u>Dem</u>: Se deja al lector.□

LEMA 2. Las inferencias débiles y los cortes prescindibles preservan el valor verdadero hacia abajo para los secuentes, i.e., si $J : \frac{S_1}{S}$ es una inferencia débil ó $J : \frac{S_2, S_3}{S'}$ es un corte prescindible tales que S_1, S_2 y S_3 son secuentes verdaderos, entonces S y S' son verdaderos.

Dem: El caso en el que J es una inferencia débil es trivial. Veamos el caso en el que J es un corte prescindible, digamos

$$J : \frac{\Gamma \rightarrow \Delta, s = t \quad s = t, \Pi \rightarrow \Lambda}{\Gamma, \Pi \rightarrow \Delta, \Lambda}$$

y supongamos que $\Gamma \rightarrow \Delta, s = t$ y $s = t, \Pi \rightarrow \Lambda$ son ambos verdaderos. Queremos demostrar que $\Gamma, \Pi \rightarrow \Delta, \Lambda$ es verdadero. Si en Γ o en Π hay una fórmula falsa nada queda por demostrar, pues entonces habrá una fórmula falsa en Γ, Π. En cambio, si este no es el caso, entonces tenemos que todas las fórmulas de Γ y Π son verdaderas, de donde se sigue que hay al menos una fórmula verdadera en $\Delta, s = t$ y tenemos dos casos que considerar:

i) $s = t$ es verdadera. Se sigue que $s = t, \Pi$ son todas verdaderas, lo cual implica que en Λ (y por lo tanto en Δ, Λ) hay una fórmula verdadera, así que $\Gamma, \Pi \rightarrow \Delta, \Lambda$ es verdadero.

ii) $s = t$ es falsa. Esto implica que en Δ hay una fórmula verdadera, y, por lo tanto, $\Gamma, \Pi \rightarrow \Delta, \Lambda$ es verdadero.

En cualquier caso concluimos que $\Gamma, \Pi \rightarrow \Delta, \Lambda$ es verdadero.□

Ahora pasamos a demostrar el resultado que necesitamos.

PROPOSICIÓN. No hay una derivación simple del secuente vacío $\rightarrow$

Dem: (Por Reducción al Absurdo)

Supongamos que P es una derivación simple del secuente vacío $\rightarrow$. Por definición P empieza con axiomas matemáticos cerrados, los cuales son verdaderos por el lema 1, y, por el lema 2, todo secuente que figure en P debe ser verdadero. Pero $\rightarrow$ es falso lo cual es una contradicción.□

A este resultado le llamaremos la propiedad de derivaciones simples y la denotaremos por *PDS*.

2.5 La Propiedad de Monotonía

En esta sección se expone la propiedad central necesaria para la prueba de consistencia, a la que llamaremos la Propiedad de Monotonía para Derivaciones, denotada con *PMD*. Esta propiedad establece que si en una derivación se sustituye una subprueba de algún secuente por otra con menor ordinal, entonces la derivación completa tendrá menor ordinal. Obviamente se necesitan ciertas restricciones, que a continuación enunciamos.

PROPOSICIÓN. (PMD) Sea P una derivación en la que figura el secuente S_1 y sea P_1 la subprueba de P que termina en S_1 (i.e. el secuente final de P_1 es S_1). Supongamos que no hay aplicaciones de inducción (IND) bajo S_1. Sean P_1^r cualquier otra derivación de S_1 y P^r la prueba que resulta de substituir en P la subprueba P_1 por P_1^r, esto es:

$$P \;:\; P_1 \begin{cases} \ddots \vdots \therefore \\ S_1 \end{cases} \qquad P^r : P_1^r \begin{cases} \ddots \vdots \therefore \\ S_1 \end{cases}$$

$$\begin{array}{ccc} \ddots \vdots \therefore & \qquad & \ddots \vdots \therefore \\ \Gamma \rightarrow \Delta & & \Gamma \rightarrow \Delta \end{array}$$

se afirma que si $o_{P^r}(S_1) < o_P(S_1)$, entonces $o(P^r) < o(P)$.

<u>**Dem**</u>: Tómese una rama cualquiera de P que pase por S_1. Veremos que para cualquier secuente S que figure en la rama, sea éste S_1 u otro abajo de él, si S^res el secuente correspondiente a S en P^r (Nótese que considerados por si solos, S es igual a S^r, pero no segun la derivación en la que figuran) se tiene que $o_{P^r}(S^r) < o_P(S)$.
Si $S = S_1$, esto es cierto por hipótesis. Analicemos ahora los distintos casos según el tipo de inferencia en la que S sea el secuente inferior, suponiendo la desigualdad para los secuentes superiores:

i) Si S se obtuvo mediante una inferencia débil, digamos $J : \frac{S_2}{S}$ con $o_{P^r}(S_2^r) < o_P(S_2)$, entonces, conforme a la asignación de ordinales, tenemos que

$$o_{P^r}(S^r) = o_{P^r}(S_2^r) < o_P(S_2) = o_P(S)$$

ii) Si S es el secuente inferior de una inferencia del tipo *CONJ-I, DISY-D, IMP-D, NEG-D, NEG-I* o alguna inferencia con cuantificadores, digamos $J : \frac{S_2}{S}$, entonces como $o_{P^r}(S_2^r) <$

$o_P(S_2)$ tenemos (por propiedad de ordinales) que:

$$o_{P^r}(S^r) = o_{P^r}(S_2^r) + 1 < o_P(S_2) + 1 = o_P(S)$$

iii) Si S es el secuente inferior de una inferencia del tipo *CONJ-D, DISY-I o IMP-I*, digamos $J : \frac{S_2\ S_3}{S}$ y $o_{P^r}(S_2^r) < o_P(S_2)$, $o_{P^r}(S_3^r) < o_P(S_3)$, entonces (por la propiedad de ordinales (*OR15*))concluimos:

$$o_{P^r}(S^r) = o_{P^r}(S_2^r) \oplus o_{P^r}(S_3^r) < o_P(S_2) \oplus o_P(S_3) = o_P(S)$$

iv) Si S es el secuente inferior de un corte, digamos $J : \frac{S_2\ S_3}{S}$, y $o_{P^r}(S_2^r) < o_P(S_2), o_{P^r}(S_3^r) < o_P(S_3)$ entonces (usando la propiedad de ordinales *OR2* repetidamente, *OR15* y el hecho de que $h_{P^r}(S_2^r) = h_P(S_2)$) concluimos que

$$o_{P^r}(S^r) = \omega_{h_{P^r}(S_2^r)-h_P(S)}(o_{P^r}(S_2^r) \oplus o_{P^r}(S_3^r)) < \omega_{h_P(S_2)-h_P(S)}(o_P(S_2) \oplus o_P(S_3)) = o_P(S)$$

Con esto hemos demostrado que todas las reglas de inferencia preservan la desigualdad, así que tomando a S como el secuente final, obtenemos el resultado deseado $o(P^r) < o(P)$.□

2.6 El Lema Fundamental

En esta sección se expone un resultado llamado Lema Fundamental y constituye la parte medular de todo el trabajo. La prueba de consistencia vendrá a ser un corolario de este resultado que demostraremos detalladamente.

Pero antes de pasar al lema fundamental, demostraremos un par de resultados auxiliares.

PROPOSICIÓN. Si P es una derivación de $\rightarrow$, entonces todas las inferencias lógicas de P son implícitas.

Dem: El resultado es una consecuencia inmediata de las definiciones, pues de otra manera todo haz al que pertenezca la fórmula principal de una inferencia explícita terminará con una fórmula final, lo cual es absurdo, ya que no hay fórmulas finales.□

Una consecuencia importante de este resultado es el hecho de que la definición de segmento final de una derivación del secuente vacío puede ser enunciada como sigue:

Segmento Final de una Derivación de $\rightarrow$: El segmento final de una derivación del secuente vacío consiste de todos aquellos secuentes que se encuentran al recorrer cada rama desde el secuente final hasta llegar a una inferencia lógica. En tal caso el secuente superior de esta inferencia ya no pertenece al segmento final, pero el secuente inferior y todos lo secuentes bajo el sí. Dicha inferencia pertenece a la frontera.

Un resultado crucial para el lema fundamental es el hecho de que bajo ciertas hipótesis el segmento final de cualquier derivación del secuente vacío contiene un corte adecuado. Aquí probaremos un resultado más fuerte.

LEMA AUXILIAR. Sea P una AP-derivación que satisface las siguientes condiciones:

i) $P \neq$ segfin(P)

ii) segfin(P) no contiene ninguna inferencia lógica, inducción o dilución.

iii) Si un axioma pertenece a segfin(P), entonces en él no figura ningún símbolo lógico.

En tal caso el segmento-final de P contiene un corte adecuado[3].

<u>Dem</u>: Por inducción fuerte sobre el número de cortes imprescindibles que figuren en segfin(P).

Para esto necesitamos probar primero que hay al menos un corte imprescindible en segfin(P). Por i) tenemos que en P hay inferencias lógicas implícitas, lo cual nos implica que debe haber al menos un corte en segfin(P) (de otra manera habría un número infinito de inferencias lógicas implícitas en la derivación, lo cual es imposible), si tal corte no era ya imprescindible, se puede substituir por uno que sí lo sea (de lo cual puede cerciorarse el lector, por ejemplo, usando el hecho de que si A es derivable también lo es $A \wedge A$).

Sea I un corte imprescindible minimal en segfin(P), i.e., un corte debajo del cual ya no figura ningún corte imprescindible. Si I es un corte adecuado, nada queda por hacer, si no,

[3]Notese que en este resultado no se asume que el secuente final sea $\rightarrow$.

entonces P es de la siguiente forma:

$$I: \frac{P_1 : \left\{ \begin{array}{c} \because\vdots\because \\ \Gamma \rightarrow \Delta, D \end{array} \right. \quad P_2 : \left\{ \begin{array}{c} \because\vdots\because \\ D, \Pi \rightarrow \Lambda \end{array} \right.}{\Gamma, \Pi \rightarrow \Delta, \Lambda}$$

$$\because\vdots\because$$

$$S$$

donde S es el secuente final de P. Como I no es un corte adecuado, una de sus 2 fórmulas de corte no es descendiente de una fórmula principal de una inferencia frontera. Sin perdida de generalidad digamos que tal fórmula es la de la izquierda, i.e., la D en $\Gamma \rightarrow \Delta, D$. A continuación probaremos tres cosas:

a) En P_1 figura una inferencia frontera de P.

Por reducción al absurdo, supongamos que ninguna inferencia frontera de P figura en P_1. En tal caso la D en $\Gamma \rightarrow \Delta, D$ es, necesariamente, descendiente de alguna D que figura en algún axioma que pertenezca a segfin(P). Es más, tal D solamente puede provenir del axioma $D \rightarrow D$, puesto que de otra manera la D habría aparecido de una de las siguientes formas:

$$\frac{\neg D, \Gamma \rightarrow \Delta}{\Gamma \rightarrow \Delta, D} \ (NEG\text{-}D) \qquad \frac{\Gamma \rightarrow \Delta}{\Gamma \rightarrow \Delta, D} \ (DIL\text{-}D)$$

donde tales inferencias pertenecen a segfin(P), pues en P_1 no figuran inferencias frontera, mas tales casos no son posibles debido a la propiedad ii).

Como D desciende del secuente inicial $D \rightarrow D$, el cual pertenece a segfin(P), tenemos, por la propiedad iii), que D es una fórmula atómica, lo cual es una contradicción, pues D es la fórmula de corte en I e I sería en tal caso un corte prescindible.

Por lo tanto, en P_1 figura una inferencia frontera de P.□

b) Si una inferencia J que figura en P_1 es una inferencia frontera de P, entonces J es también una inferencia frontera de P_1.

Sea J una inferencia frontera de P que figure en P_1, i.e. el secuente inferior de J pertenece al segmento final de P, pero su secuente (o secuentes) superior ya no. En tal caso tenemos que:

I) El secuente inferior de J pertenece a segfin(P_1).

Como J es una inferencia frontera de P, entonces, en P, J es una inferencia lógica implícita. Basta ver que no hay una inferencia lógica implícita (según P_1) bajo el secuente inferior de J, pero esto resulta inmediato ya que como J pertenece a segfin(P), entonces toda inferencia de P_1 bajo J se queda en segfin(P) y (por ii)) bajo J no hay inferencias lógicas. En particular, no hay inferencias lógicas implícitas. Por lo tanto el secuente inferior de J pertenece a segfin(P_1).

II) El secuente superior de J ya no pertenece a segfin(P_1).

Basta ver que J, siendo una inferencia implícita en P, lo sigue siendo en P_1, pues de esta forma J será una inferencia implícita que, por supuesto, esta bajo su secuente superior.
Lo anterior es cierto en virtud de que todo haz de P_1 que contenga al secuente superior de J, debe terminar en un corte, pues de lo contrario terminaría en el secuente final de P_1 que es $\Gamma \rightarrow \Delta, D$, lo que no es posible ya que en tal caso D sería descendiente de la fórmula principal de J, contradiciendo nuestra hipótesis.

De I y II concluimos que J es una inferencia frontera de P_1.□

c) segfin(P_1) $\neq P_1$ y el segmento final de P_1 es la intersección de P_1 y el segmento final de P, i.e., segfin(P_1) $= P_1 \cap$ segfin(P).

Que P_1 no es igual a su propio segmento final es claro porque a) y b) implican que en P_1 hay una inferencia lógica implícita.

Veamos que segfin(P_1) $= P_1 \cap$ segfin(P)

$\supseteq$) Basta ver que la contención es valida para las inferencias frontera (¿ Por qué ?). Sea J una inferencia frontera de P que figura en P_1. Por b), J es una inferencia frontera de P_1 que pertenece, por tanto, a segfin(P_1).

$\subseteq$) Tomemos un secuente S en segfin(P_1). En este caso no hay una inferencia lógica implícita, segun P_1, bajo S. Supongamos que $S \notin$ segfin(P), esto es, bajo S hay una inferencia lógica implícita según P. Como sabemos, tal inferencia tiene que estar arriba de I y sus haces asociados no pueden terminar en I (por la hipótesis principal) así que tal inferencia tendría que ser también implícita según P_1, lo cual es una contradicción.□

Como P_1 tiene menos cortes que P, la hipótesis de inducción nos dice que en segfin(P_1)

figura un corte adecuado, así que por c) concluimos que hay un corte adecuado en segfin(P).□

Ahora estamos listos para demostrar el lema fundamental. Su demostración se hará en varios pasos y es completamente constructiva. Se trata en el fondo de un algoritmo que nos permite, a partir de una derivación del secuente vacío, obtener otra con ordinal menor.

LEMA FUNDAMENTAL. Sea P una derivación de $\rightarrow$, entonces existe otra derivación P' de $\rightarrow$ tal que $o(P') < o(P)$.

<u>**Dem**</u>: Suponemos que P es una derivación regular de $\rightarrow$, (si no lo es sabemos que la podemos transformar en una derivación regular, conforme a una proposición anterior, (ver sección 1.6)). Lo que haremos sera describir una reducción de P para obtener P'. Esta reducción consiste de varios pasos, los cuales se aplican un número finito de veces. Además en cada paso que describamos supondremos que el procedimiento anterior ya ha sido aplicado el número de veces que sea posible. En cada paso, el ordinal de la derivación obtenida no crece y al menos en un paso, dicho ordinal decrece.

Primer Paso de Reducción: Supongamos que en el segmento final de P hay presencias libres de una variable, digamos x, que no figura como variable propia. En tal caso usemos el procedimiento de reemplazo, substituyendo cualquier presencia de x por 0. De esta manera obtenemos una derivación de $\rightarrow$ con el mismo ordinal.

El paso 1 se repite hasta asegurar que las únicas variables que figuran libres en P sean las que funcionan como variables propias.

Segundo Paso de Reducción: Supongamos que segfin(P) contiene una inducción. En tal caso P es de la siguiente forma:

$$\begin{array}{c} \because\vdots\because \\ I : \dfrac{F(x), \Gamma \xrightarrow{\mu} \Delta, F(sx)}{F(0), \Gamma \rightarrow \Delta, F(t)} \\ \because\vdots\because \\ \rightarrow \end{array}$$

donde I es una inducción minimal. Denotemos con S y S_0 a los secuentes superior e inferior de I respectivamente y con $P_0(x)$ a la subprueba de P que finaliza con S. Sean $l = h_P(S)$, $k = h_P(S_0)$ y $o_P(S) = \mu$. En tal caso, $o_P(S_0) = \omega_{l-k+1}(\mu_1 + 1)$ donde μ_1 es el primer exponente en la FNC de μ.

Por el primer paso tenemos que ninguna variable libre figura en P bajo I, así que el término t es cerrado. Usando el lema 1 tenemos que hay un número natural m tal que $\to t = \bar{m}$ es derivable sin usar cortes imprescindibles o inducción. Por lo tanto (lema 4), hay una derivación, digamos Q, del secuente $F(\bar{m}) \to F(t)$ que no utiliza cortes imprescindibles ni inducción. Sea $P_0(\bar{n})$ la prueba que se obtiene a partir de $P_0(x)$ mediante el lema del reemplazo. Consideremos la siguiente prueba P':

$$\dfrac{\begin{array}{c} P_0(\bar{0}) \\ \vdots \\ F(0), \Gamma \to \Delta, F(s0) \end{array} \qquad \begin{array}{c} P_0(\bar{1}) \\ \vdots \\ F(s0), \Gamma \to \Delta, F(\bar{2}) \end{array}}{F(0), \Gamma \to \Delta, F(\bar{2})}$$

$$\dfrac{F(0), \Gamma \to \Delta, F(\bar{2}) \qquad \begin{array}{c} P_0(\bar{2}) \\ \vdots \\ F(\bar{2}), \Gamma \to \Delta, F(\bar{3}) \end{array}}{F(0), \Gamma \to \Delta, F(\bar{3})}$$

$$\begin{array}{c} \dfrac{\begin{array}{c} \vdots \\ F(0), \Gamma \to \Delta, F(\bar{m}) \end{array} \qquad \begin{array}{c} Q \\ \vdots \\ F(\bar{m}), \Gamma \to \Delta, F(t) \end{array}}{F(0), \Gamma \to \Delta, F(t)} \\ \vdots \\ \to \end{array}$$

denotemos con S_k al secuente $F(0), \Gamma \rightarrow \Delta, F(\bar{k})$ para $0 < k \leq m$. En este caso todos los S_k tienen la misma altura que S, i.e. $h_{P'}(S_k) = h_P(S) = l$, $0 < k \leq m$, pues las fórmulas $F(\bar{k})$ tienen todas el mismo grado que $F(0)$, no hay inducción y en las fórmulas de corte solo aparecen ellas mismas, de lo cual podemos concluir que:

$$o_{P'}(F(\bar{k}), \Gamma \rightarrow \Delta, F(s\bar{k})) = \mu, \text{ p. t. } 0 \leq k \leq m$$

además, como Q no contiene cortes imprescindibles ni inducción, $o_{P'}(F(\bar{m}), \Gamma \rightarrow \Delta, F(t))$ es un número natural, digamos q, ya que la única manera de que el ordinal pase de finito a infinito es con un corte imprescindible (el grado de un corte prescindible es cero) o con inducción.
Calculemos ahora el ordinal de S_k, $o_{P'}(S_1) = \mu$, $o_{P'}(S_2) = \omega_{l-l}(\mu \oplus \mu) = \omega_0(\mu \oplus \mu) = \mu \oplus \mu$, $o_{P'}(S_3) = \mu \oplus \mu \oplus \mu, \ldots, o_{P'}(S_k) =$ [4] $\mu \otimes k$. Por lo tanto,

$$o_{P'}(S_0) = \omega_{l-k}((\mu \otimes m) \oplus q)$$

y de $q < \omega$ se sigue que ($OR15$) $(\mu \otimes m) \oplus q < (\mu \otimes m) \oplus \omega$. Además, $(\mu \otimes m) \oplus \omega < \omega^{\mu_1+1}$ por $OR10$, así que , usando $OR2$, concluimos lo siguiente:

$$o_{P'}(S_0) = \omega_{l-k}((\mu \otimes m) \oplus q) < \omega_{l-k+1}(\mu_1 + 1) = o_P(S_0)$$

De lo anterior se sigue, por PMD, que $o(P') < o(P)$. Por lo tanto, si segfin(P) contiene una inducción, aquí termina el procedimiento. En adelante suponemos que no hay inducciones en el segmento final de P y pasamos al tercer paso.

Tercer Paso de Reducción: Supongamos que en segfin(P) figura un axioma lógico de la forma $D \rightarrow D$. Como el secuente final es vacío, ambas D deben desaparecer mediante cortes o para ser más precisos, descendientes de ambas D deben desaparecer por cortes.
Supongamos, sin perdida de generalidad que se elimina primero un descendiente de la D en el

[4] Aquí $\mu \otimes k$ denota a $\underbrace{\mu \oplus \ldots \oplus \mu}_{k \text{ veces } \mu}$

antecedente, así que P es de la siguiente forma:

$$\dfrac{\begin{array}{cc} & D \to D \\ \ddots\vdots\cdot\cdot & \ddots\vdots\cdot\cdot \\ \Gamma \to \Delta, D & D, \Pi \to \Lambda \end{array}}{\begin{array}{c}\Gamma, \Pi \to \Delta, \Lambda \\ \ddots\vdots\cdot\cdot \\ \to \end{array}}$$

donde en Λ figura un descendiente de la D del consecuente de $D \to D$; reducimos a P a la siguiente derivación P', utilizando DIL e INT tantas veces como sea necesario:

$$\begin{array}{c} \ddots\vdots\cdot\cdot \\ \dfrac{\Gamma \to \Delta, D}{\Gamma, \Pi \to \Delta, \Lambda}\ (DIL \text{ e } INT) \\ \ddots\vdots\cdot\cdot \\ \to \end{array}$$

denotemos con S al secuente $\Gamma, \Pi \to \Delta, \Lambda$. Obsérvese que bajo S debe figurar otro corte para eliminar al descendiente de D que figura en Λ, lo que implica que $h_P(\Gamma \to \Delta, D) = h_{P'}(\Gamma \to \Delta, D)$, por lo tanto:

$$o_{P'}(S) = o_P(\Gamma \to \Delta, D) < \omega_{h_P(\Gamma \to \Delta, D) - h_P(S)}(o_P(\Gamma \to \Delta, D) \oplus o_P(D, \Pi \to \Lambda)) = o_P(S)$$

Así que por PMD concluimos que $o(P') < o(P)$. Por lo que de ahora en adelante suponemos que en segfin(P) no figuran axiomas lógicos de la forma $D \to D$.

Cuarto Paso de Reducción: Supongamos que en segfin(P) hay una aplicación de dilución y denotemos por I a una dilución minimal dentro de segfin(P). Como el secuente final es vacío, debe existir un corte J bajo I tal que su fórmula de corte sea descendiente de la fórmula principal de I, es decir, P es de la siguiente forma:

$$I : \frac{\Pi' \rightarrow \Xi'}{D, \Pi' \rightarrow \Xi'}$$

$$J : \frac{\Gamma \rightarrow \Delta, D \qquad D, \Pi \rightarrow \Xi}{\Gamma, \Pi \rightarrow \Delta, \Xi}$$

$$\rightarrow$$

vamos a analizar dos casos:

i) Supongamos que en el segmento de P que va desde I hasta J no hay aplicaciones de la regla de contracción. En tal caso transformamos a P en la siguiente derivación P' :

$$\Pi' \rightarrow \Xi'$$

$$\frac{\Pi \rightarrow \Xi}{\Gamma, \Pi \rightarrow \Delta, \Xi} \; (DIL \text{ e } INT)$$

$$\rightarrow$$

en realidad, lo que hemos hecho ha sido podar la rama que contenía a la D, de modo que en P' no hay descendientes de D. Nótese que esto no lleva a ningún problema, pues si bien se introdujo la D mediante una dilución, al final se elimino mediante un corte. Analicemos ahora lo que sucede con los ordinales.

Sean $l = h_P(\Gamma, \Pi \rightarrow \Delta, \Xi)$ y $k = h_P(D, \Pi \rightarrow \Xi)$. Es claro que $l \leq k$ y que $h_{P'}(\Pi \rightarrow \Xi) = h_{P'}(\Gamma, \Pi \rightarrow \Delta, \Xi) = l$.

Sea S un secuente que figura en P arriba de $D, \Pi \rightarrow \Xi$, y sea S' el secuente correspondiente a

S en P' y sean $k_1 = h_P(S), k_2 = h_{P'}(S')$, entonces:

$$o_{P'}(S') \leq \omega_{k_1-k_2}(o_P(S))$$

Omitimos la prueba, que es por inducción sobre el número de inferencias hasta $D, \Pi \to \Xi$.
Sean $\mu_1 = o_P(\Gamma \to \Delta, D)$, $\mu_2 = o_P(D, \Pi \to \Xi)$, $\nu = o_P(\Gamma, \Pi \to \Delta, \Xi)$, $\mu_2' = o_{P'}(\Pi \to \Xi)$ y $\nu' = o_{P'}(\Gamma, \Pi \to \Delta, \Xi)$[5]. Utilizando el resultado anterior tenemos que:

$$\mu_2' \leq \omega_{k-l}(\mu_2)$$

además:

Si $\mu_2 < \mu_2 \oplus \mu_1$ entonces (por $OR2$) $\omega_{k-l}(\mu_2) < \omega_{k-l}(\mu_2 \oplus \mu_1) = \nu$

de donde concluimos que

$$\nu' = \mu_2' \leq \nu$$

es decir, $o_{P'}(\Gamma, \Pi \to \Delta, \Xi) \leq o_P(\Gamma, \Pi \to \Delta, \Xi)$ por lo que, (usando PMD)concluimos que $o(P') \leq o(P)$.

ii) Si no se da el caso i), sea I^+ la contracción aplicada a D que se encuentre más arriba entre I y J, esto es, P es de la siguiente forma:

$$\begin{array}{c} \ddots \vdots \cdot^{\cdot^{\cdot}} \\ I : \dfrac{\Pi' \to \Xi'}{D, \Pi' \to \Xi'} \\ \ddots \vdots \cdot^{\cdot^{\cdot}} \\ I^+ : \dfrac{D, D, \Pi'' \to \Xi''}{D, \Pi'' \to \Xi''} \end{array}$$

[5]Notese que $\mu_2' = \nu'$

$$J: \frac{\begin{matrix} \ddots\vdots\cdot\cdot & & \ddots\vdots\cdot\cdot \\ \Gamma \to \Delta, D & & D, \Pi \to \Xi \end{matrix}}{\Gamma, \Pi \to \Delta, \Xi}$$

$$\ddots\vdots\cdot\cdot$$

$$\to$$

En tal caso reducimos a P a la siguiente derivación P' :

$$\ddots\vdots\cdot\cdot$$

$$\Pi' \to \Xi'$$

$$\ddots\vdots\cdot\cdot$$

$$D, \Pi'' \to \Xi''$$

$$\ddots\vdots\cdot\cdot$$

$$D, \Pi \to \Xi$$

$$\ddots\vdots\cdot\cdot$$

Lo que hemos hecho para obtener P' es lo mismo que en el caso anterior: eliminar la rama que contiene a la D de la inferencia I. En tal caso, al llegar a las contracciones, su secuente superior se vuelve idéntico al inferior, así que se borra la inferencia y se conserva el secuente superior, quedando intacta la prueba. Es claro que en este caso $o(P') = o(P)$. Por lo tanto de ahora en adelante suponemos que en el segmento final de P no figura ninguna dilución.

OBSERVACIÓN: De los 4 pasos de reducción anteriores, podemos concluir que

$$segfin(P) \neq P$$

Porque de lo contrario tendríamos lo siguiente:

i) En P no figuran inferencias lógicas y por lo tanto no hay presencias libres de variables, pues P es regular.

ii) En P todos los cortes son prescindibles, porque las únicas maneras en las que puede aparecer una fórmula con símbolos lógicos es mediante inferencias lógicas o mediante axiomas del tipo $D \to D$, con D una fórmula con símbolos lógicos.

iii) Por lo tanto i) y ii) implican que P es una derivación simple.

con base en la PDS concluimos que el secuente final de P no puede ser vacío, lo cual es un absurdo. Por lo tanto segfin$(P) \neq P$.

Hasta este momento hemos transformado nuestra derivación original en una derivación con las siguientes propiedades:

i) segfin$(P) \neq P$

ii) En segfin(P) no figuran inferencias lógicas, pues éstas tendrían que ser explícitas.

iii) En segfin(P) no figuran inducciones ni diluciones, por los pasos de reducción 2 y 4.

iv) En segfin(P) no figura ningún axioma con un símbolo lógico, por el tercer paso de reducción.

De manera que por el lema auxiliar concluimos que en segfin(P) figura un corte adecuado con lo cual procedemos a nuestro quinto paso de reducción, el cual es el mas importante de todos.

Quinto Paso de Reducción (Reducción Esencial): Sea I un corte adecuado minimal en segfin(P). Analizaremos varios casos.

I) La fórmula de corte de I es de la forma $A \wedge B$, digamos que P es:

$$
\begin{array}{c}
\begin{array}{ccc}
\begin{array}{c}
\vdots \qquad\qquad \vdots \\
I_1 : \dfrac{\Gamma' \to \Theta', A \quad \Gamma' \to \Theta', B}{\Gamma' \to \Theta', A \wedge B} \\
\vdots \\
\Gamma \xrightarrow{l} \Theta, A \wedge B
\end{array}
& \qquad\qquad &
\begin{array}{c}
\vdots \\
I_2 : \dfrac{A, \Pi' \to \Lambda'}{A \wedge B, \Pi' \to \Lambda'} \\
\vdots \\
A \wedge B, \Pi \xrightarrow{l} \Lambda
\end{array}
\end{array} \\
I : \overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad} \; (l) \\
\Gamma, \Pi \to \Theta, \Lambda \\
\vdots \\
\Delta \xrightarrow{k} \Xi \qquad (k) \\
\vdots \\
\to
\end{array}
$$

donde $l = h_P(\Gamma \to \Theta, A \wedge B) = h_P(A \wedge B, \Pi \to \Lambda)$, $k = h_P(\Delta \to \Xi)$ y $\Delta \to \Xi$ denota al secuente bajo I que tiene menor altura que la de los secuentes superiores de I y que está más arriba en la prueba (i.e. entre I y $\Delta \to \Xi$ todos los secuentes tienen altura l)[6]. De lo anterior se sigue que $\Delta \to \Xi$ es el secuente inferior de un corte, pues no hay aplicaciones de IND bajo I.

Sean $\mu = o(\Gamma \to \Theta, A \wedge B)$, $\nu = o(A \wedge B, \Pi \to \Lambda)$, $\lambda = o(\Delta \to \Xi)$ como se ve en el esquema. Consideremos las siguientes derivaciones:

P_1 :

$$\ddots\vdots\ddots$$

$$\frac{\Gamma' \to \Theta', A}{\Gamma' \to A, \Theta'}(INT)$$

$$\frac{\Gamma' \to A, \Theta'}{\Gamma' \to A, \Theta', A \wedge B}(DIL-D)$$

$$\ddots\vdots\ddots$$

$$J_1 : \quad \frac{\Gamma \xrightarrow{\mu_1} A, \Theta, A \wedge B \qquad A \wedge B, \Pi \xrightarrow{\nu_1} \Lambda}{\Gamma, \Pi \to A, \Theta, \Lambda}\ (l)$$

$$\ddots\vdots\ddots$$

$$\frac{\Delta \xrightarrow{\lambda_1} A, \Xi}{\Delta \to \Xi, A}\ (INT)\ (m)$$

P_2 :

$$\ddots\vdots\ddots$$

$$\frac{A, \Pi' \to \Lambda'}{\Pi', A \to \Lambda'}$$

$$\frac{\Pi', A \to \Lambda'}{A \wedge B, \Pi', A \to \Lambda'}\ (DIL-I)$$

$$\ddots\vdots\ddots$$

$$\ddots\vdots\ddots \qquad\qquad \ddots\vdots\ddots$$

$$J_2 : \frac{\Gamma \xrightarrow{\mu_2} \Theta, A \wedge B \qquad A \wedge B, \Pi, A \xrightarrow{\nu_2} \Lambda}{\Gamma, \Pi, A \to \Theta, \Lambda}\ (l)$$

$$\ddots\vdots\ddots$$

[6]Tal secuente bien podria ser $\to$ ó $\Gamma, \Pi \to \Theta, \Lambda$ y existe por propiedades de la altura.

$$\frac{\Delta, A \xrightarrow{\lambda_3} \Xi}{A, \Delta \rightarrow \Xi} \; (INT) \; (m)$$

nótese que P_1 y P_2 se obtienen a partir de la subprueba de P que termina en $\Delta \rightarrow \Xi$, agregando en toda la prueba la fórmula A y eliminando en cada caso la inferencia lógica I_1 o I_2.
Definimos la derivación P' como sigue:

$$\begin{array}{c}
\begin{array}{cc} P_1 & P_2 \\ \cdot\cdot\vdots\cdot\cdot & \cdot\cdot\vdots\cdot\cdot \end{array} \\
\dfrac{\Delta \xrightarrow{\lambda_1} \Xi, A \qquad A, \Delta \xrightarrow{\lambda_3} \Xi}{\dfrac{\Delta, \Delta \xrightarrow{\lambda_0} \Xi, \Xi}{\Delta \rightarrow \Xi}} \; (m) \\
\cdot\cdot\vdots\cdot\cdot \\
\rightarrow
\end{array}$$

Donde $m = h_{P'}(\Delta \rightarrow A, \Xi) = h_{P'}(A, \Delta \rightarrow \Xi)$, $l = h_{P'}(\Gamma \rightarrow A, \Theta, A \wedge B) = h_{P'}(A \wedge B, \Pi \rightarrow \Lambda)$, $k = h_P(\Delta \rightarrow \Xi)$. Un hecho que le debe quedar claro al lector es que la altura de $\Gamma \rightarrow A, \Theta, A \wedge B$ en P' es la misma que la altura de $\Gamma \rightarrow \Theta, A \wedge B$ en P, que es l. puesto que todas las fórmulas de corte que figuran en P bajo I, figuran en P' bajo J_1 y todas las fórmulas de corte bajo J_1 en P', (excepto A) figuran en P bajo I, y $grd(A) < grd(A \wedge B) \leq l$. Tenemos un resultado análogo para el secuente $A \wedge B, \Pi, A \rightarrow \Lambda$.

Veamos ahora que relación hay entre k, m y l. Para lo cual analizaremos dos casos:

a) $k \leq grd(A)$. En tal caso es inmediato que $m = h_{P'}(\Delta \rightarrow A, \Xi) = grd(A)$ conforme a las definiciones.

b) $k > grd(A)$. Podemos concluir, también de manera inmediata que $m = k$.

En cualquier caso tenemos que $k \leq m < l$.

Sean $\mu, \nu, \mu_1, \nu_1, \mu_2, \nu_2, \lambda_0, \lambda_1, \lambda_2$ como aparecen en las derivaciones anteriores. En tal caso:

i) $\mu_1 < \mu$. Esto es claro porque en P el secuente $\Gamma' \rightarrow \Theta', A \wedge B$ se obtuvo mediante una inferencia *DISY-D* y en P' el secuente correspondiente $\Gamma' \rightarrow A, \Theta', A \wedge B$ se obtuvo por dilución, explícitamente:

$$o_{P'}(\Gamma' \rightarrow A, \Theta', A \wedge B) = o_{P'}(\Gamma' \rightarrow A, \Theta') = o_P(\Gamma' \rightarrow A, \Theta') < o_P(\Gamma' \rightarrow \Theta', A \wedge B)$$

Así que por la PMD concluimos que $\mu_1 < \mu$.

ii) $\nu_1 = \nu$. Esto es obvio, por la construcción de P_1.

iii) $\mu_2 = \mu$. Igual que ii).

iv) $\nu_2 < \nu$. Análogo a i).

Ahora, sea

$$J' : \frac{S_1' \quad S_2'}{S} \quad \begin{matrix} (k_1) \\ (k_2) \end{matrix}$$

una inferencia cualquiera[7] que figure entre J_1 y $\Delta \to A, \Xi$, y sea

$$J : \frac{S_1 \quad S_2}{S}$$

la inferencia en P correspondiente a J' entre I y $\Delta \to \Xi$. Además sean

$$\begin{array}{lll} \alpha_1' = o_{P'}(S_1') & \alpha_2' = o_{P'}(S_2') & \alpha' = o_{P'}(S') \\ \alpha_1 = o_P(S_1) & \alpha_2 = o_P(S_2) & \alpha = o_P(S) \\ k_1 = h_{P'}(S_1') & k_1 = h_{P'}(S_2') & k_2 = h_{P'}(S') \end{array}$$

De lo anterior se sigue que $\alpha' = \omega_{k_1-k_2}(\alpha_1' \oplus \alpha_2')$ y $\alpha = \omega_{l-k}(\alpha_1 \oplus \alpha_2)$, cuando S' es $\Delta \to A, \Xi$ y $\alpha = \alpha_1 \oplus \alpha_2$ en otro caso, pues J' es necesariamente un corte, en virtud de que está en el segmento final de P y el secuente inferior de J tiene la misma altura que sus secuentes superiores (por la propiedad del secuente $\Delta \to \Xi$), así que:

$$\alpha = \omega_{h_P(S_1)-h_P(S)}(\alpha_1 \oplus \alpha_2) = \omega_0(\alpha_1 \oplus \alpha_2) = \alpha_1 \oplus \alpha_2$$

es más, la siguiente desigualdad es valida, siempre y cuando S' no sea $\Delta \to A, \Xi$:

$$\alpha' < \omega_{l-k_2}(\alpha)$$

la demostración de este hecho es análoga a la demostración de la Propiedad de Monotonía y nos limitaremos al caso en que $J' = J_1$:

[7]Cuidado!. no estamos diciendo que entre J_1 y $\Delta \to A, \Xi$ solamente haya inferencias de este tipo, sino que estamos considerando sólo a estas.

En tal caso tenemos que: $\alpha' = \omega_{l-k_2}(\mu_1 \oplus \nu_1)$ y $\alpha = \omega_{l-l}(\mu \oplus \nu) = \mu \oplus \nu$. Por lo tanto: como $\mu_1 < \mu$ entonces, por $OR15$, $\mu_1 \oplus \nu_1 < \mu \oplus \nu_1 = \mu \oplus \nu$ lo cual implica, por $OR2$, que

$$\alpha' = \omega_{l-k_2}(\mu_1 \oplus \nu_1) < \omega_{l-k_2}(\mu \oplus \nu) = \omega_{l-k_2}(\alpha)$$

dicho resultado nos indica que:

$$\lambda_1 < \omega_{l-m}(\kappa) \quad \text{y} \quad \lambda_2 < \omega_{l-m}(\kappa)$$

donde κ es la suma natural de los ordinales de los secuentes superiores del corte cuyo secuente inferior es $\Delta \rightarrow A, \Xi$ ó $\Delta, A \rightarrow \Xi$. Por $OR7$ esto implica que $\lambda_1 \oplus \lambda_2 < \omega_{l-m}(\kappa)$ así que:

$$\lambda_0 = \omega_{m-k}(\lambda_1 \oplus \lambda_2) < \omega_{m-k}(\omega_{l-m}(\kappa)) = \omega_{l-k}(\kappa) = \lambda$$

por último, la Propiedad de monotonía nos permite concluir que:

$$o(P') < o(P)$$

II) La fórmula de corte es de la forma $\forall x F(x)$, de modo que P es de la siguiente forma:

$$
\dfrac{\begin{array}{c}\ddots\vdots\ddots \\ I_1 : \dfrac{\Gamma' \rightarrow \Theta', F(a)}{\Gamma' \rightarrow \Theta', \forall x F(x)} \\ \ddots\vdots\ddots \\ \Gamma \rightarrow \Theta, \forall x F(x)\end{array} \qquad \begin{array}{c}\ddots\vdots\ddots \\ I_2 : \dfrac{F(s), \Pi' \rightarrow \Lambda'}{\forall x F(x), \Pi' \rightarrow \Lambda'} \\ \ddots\vdots\ddots \\ \forall x F(x), \Pi \rightarrow \Lambda\end{array}}{\Gamma, \Pi \rightarrow \Theta, \Lambda}\; I
$$

$$\begin{array}{c}\ddots\vdots\ddots \\ \Delta \rightarrow \Xi \\ \ddots\vdots\ddots \\ \rightarrow\end{array}$$

donde el secuente $\Delta \rightarrow \Xi$ tiene la misma propiedad que en el caso I). La derivación P' se define

en términos de las siguientes derivaciones P_1 y P_2 :

P_1 :

$$\begin{array}{c} \ddots\vdots\cdot\cdot \\ \dfrac{\Gamma' \rightarrow \Theta', F(s)}{\Gamma' \rightarrow F(s), \Theta'}(INT) \\ \dfrac{\Gamma' \rightarrow F(s), \Theta'}{\Gamma' \rightarrow A, \Theta', \forall x F(x)}(DIL-D) \\ \ddots\vdots\cdot\cdot \end{array}$$

$$J_1 : \quad \dfrac{\Gamma \rightarrow F(s), \Theta, \forall x F(x) \qquad \forall x F(x), \Pi \rightarrow \Lambda}{\Gamma, \Pi \rightarrow F(s), \Theta, \Lambda}$$

$$\begin{array}{c} \ddots\vdots\cdot\cdot \\ \dfrac{\Delta \rightarrow F(s), \Xi}{\Delta \rightarrow \Xi, F(s)}(INT) \end{array}$$

aquí se obtuvo una derivación de $\Gamma' \rightarrow \Theta', F(s)$ a partir de una prueba de $\Gamma' \rightarrow \Theta', F(a)$ mediante el lema del reemplazo.

P_2 :

$$\begin{array}{c} \ddots\vdots\cdot\cdot \\ \dfrac{F(s), \Pi' \rightarrow \Lambda'}{\Pi', F(s) \rightarrow \Lambda'} \\ \dfrac{\Pi', F(s) \rightarrow \Lambda'}{\forall x F(x), \Pi', F(s) \rightarrow \Lambda'}(DIL-I) \\ \ddots\vdots\cdot\cdot \end{array}$$

$$J_2 : \dfrac{\begin{array}{c}\ddots\vdots\cdot\cdot \\ \Gamma \rightarrow \Theta, \forall x F(x)\end{array} \qquad \begin{array}{c}\ddots\vdots\cdot\cdot \\ \forall x F(x), \Pi, F(s) \rightarrow \Lambda\end{array}}{\Gamma, \Pi, F(s) \rightarrow \Theta, \Lambda}$$

$$\begin{array}{c} \ddots\vdots\cdot\cdot \\ \dfrac{\Delta, F(s) \rightarrow \Xi}{F(s), \Delta \rightarrow \Xi}(INT) \end{array}$$

finalmente construimos P' :

$$\cfrac{\cfrac{\begin{array}{cc} P_1 & P_2 \\ \vdots & \vdots \\ \Delta \rightarrow \Xi, F(s) & F(s), \Delta \rightarrow \Xi \end{array}}{\Delta, \Delta \rightarrow \Xi, \Xi}}{\begin{array}{c} \Delta \rightarrow \Xi \\ \vdots \\ \rightarrow \end{array}}$$

y en este caso el argumento para los ordinales es completamente análogo, concluyéndose lo siguiente:

$$o(P') < o(P)$$

III) La fórmula de corte es de la forma $\neg A$, de modo que P es de la siguiente forma:

$$\begin{array}{c} \begin{array}{cc} \vdots & \vdots \\ I_1 : \dfrac{A, \Gamma' \rightarrow \Theta'}{\Gamma' \rightarrow \Theta', \neg A} & I_2 : \dfrac{\Pi' \rightarrow \Lambda', A}{\neg A, \Pi' \rightarrow \Lambda'} \\ \vdots & \vdots \end{array} \\ I : \dfrac{\Gamma \rightarrow \Theta, \neg A \qquad\qquad \neg A, \Pi \rightarrow \Lambda}{\Gamma, \Pi \rightarrow \Theta, \Lambda} \\ \vdots \\ \Delta \rightarrow \Xi \\ \vdots \\ \rightarrow \end{array}$$

donde $\Delta \rightarrow \Xi$ es como en I). De manera análoga a los casos anteriores, construimos las pruebas P_1 y P_2 de la siguiente manera:

P_1 :

$$\frac{A, \Gamma' \rightarrow \Theta'}{A, \Gamma' \rightarrow \Theta', \neg A}(DIL - D)$$

$$
J_1 : \quad \dfrac{\begin{array}{cc} \vdots & \vdots \\ A, \Gamma \to \Theta, \neg A & \neg A, \Pi \to \Lambda \end{array}}{\begin{array}{c} A, \Gamma, \Pi \to \Theta, \Lambda \\ \vdots \\ A, \Delta \to \Xi \end{array}}
$$

P_2 :

$$
\dfrac{\Pi' \to \Lambda', A}{\neg A, \Pi' \to \Lambda', A}\ (DIL - I)
$$
$$
\vdots
$$

$$
J_2 : \quad \dfrac{\begin{array}{cc} \vdots & \vdots \\ \Gamma \to \Theta, \neg A & \neg A, \Pi \to \Lambda, A \end{array}}{\begin{array}{c} \Gamma, \Pi \to \Theta, \Lambda, A \\ \vdots \\ \Delta \to \Xi, A \end{array}}
$$

sólo que en este caso P' sufre una variación, que es el intercambiar las derivaciones P_1 y P_2 de su lugar original.

P' :

$$
\dfrac{\begin{array}{cc} P_2 & P_1 \\ \vdots & \vdots \\ \Delta \to \Xi, A & A, \Delta \to \Xi \end{array}}{\dfrac{\Delta, \Delta \to \Xi, \Xi}{\begin{array}{c} \Delta \to \Xi \\ \vdots \\ \to \end{array}}}
$$

Las relaciones entre los ordinales son análogas al caso I) y su demostración se deja al lector. En cualquiera de los 3 casos construimos una derivación P' tal que

$$
o(P') < o(P)
$$

Con lo que damos por concluida la demostración del lema fundamental.□

2.7 AP es Consistente

Esta sección es el núcleo de todo el trabajo, pues si bien la prueba de consistencia es un corolario del lema fundamental, creemos que merece un tratamiento independiente, dada la importancia del resultado.

TEOREMA. AP es Consistente.

<u>Dem</u>: Por reducción al absurdo, supongamos que la aritmética es inconsistente. En tal caso en AP es derivable el secuente vacío $\rightarrow$. Con base en lo anterior construiremos una sucesión de ordinales ε_0-dominada que no será finita, contradiciendo así el hecho de que ε_0 es accesible. Nuestra construcción se hace por recursión para naturales. Sea P una derivación cualquiera de $\rightarrow$. Definimos la sucesión de derivaciones (P_n) como:

$$\begin{aligned} P_1 &= P \\ P_{n+1} &= P'_n \end{aligned}$$

donde P'_n es la derivación de $\rightarrow$ obtenida a partir de P_n mediante el lema fundamental. Entonces la sucesión (μ_n) definida como:

$$\begin{aligned} \mu_1 &= o(P_1) \\ \mu_{n+1} &= o(P_{n-1}) \end{aligned}$$

es estrictamente decreciente e infinita, lo cual es una contradicción, ya que (μ_n) es ε_0-dominada y ε_0 es accesible. Por lo tanto, no puede existir una derivación de $\rightarrow$, i.e., AP es consistente.□

OBSERVACIÓN: Con frecuencia se dice que la consistencia de AP se demuestra mediante una inducción transfinita sobre los ordinales de las derivaciones, como si estuviéramos usando un principio general de inducción transfinita para demostrar la consistencia de la inducción finita.

Sin embargo esto es incorrecto. Lo que realmente sucede es que la prueba de consistencia que

acabamos de desarrollar utiliza la noción de accesibilidad del ordinal ε_0 tal como está explicada en la sección 2.2. Además de esto, solamente se utilizaron métodos estrictamente finitistas.
En cuanto a la inducción transfinita tenemos lo siguiente: El principio de inducción transfinita para el buen orden $\prec$ se puede expresar con el siguiente esquema:

$$IT(\prec, F(x)) : \forall x[\forall y(y \prec x \Rightarrow F(y)) \Rightarrow F(x)] \rightarrow \forall x F(x)$$

Donde $F(x)$ denota a una fórmula cualquiera del sistema considerado. Ahora bien, si consideramos a los ordinales menores que ε_0 junto con su orden usual $<$, ($ORD.$ $<$) tenemos que la prueba de consistencia de AP se puede formalizar en el sistema de la aritmética recursiva primitiva junto con el axioma $IT(<, F(x))$.
Lo que haremos en el último capitulo es mostrar que la inducción transfinita hasta ε_0 no puede ser formalizada en AP.

2.7.1 Otras Pruebas de Consistencia

Cabe señalar que la prueba que acabamos de presentar, aunque esta basada en la primera prueba de consistencia de la aritmética que se conoce ([Gen1]), no es la única, a continuación mencionaremos otras pruebas en orden cronológico.
1940 Ackermann W. Zur widerspruchsfreiheit der Zahlentheorie. Mathematische Annalen Vol. 117. Una exposición de esta prueba se encuentra en: Wang Hao. A Survey of Mathematical Logic. North Holland 1964.
1951 Lorenzen P. Algebraische und logistische untersuchungen über freien Verhände. Journal of Symbolic Logic Vol. 16.
1951 Schütte K. Beweistheoretische Erfassung der unendlichen Induktion in der Zahlentheorie. Mathematische Annalen Vol. 122. Una prueba más elemental que la de este trabajo y que esta basada en la prueba de Schütte se puede encontrar en el apéndice de la primera edición del libro de Mendelson [Men], desgraciadamente dicha prueba no aparece en ediciones posteriores.
1958 Gödel K. Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes. Hay traducción al ingles en: Collected Works of Kurt Gödel Vol. II, editado por Solomon Feferman, Oxford University Press, 1990.

1959 Hlodovskii. A New Proof of the Consistency of Arithmetic. Usp. Mat. Nauk. Vol. 14 No. 6, (En Ruso).
1960 Schütte. Beweistheorie. Hay traducción al ingles en [Sch]. Esta segunda prueba de Schütte utiliza los métodos de Gödel, hay un trabajo reciente basado en estas pruebas en [Ru].
1967 Shoenfield J. Mathematical Logic. Addison Wesley. Esta prueba también esta basada en la prueba de Gödel.

2.8 Algunos Ejercicios Interesantes

En esta sección enunciaremos 4 ejercicios de interés, los cuales no son sencillos pero se basan en lo que se ha hecho en este capítulo.

1) Es posible extender el procedimiento de reducción del lema fundamental de la siguiente manera:

Decimos que un secuente S cumple la propiedad P syss:

i) Todas las fórmulas de S son cerradas.

ii) Cada fórmula en el consecuente de S esta libre de cuantificadores o es de la forma $\exists y_1 ... \exists y_m R(y_1, ..., y_m)$ donde R esta libre de cuantificadores.

iii) Cada fórmula en el antecedente de S esta libre de cuantificadores o es de la forma $\forall y_1 ... \forall y_m R(y_1, ..., y_m)$ donde R esta libre de cuantificadores.

Muestre que si un secuente que cumple P es derivable en AP entonces es derivable sin cortes imprescindibles ni inducción. (Sugerencia: Se puede suponer que en el segmento final de la derivación de tal secuente no figura ninguna variable libre que no sea usada como eigenvariable.)

2) La Aritmética Intuicionista se puede formalizar como el subsistema de AP que consiste de todos los secuentes cuyo consecuente tiene a lo más una fórmula, la cual tiene cuantificadores. Este sistema se llama AH (en honor de Arend Heyting).

El método de reducción del lema fundamental de AP funciona también para AH con la siguiente modificación: En una reducción esencial, si la fórmula de corte en un corte adecuado contiene un cuantificador entonces la inferencia DIL-D no se introduce.

Defina de manera precisa el método de reducción para AH, probando así de manera directa la consistencia de AH y no como un subsistema de AP.

3) Considérese la siguiente propiedad (*) de fórmulas: Decimos que una fórmula A cumple (*) syss cualquier conectivo $\vee$ o $\exists$ que figure en A esta en el alcance de un conectivo $\neg$ o en el alcance izquierdo de un conectivo $\Rightarrow$.
Muestre que si cada fórmula de Γ cumple (*) y las fórmulas de Γ, A, B y $\exists x F(x)$ son cerradas, entonces en AH :

i) $\Gamma \rightarrow A \vee B$ syss $\Gamma \rightarrow A$ o $\Gamma \rightarrow B$

ii) $\Gamma \rightarrow \exists x F(x)$ syss $\Gamma \rightarrow F(s)$ para algún término cerrado s.

Sugerencia: (B. Scarpellini) Inducción Transfinita sobre $o(P)$, donde P es una derivación de $\Gamma \rightarrow A \vee B$ o de $\Gamma \rightarrow \exists x F(x)$ respectivamente, siguiendo el método de reducción para AP. Es más fácil si se analizan primero las inferencias en $segfin(P)$.

4) Considérese el subsistema de la aritmética obtenido al restringir las fórmulas de inducción a aquellas que tienen a lo más k cuantificadores, dicho sistema se denota AP_k. Pruebe que la consistencia de AP_k puede derivarse mediante inducción transfinita hasta ω_{k+1}.
Para un esbozo de la prueba ver [Tak].

Capítulo 3

LA NO DEMOSTRABILIDAD DE IT(ε_0)

En este capítulo probaremos la no demostrabilidad de la inducción transfinita hasta el ordinal ε_0, cosa que podemos hacer de dos maneras. La primera y más simple es apelando al segundo teorema de incompletud de Gödel. No obstante, dado que dicho teorema no ha sido estudiado con detalle, preferimos probar la no demostrabilidad basándonos nuevamente en un artículo de *Gerhard Gentzen* de 1943 ([Gen3]).

Como veremos, nuestro resultado es óptimo, es decir, realmente tenemos que llegar al ordinal ε_0 para demostrar la consistencia de AP, pues el principio de inducción hasta cualquier ordinal estrictamente menor que ε_0 si es demostrable en AP. Formalicemos un poco estas ideas:

Con $IT(\mu)$ abreviamos a la familia de secuentes de la forma:

$$\forall x[\forall y[y < x \Rightarrow A(y)] \Rightarrow A(x)] \rightarrow \forall x[x \leq \mu \Rightarrow A(x)]$$

para cualquier fórmula A de AP. Es claro que estas fórmulas están formalizando el principio de inducción transfinita hasta el ordinal μ[1].

Lo que vamos a hacer en este capítulo son dos cosas:

[1] Aunque parece más correcto formalizar la Inducción Transfinita hasta μ con el secuente

$$\forall x[x \leq \mu \Rightarrow (\forall y[y < x \Rightarrow A(y)] \Rightarrow A(x))] \rightarrow \forall x[x \leq \mu \Rightarrow A(x)]$$

ambos secuentes, este y el que utilizaremos, son equivalentes.

i) Probaremos que la inducción transfinita hasta cualquier ordinal menor que ε_0 es derivable, para lo cual basta ver que $IT(\omega_n)$ es derivable (abusando de la manera de hablar), para cualquier $n \in \mathbb{N}$. y

ii) Probaremos que $IT(\varepsilon_0)$ no es derivable, i.e., que la inducción transfinita hasta ε_0 no es demostrable en AP.

Empezamos con la prueba más sencilla, que es la prueba indirecta.

3.1 Prueba Indirecta

La imposibilidad de demostrar el principio de inducción transfinita hasta el ordinal ε_0 con técnicas de la aritmética se deriva indirectamente de los siguientes dos hechos:

I) El Segundo Teorema de Incompletud de Gödel: Si la Aritmética es consistente, entonces es imposible derivar en ella la fórmula que "asevera" su consistencia. Esto es, la consistencia de AP no puede ser probada con recursos formalizables en AP.

II) La consistencia de AP se puede probar en un sistema en donde también es posible probar la inducción transfinita hasta ε_0 (cfr. última observación del capítulo 2).

Dado que hemos probado que la aritmética es realmente consistente, el Segundo Teorema de Gödel realmente se puede enunciar (con base en la aceptación de tal prueba) de la siguiente forma: La Aritmética es incapaz de probar su propia consistencia.

De lo anterior se sigue que el principio de inducción hasta ε_0 es indemostrable en AP.

3.2 Extensión de la Aritmética

Lo primero que necesitaremos para nuestra prueba directa de no demostrabilidad es extender nuestro sistema AP de la siguiente forma. Sea ξ una nueva letra predicativa de aridad uno y sea $\mathfrak{L}_{AP}(\xi)$ el lenguaje obtenido a partir del lenguaje de la aritmética $\mathfrak{L}_{AP}$ admitiendo $\xi(t)$ como fórmula atómica para cualquier término t. Con $AP(\xi)$ denotamos a la extensión del sistema formal AP obtenida aceptando como secuentes iniciales a los de la forma:

$$s = t, \xi(s) \rightarrow \xi(t)$$

para cualesquiera términos s y t, y permitiendo la aplicación de la regla de inducción a todas las fórmulas de $AP(\xi)$. Además nuestro universo de discurso contara entre sus "habitantes" a todos los ordinales menores que ε_0. Debe quedar claro que todos nuestros conceptos gramaticales, como el ser fórmula, secuente, axioma, etc..., quedan sin cambio alguno. A una derivación según AP le llamaremos derivación ordinaria en $AP(\xi)$ para distinguirla de lo que llamaremos una derivación por inducción transfinita, concepto que utilizaremos frecuentemente y que explicaremos en la siguiente sección.

Aceptaremos como axiomas a los secuentes de la forma

$$A, A \Rightarrow B \to B$$

para evitar escribir toda su derivación en nuestro desarrollo, a los secuentes

$$\to s = t \text{ ó } t = s \to$$

donde s, t son términos cerrados, segun sea el caso, de acuerdo a la demostración del lema 2 del capítulo 2. Por último, a cualquier teorema aritmético elemental , como por ejemplo

$$\to \beta < \alpha + 1 \Rightarrow \beta \leq \alpha$$

o lo que es lo mismo

$$\beta < \alpha + 1 \to \beta \leq \alpha$$

puesto que el derivar este tipo de teoremas no debe presentar ninguna dificultad, la justificación para este tipo de secuentes se denotara (TA).

Tenemos también las siguientes reglas de inferencia derivadas, cuya prueba de validez es un excelente ejercicio.

$$i)\frac{\Gamma \to A \Rightarrow B, \Delta}{\Gamma, A \to B, \Delta} \qquad ii)\frac{\Gamma \to \Delta, \forall x F(x)}{\Gamma \to \Delta, F(a)}$$

Estas reglas se justificaran con la notación (RDI) y (RDU) respectivamente. En la regla $ii)$, a debe ser substituible por x.

3.3 IT-Derivaciones

Para poder precisar el concepto de derivación por inducción transfinita o IT-Derivación, formularemos primero un esquema para dicho tipo de inducción. Modifiquemos para ello nuestra regla de inducción, puesto que ahora estamos considerando a todos los ordinales, de la siguiente manera[2]:

$$\frac{a < \omega, F(a), \Gamma \to \Delta, F(sa)}{t < \omega, F(0), \Gamma \to \Delta, F(t)}\ (IND).$$

El esquema de inferencia llamado regla de inducción transfinita, es similar al esquema de inducción:

$$\frac{a > 0, \forall x[x < a \Rightarrow F(x)], \Gamma \to \Delta, F(a)}{F(0), \Gamma \to \Delta, F(t)}\ (INDT)$$

donde a debe cumplir las mismas restricciones que en la regla IND. (cfr. sección 2.1) y t debe ser un término cerrado.

Este esquema esta formalizando el principio de inducción transfinita hasta el ordinal representado por el termino t. El lector debe cerciorarse de que la validez de esta inferencia es equivalente a la derivabilidad de $IT(t)$. En este caso una prueba que utiliza el principio de inducción transfinita será formalizada con una derivación en la que aparecerá alguna aplicación de la regla $INDT$.

Dicho esquema no será utilizado en nuestro desarrollo, su único propósito es el de aclarar la siguiente

DEFINICIÓN. Una IT-Derivación hasta t es una derivación con las siguientes propiedades:

i) La letra predicativa ξ figura en la derivación.

ii) El secuente final de la derivación es de la forma $\xi(0) \to \xi(t)$.

iii) Los siguientes secuentes son admitidos como iniciales:

$$t > 0, \forall x[x < t \Rightarrow \xi(x)] \to \xi(t)$$

y se llaman IT-Secuentes Superiores ($ITSS$). La fórmula $\xi(t)$ es la fórmula principal del secuente.

---

[2]Recuerdese que $\omega = \mathbf{N}$

Aclaremos por qué una IT-Derivación realmente formaliza lo que entendemos por una prueba de la validez del principio de inducción transfinita.
Una prueba informal que se sirve del principio de inducción transfinita hasta t, se formalizaría en una derivación en la cual figuraría una aplicación de la regla $INDT$. Supongamos pues que tenemos una tal derivación y que tenemos una IT-Derivación hasta t. En tal caso podríamos eliminar la aplicación de $INDT$ de la siguiente manera:
Se hace un injerto en el árbol de derivación, eliminando la aplicación de $INDT$ y substituyéndola con la IT-Derivación que ya teníamos, de manera que resulte una derivación correcta.
A continuación explicamos de que manera se tiene que hacer una substitución de tal tipo. Que las derivaciones permanecen correctas es una tarea que se le deja al lector. Todas las expresiones de la forma $\xi(v)$ donde v es cualquier término se substituyen por $F(v)$, así mismo, las sucesiones de fórmulas Γ y Δ se agregan mediante diluciones a los IT-Secuentes superiores, y serán llevadas por toda la derivación hasta que aparezcan en el secuente final de la IT-Derivación que será de la forma $F(0), \Gamma \rightarrow \Delta, F(t)$. Obviamente, la parte del árbol debajo de este secuente permanece exactamente igual. Finalmente, la parte de la derivación que aparecía arriba del secuente superior de la aplicación $INDT$ se agrega arriba de los IT-Secuentes superiores, substituyendo respectivamente la variable libre a por el término que aparece en el secuente.
En este momento el lector ya se habrá dado cuenta del papel que está jugando el símbolo ξ : Nos esta sirviendo como una "variable" para las fórmulas de AP.
Ahora lo que vamos a hacer es demostrar que para cualquier $n \in \mathbb{N}$ hay una IT-Derivación hasta el ordinal ω_n, lo cual implica que si tuviéramos una inferencia $INDT$ de la forma:

$$\frac{a > 0, \forall x[x < a \Rightarrow F(x)], \Gamma \rightarrow \Delta, F(a)}{F(0), \Gamma \rightarrow \Delta, F(\omega_n)}$$

la podríamos eliminar de la manera antes dicha. En otras palabras, la inducción transfinita hasta ω_n sería demostrable. Para ello necesitamos el siguiente
LEMA. El secuente

$$t > 0, \forall x[x < t \Rightarrow \forall \mu[\xi^*(\mu) \Rightarrow \xi^*(\mu + \omega^x)]] \rightarrow \forall \mu[\xi^*(\mu) \Rightarrow \xi^*(\mu + \omega^t)]$$

es derivable.

Dem: Dicho secuente se deriva como sigue: llamemos Q a la segunda fórmula en el antecedente del secuente anterior y utilicemos la siguiente abreviatura: $\xi^*(x)$ abrevia a la fórmula $\forall y[y \leq x \Rightarrow \xi(y)]$, empezamos con la siguiente derivación[3]:

$$\dfrac{s < t, s < t \Rightarrow \forall\mu[\xi^*(\mu) \Rightarrow \xi^*(\mu + \omega^s)] \rightarrow \forall\mu[\xi^*(\mu) \Rightarrow \xi^*(\mu + \omega^s)]}{s < t, \forall x[x < t \Rightarrow \forall\mu[\xi^*(\mu) \Rightarrow \xi^*(\mu + \omega^x)]] \rightarrow \forall\mu[\xi^*(\mu) \Rightarrow \xi^*(\mu + \omega^s)]}\ (UNIV\text{-}I)$$

$$\dfrac{s < t, Q \rightarrow \forall\mu[\xi^*(\mu) \Rightarrow \xi^*(\mu + \omega^s)]}{Q, s < t, \xi^*(\gamma + \omega^s \cdot \alpha) \rightarrow \xi^*(\gamma + \omega^s \cdot \alpha + \omega^s)}\ (RDU)\ (RDI)$$

$$\dfrac{Q, s < t, \xi^*(\gamma + \omega^s \cdot \alpha) \rightarrow \xi^*(\gamma + \omega^s \cdot \alpha + \omega^s)}{Q, s < t, \xi^*(\gamma + \omega^s \cdot \alpha) \rightarrow \xi^*(\gamma + \omega^s \cdot (\alpha + 1))}\ (IG)$$

$$\dfrac{Q, s < t, \xi^*(\gamma + \omega^s \cdot \alpha) \rightarrow \xi^*(\gamma + \omega^s \cdot (\alpha + 1))}{\alpha < \omega, Q, s < t, \xi^*(\gamma + \omega^s \cdot \alpha) \rightarrow \xi^*(\gamma + \omega^s \cdot (\alpha + 1))}\ (DIL\text{-}I)$$

A este último secuente le aplicamos ahora una inducción:

$$\dfrac{\alpha < \omega, Q, s < t, \xi^*(\gamma + \omega^s \cdot \alpha) \rightarrow \xi^*(\gamma + \omega^s \cdot (\alpha + 1))}{t_1 < \omega, Q, , s < t, \xi^*(\gamma + \omega^s \cdot 0) \rightarrow \xi^*(\gamma + \omega^s \cdot t_1)}\ (IND)$$

$$\dfrac{t_1 < \omega, Q, , s < t, \xi^*(\gamma + \omega^s \cdot 0) \rightarrow \xi^*(\gamma + \omega^s \cdot t_1)}{t_1 < \omega, Q, , s < t, \xi^*(\gamma) \rightarrow \xi^*(\gamma + \omega^s \cdot t_1)}\ (IG)$$

$$\dfrac{t_1 < \omega, Q, , s < t, \xi^*(\gamma) \rightarrow \xi^*(\gamma + \omega^s \cdot t_1)}{t_1 < \omega, Q, s < t, \xi^*(\gamma), \beta \leq \gamma + \omega^s \cdot t_1 \rightarrow \xi(\beta)}\ (RDU)\ (RDI)$$

donde en toda esta derivación los términos s y t_1 representan a ordinales con las siguientes propiedades: $s < t$, $t_1 < \omega$ y $\beta \leq \gamma + \omega^s \cdot t_1$. La prueba de que estos ordinales existen es un simple ejercicio de aritmética ordinal.

De lo anterior se sigue que los siguientes secuentes son derivables mediante simples diluciones:

$$\begin{aligned} t &> 0,\ \beta < \gamma + \omega^t \rightarrow \beta \leq \gamma + \omega^s \cdot t_1 \\ t &> 0,\ \beta < \gamma + \omega^t \rightarrow s < t \\ t &> 0,\ \beta < \gamma + \omega^t \rightarrow t_1 < \omega \end{aligned}$$

[3]Con IG denotamos a las aplicaciones de axiomas de igualdad.

A partir de estos secuentes y de la derivación anterior, se obtiene (mediante tres cortes e inferencias estructurales) lo siguiente:

$$\dfrac{\dfrac{t > 0, Q, \xi^*(\gamma), \beta < \gamma + \omega^t \rightarrow \xi(\beta)}{t > 0, Q, \xi^*(\gamma) \rightarrow \beta < \gamma + \omega^t \Rightarrow \xi(\beta)}\ (IMP\text{-}D)}{}$$

$$\dfrac{t > 0, Q, \xi^*(\gamma) \rightarrow \beta < \gamma + \omega^t \Rightarrow \xi(\beta)}{t > 0, Q, \xi^*(\gamma) \rightarrow \forall\mu[\mu < \gamma + \omega^t \Rightarrow \xi(\mu)]}\ (UNIV\text{-}D)$$

si ahora cortamos este último secuente junto con el secuente inferior de

$$\dfrac{\rightarrow \gamma + \omega^t > 0\ \ (TA) \quad \gamma + \omega^t > 0, \forall\mu[\mu < \gamma + \omega^t \Rightarrow \xi(\mu)] \rightarrow \xi(\gamma + \omega^t)\ \ (ITSS)}{\forall\mu[\mu < \gamma + \omega^t \Rightarrow \xi(\mu)] \rightarrow \xi(\gamma + \omega^t)}$$

obtenemos el secuente $t > 0,\ Q,\ \xi^*(\gamma) \rightarrow \xi(\gamma + \omega^t)$ y, más aún,

$$\dfrac{t > 0, Q, \xi^*(\gamma) \rightarrow \xi(\gamma + \omega^t)}{t > 0, Q, \xi^*(\gamma), \delta = \gamma + \omega^t \rightarrow \xi(\delta)}\ (Ig)$$

Por otra parte, a partir del mismo secuente obtenemos mediante RDU, RDI e inferencias estructurales:

$$t > 0, Q, \xi^*(\gamma), \delta < \gamma + \omega^t \rightarrow \xi(\delta)$$

y mediante una inferencia *DISY-I:*

$$\dfrac{t > 0, Q, \xi^*(\gamma), \delta = \gamma + \omega^t \rightarrow \xi(\delta) \quad t > 0, Q, \xi^*(\gamma), \delta < \gamma + \omega^t \rightarrow \xi(\delta)}{t > 0, Q, \xi^*(\gamma), \delta = \gamma + \omega^t\ \vee\ \delta < \gamma + \omega^t \rightarrow \xi(\delta)}$$

Por último tenemos la siguiente derivación. Denotemos con S al secuente inmediato anterior:

$$\dfrac{\delta \leq \gamma + \omega^t \rightarrow \delta = \gamma + \omega^t\ \vee\ \delta < \gamma + \omega^t \quad S}{t > 0, Q, \xi^*(\gamma), \delta \leq \gamma + \omega^t \rightarrow \xi(\delta)}$$

$$\dfrac{t > 0, Q, \xi^*(\gamma), \delta \leq \gamma + \omega^t \rightarrow \xi(\delta)}{t > 0, Q, \xi^*(\gamma) \rightarrow \xi^*(\gamma + \omega^t)}\ (IMP\text{-}D,\ UNIV\text{-}D)$$

$$\dfrac{t > 0, Q, \xi^*(\gamma) \rightarrow \xi^*(\gamma + \omega^t)}{t > 0, Q \rightarrow \forall\mu[\xi^*(\mu) \Rightarrow \xi^*(\mu + \omega^t)]}\ (IMP\text{-}D,\ UNIV\text{-}D)$$

Este último secuente es precisamente el que queríamos derivar.□

Pasemos al resultado principal

PROPOSICIÓN. Para toda $n \in \mathbb{N}$, hay una IT-Derivación hasta el ordinal ω_n

Dem: Por inducción sobre n.

Base de la Inducción ($n = 0$): Este caso es trivial, pues una IT-derivación hasta cero consta simplemente del secuente

$$\xi(0) \rightarrow \xi(0)$$

que obviamente es derivable.

Hipótesis de Inducción: Hay una IT-Derivación hasta ω_n, llamémosla P_n.

Queremos demostrar que existe una IT-derivación hasta ω_{n+1}. Nuestra prueba es totalmente constructiva a partir de la hipótesis de inducción.

Podemos suponer S.P.G. que todas las variables que introducimos en lo que sigue no figuran en P_n, pues disponemos de un número infinito de variables.

Reemplacemos el símbolo ξ en toda la derivación de la siguiente manera: $\xi(\tau)$ se reemplazará por $\forall\mu[\xi^*(\mu) \Rightarrow \xi^*(\mu+\omega^\tau)]$. Dejamos como ejercicio al lector el asegurarse que todos las inferencias, los axiomas lógicos y de igualdad siguen siendo correctos, al igual que los axiomas matemáticos. En cambio, los IT-Secuentes superiores se vuelven secuentes de otro tipo, así como el secuente final. En tales casos la derivación debe ser arreglada como a continuación lo describimos.

Los IT-Secuentes superiores se vuelven de la forma

$$t > 0, \forall x[x < t \Rightarrow \forall\mu[\xi^*(\mu) \Rightarrow \xi^*(\mu + \omega^x)]] \rightarrow \forall\mu[\xi^*(\mu) \Rightarrow \xi^*(\mu + \omega^t)]$$

así que por el lema anterior son substituidos por su derivación completa.

Por último analicemos al secuente final, el cual es ahora de la siguiente forma:

$$\forall\mu[\xi^*(\mu) \Rightarrow \xi^*(\mu + \omega^0)] \rightarrow \forall\mu[\xi^*(\mu) \Rightarrow \xi^*(\mu + \omega^{\omega_n})]$$

Queremos llegar a demostrar el secuente:

$$\xi(0) \rightarrow \xi(\omega_{n+1})$$

para lo cual haremos un injerto a P_n, que construiremos en partes por razones tipográficas y porque creemos que será más clara su comprensión de esta manera.

a) Construcción de una derivación del secuente $\xi(0) \to \xi^*(0)$.

$$\frac{\alpha \leq 0 \to 0 = \alpha \ \ (TA) \qquad 0 = \alpha, \xi(0) \to \xi(\alpha)}{\xi(0), \alpha \leq 0 \to \xi(\alpha)}$$

$$\frac{\xi(0), \alpha \leq 0 \to \xi(\alpha)}{\xi(0) \to \alpha \leq 0 \Rightarrow \xi(\alpha)} \ (\ IMP\text{-}D)$$

$$\frac{\xi(0) \to \alpha \leq 0 \Rightarrow \xi(\alpha)}{\xi(0) \to \xi^*(0)} \ (UNIV\text{-}D) \quad .$$

b) Construcción de una derivación del secuente $\xi^*(\alpha) \to \xi(\alpha + 1)$.

Sea J_1 el siguiente corte:

$$\frac{\to \alpha + 1 > 0 \qquad \alpha + 1 > 0, \forall\eta[\eta < \alpha + 1 \Rightarrow \xi(\eta)] \to \xi(\alpha + 1)}{\forall\eta[\eta < \alpha + 1 \Rightarrow \xi(\eta)] \to \xi(\alpha + 1)}$$

La siguiente es una derivación de $\xi^*(\alpha) \to \xi(\alpha + 1)$:

$$\frac{\beta \leq \alpha \Rightarrow \xi(\beta), \beta \leq \alpha \to \xi(\beta)}{\xi^*(\alpha), \beta \leq \alpha \to \xi(\beta)} \ (UNIV\text{-}I)$$

$$\frac{\beta < \alpha + 1 \to \beta \leq \alpha \ \ (TA) \qquad \xi^*(\alpha), \beta \leq \alpha \to \xi(\beta)}{\xi^*(\alpha), \beta < \alpha + 1 \to \xi(\beta)}$$

$$\frac{\xi^*(\alpha), \beta < \alpha + 1 \to \xi(\beta)}{\xi^*(\alpha) \to \forall\eta[\eta < \alpha + 1 \Rightarrow \xi(\eta)]} \ (IMP\text{-}D)(UNIV\text{-}D) \qquad J_1$$

$$\frac{\xi^*(\alpha) \to \forall\eta[\eta < \alpha + 1 \Rightarrow \xi(\eta)] \quad \forall\eta[\eta < \alpha + 1 \Rightarrow \xi(\eta)] \to \xi(\alpha + 1)}{\xi^*(\alpha) \to \xi(\alpha + 1)}$$

c) Construcción de una derivación del secuente $\xi^*(\alpha) \to \xi^*(\alpha + 1)$ a partir de una derivación del secuente $\xi^*(\alpha) \to \xi(\alpha + 1)$.

A la derivación dada en b) se le injerta la siguiente[4]:

$$\frac{\gamma \leq \alpha \Rightarrow \xi(\gamma), \gamma \leq \alpha \to \xi(\gamma)}{\xi^*(\alpha), \gamma \leq \alpha \to \xi(\gamma)} \ (UNIV\text{-}I) \qquad \frac{\xi^*(\alpha) \to \xi(\alpha + 1)}{\xi^*(\alpha), \alpha + 1 = \gamma \to \xi(\gamma)} \ (EST,\ IG)$$

[4] A veces denotaremos con EST la aplicación de una inferencia estructural, aunque casi nunca lo haremos

$$\dfrac{\gamma \leq \alpha + 1 \rightarrow \gamma \leq \alpha \ \vee \ \alpha + 1 = \gamma \qquad \dfrac{\xi^{*}(\alpha), \gamma \leq \alpha \rightarrow \xi(\gamma) \qquad \xi^{*}(\alpha), \alpha + 1 = \gamma \rightarrow \xi(\gamma)}{\gamma \leq \alpha \ \vee \ \alpha + 1 = \gamma, \xi^{*}(\alpha) \rightarrow \xi(\gamma)}\ (DISY\text{-}I,\ EST)}{\xi^{*}(\alpha), \gamma \leq \alpha + 1 \rightarrow \xi(\gamma)}$$

$$\dfrac{\xi^{*}(\alpha), \gamma \leq \alpha + 1 \rightarrow \xi(\gamma)}{\xi^{*}(\alpha) \rightarrow \xi^{*}(a + 1)}\ (IMP\text{-}D,\ UNIV\text{-}D)$$

d) Construcción de una derivación del secuente $\rightarrow \forall\mu[\xi^{*}(\mu) \Rightarrow \xi^{*}(\mu + \omega^{\omega_n})]$ a partir de una $\mathcal{IT}$-Derivación hasta ω_n y de una derivación del secuente $\xi^{*}(\alpha) \rightarrow \xi^{*}(a + 1)$.
A la derivación dada por c) junto con la $\mathcal{IT}$-Derivación P_n después de aplicársele el proceso de reemplazo se les injerta lo siguiente:

$$\dfrac{\dfrac{\dfrac{\xi^{*}(\alpha) \rightarrow \xi^{*}(a + 1)}{\rightarrow \xi^{*}(\alpha) \Rightarrow \xi^{*}(a + 1)}\ (IMP\text{-}D)}{\rightarrow \forall\mu[\xi^{*}(\mu) \Rightarrow \xi^{*}(\mu + 1)]}\ (UNIV\text{-}D) \qquad \forall\mu[\xi^{*}(\mu) \Rightarrow \xi^{*}(\mu + 1)] \rightarrow \forall\mu[\xi^{*}(\mu) \Rightarrow \xi^{*}(\mu + \omega^{\omega_n})]}{\rightarrow \forall\mu[\xi^{*}(\mu) \Rightarrow \xi^{*}(\mu + \omega^{\omega_n})]}$$

e) Construcción de una derivación del secuente $\xi(0) \rightarrow \xi^{*}(\omega_{n+1})$ a partir de una derivación de $\rightarrow \forall\mu[\xi^{*}(\mu) \Rightarrow \xi^{*}(\mu + \omega^{\omega_n})]$ y de una derivación de $\xi(0) \rightarrow \xi^{*}(0)$.
A las derivaciones dadas en a) y en d) se les agrega lo siguiente:

$$\dfrac{\xi(0) \rightarrow \xi^{*}(0) \qquad \dfrac{\dfrac{\dfrac{\rightarrow \forall\mu[\xi^{*}(\mu) \Rightarrow \xi^{*}(\mu + \omega^{\omega_n})]}{\rightarrow \xi^{*}(0) \Rightarrow \xi^{*}(0 + \omega^{\omega_n})}\ (RDU)}{\xi^{*}(0) \rightarrow \xi^{*}(0 + \omega^{\omega_n})}\ (RD)}{\xi^{*}(0) \rightarrow \xi^{*}(\omega_{n+1})}\ (IG)}{\xi(0) \rightarrow \xi^{*}(\omega_{n+1})}$$

Por último construiremos una derivación de $\xi(0) \rightarrow \xi(\omega_{n+1})$.

f) Construcción de una derivación del secuente $\xi(0) \rightarrow \xi(\omega_{n+1})$ a partir de una derivación de $\xi(0) \rightarrow \xi^{*}(\omega_{n+1})$.

A la derivación en e) se le agrega lo siguiente:

$$\dfrac{\rightarrow \omega_{n+1} \leq \omega_{n+1} \quad (TA) \qquad \dfrac{\dfrac{\dfrac{\xi(0) \rightarrow \xi^{*}(\omega_{n+1})}{\xi(0) \rightarrow \omega_{n+1} \leq \omega_{n+1} \Rightarrow \xi(\omega_{n+1})}\,(RDU)}{\xi(0), \omega_{n+1} \leq \omega_{n+1} \rightarrow \xi(\omega_{n+1})}\,(RDI)}{\xi(0), \omega_{n+1} \leq \omega_{n+1} \rightarrow \xi(\omega_{n+1})}}{\xi(0) \rightarrow \xi(\omega_{n+1})}$$

Con esto terminamos nuestra demostración.□

Ahora pasamos a la sección principal de este capítulo, donde trataremos con pruebas de no demostrabilidad.

3.4 Pruebas de No Demostrabilidad.

En esta sección probaremos que la inducción transfinita hasta ε_0 no es demostrable en AP. El procedimiento que seguiremos será análogo al del lema fundamental del capítulo dos (lo cual no es de extrañarse) pues en ambos casos estamos tratando con pruebas de no demostrabilidad. En este caso también tenemos el lema fundamental, del cual se sigue la no demostrabilidad con base en la inducción transfinita, por lo que no sera formalizable en AP.

Empezamos con varias definiciones, algunas nuevas y otras ya conocidas, pero con algunas modificaciones.

DEFINICIÓN. Conservamos el concepto de IT-Derivación dado en la sección anterior con la siguiente modificación: El secuente final es de la forma

$$\xi(0) \rightarrow \xi(s_1), \xi(s_2), ..., \xi(s_n)$$

donde s_i es un término que representa a un ordinal. Definimos el número terminal de la IT-derivación P como:

$$nt(P) = \min\{s_1, ..., s_n\}$$

DEFINICIÓN. Sea P una IT-Derivación. Extendemos la definición de la función de asignación de ordinales $o_P : SEC(P) \rightarrow ORD$, con la siguiente cláusula:

Si S es un IT-Secuente Superior, entonces $o_P(S) = 7$.

DEFINICIÓN. Sea P una IT-Derivación. Decimos que P es no-crítica syss al aplicarle el metodo de reducción para AP (pasos $2, 3$ o 5)[5], se obtiene una derivación con ordinal menor. En otro caso decimos que P es crítica.

3.4.1 Método de Reducción para IT-Derivaciones

Ya tenemos asignados ordinales a todas las IT-Derivaciones. Lo que haremos ahora es definir una reducción para IT-Derivaciones no triviales, es decir, para aquellas cuyo número terminal no es cero, siguiendo la demostración del lema fundamental del capítulo dos. Aunque si una IT-Derivación es crítica necesitaremos algo más. La reducción esta definida de tal manera que toda IT-Derivación no-crítica con número terminal diferente de cero se reduce a una derivación con el mismo número terminal. En cambio, cuando es crítica se reduce a una derivación con menor número terminal y, por lo tanto, en cualquier reducción el ordinal decrece.

Empecemos pues a describir el método de reducción:

Sea Q una IT-Derivación. Aplicamos a Q los pasos de reducción 1 a 4 de la demostración del lema fundamental para AP , obteniendo una IT-Derivación P con las siguientes propiedades:

P1) El segmento final de P no tiene variables libres.

P2) El segmento final de P no contiene inducciones.

P3) El segmento final de P no contiene axiomas lógicos.

P4) Si en el segmento final de P figura una dilución I entonces cualquier inferencia bajo I es una dilución.

Si P es una prueba que cumple estas 4 propiedades diremos que P es una prueba previamente reducida.

Necesitamos hacer un par de observaciones antes de continuar. Estas se refieren a la manera

[5] Nótese que es posible que el paso 5 no se le pueda aplicar a una IT-Derivación, pues el secuente final no es vacío.

de eliminar inducciones y la justificación de la propiedad 4. El procedimiento para eliminar inducciones requiere de dos modificaciones, puesto que ahora en nuestra inferencia aparece la fórmula $t < \omega$. Esto se arregla de la siguiente manera, considerando dos casos:

I) Si $t < \omega$ resulta falso, entonces el secuente $t < \omega \rightarrow$ es demostrable, y la inducción es substituida por:

$$\frac{t < \omega \rightarrow}{t < \omega, F(0), \Gamma \rightarrow \Delta, F(t)} \ (DIL)$$

en este caso es claro que el ordinal disminuye pues las diluciones no afectan al ordinal.

II) Si $t < \omega$ es cierto, entonces el proceso es análogo al del segundo paso de reducción, sólo que ahora $P_0(\bar{n})$ es una derivación del secuente $n < \omega, F(\bar{n}), \Gamma \rightarrow \Delta, F(\overline{n+1})$, de manera que el secuente $F(\bar{n}), \Gamma \rightarrow \Delta, F(\overline{n+1})$ se obtiene agregando el siguiente corte:

$$\frac{\rightarrow \bar{n} < \omega \quad \bar{n} < \omega, F(\bar{n}), \Gamma \rightarrow \Delta, F(\overline{n+1})}{F(\bar{n}), \Gamma \rightarrow \Delta, F(\overline{n+1})}$$

y el secuente inferior de la inducción eliminada se obtiene mediante una dilución:

$$\frac{F(0), \Gamma \rightarrow \Delta, F(t)}{t < \omega, F(0), \Gamma \rightarrow \Delta, F(t)}$$

En este caso no sabemos si el ordinal disminuye por culpa de los secuentes $\rightarrow \bar{n} < \omega$.

Ahora analicemos por qué es válida la propiedad 4. Supongamos que se ha aplicado exhaustivamente el cuarto paso de reducción, de modo que ahora en la derivación ya no hay diluciones. Como esta vez el secuente final es no-vacío, la única manera de restaurar el secuente final original es agregando diluciones al final de la prueba reducida. Resulta claro que las únicas diluciones que figuran en la derivación están juntas.

Continuamos con el método de reducción probando algunos resultados, comenzando con la siguiente

PROPOSICIÓN. Si P es una IT-Derivación previamente reducida, entonces en P figura al menos una inferencia lógica, la cual es implícita, o un IT-Secuente Superior.

<u>Dem</u>: (Reducción al absurdo). Supongamos que P no contiene ni una inferencia lógica ni un IT-Secuente superior. En tal caso su secuente final $\xi(0) \rightarrow \xi(s_1), ..., \xi(s_k)$ se habría derivado a partir de axiomas matemáticos, sin el uso de conectivos lógicos ni variables (pues nuestra

prueba es previamente reducida), por lo que podríamos reemplazar la fórmula $\xi(t)$ por $t = 0$ obteniendo una derivación correcta del secuente $0 = 0 \rightarrow s_1 = 0, ..., s_k = 0$. No obstante, lo anterior contradice el hecho de que ninguna de las s_k es cero.□

De esta proposición se desprende inmediatamente que segfin(P) contiene una fórmula principal en la frontera o en un IT-Secuente Superior, lo que justifica la siguiente

DEFINICIÓN. Una fórmula A en el segmento final de una derivación P es un *descendiente principal* (*IT-descendiente principal*), (abreviado dp (IT-dp)) syss A es descendiente de una fórmula principal que esta en ∂P (en un IT-secuente superior que pertenezca a segfin(P)).

Obsérvese que un IT-descendiente en el segmento final de una derivación siempre figura en el consecuente de un secuente y es de la forma $\xi(t)$.

A continuación damos una condición suficiente para la existencia de descendientes principales.

PROPOSICIÓN. Sea P una IT-derivación previamente reducida y sea S un secuente en segfin(P). Si en S figura una fórmula B tal que $grd(B) > 0$, entonces existe una fórmula A en S o en algún secuente arriba de S tal que A es un descendiente o IT-descendiente principal.

Dem: Sea S como se pide. En tal caso, por P4 y porque el secuente final no contiene símbolos lógicos, S figura arriba de la más alta dilución en segfin (P). La propiedad "tener un símbolo lógico" se preserva hacia arriba hasta uno de los secuentes superiores de cada inferencia en segfin(P) (pero no necesariamente más allá de una inferencia frontera) o hasta un IT-secuente superior, al seguir las ramas a las que S pertenece. En algunos casos tenemos que $B = A$, pero no siempre, pues B podría ser descendiente de una fórmula "pasiva" en la frontera, i.e. una fórmula que preserva símbolos lógicos más allá de ∂P.□

La siguiente proposición es primordial, pues sirve como base del método de reducción cuando la derivación es crítica.

PROPOSICIÓN. Si P es una IT-derivación previamente reducida en la que no figura un corte adecuado, entonces el secuente final de P contiene un IT-descendiente principal.

Dem: Puesto que el secuente final de P no tiene símbolos lógicos, los conceptos descendiente e IT-descendiente principal coinciden en este caso.

La prueba es reducción al absurdo. Supongamos que el secuente final de P no contiene una fórmula tal. Puesto que segfin (P) contiene un descendiente o IT-descendiente principal (por la primera proposición de esta sección), tal fórmula debe desaparecer mediante un corte, por lo que tiene sentido hablar de la siguiente propiedad de cortes de segfin(P):

(Pr): Un corte de segfin(P) tiene la propiedad (Pr) syss al menos uno de sus secuentes superiores tiene un descendiente o IT-descendiente principal pero su secuente inferior ya no contiene una fórmula de tal tipo.

Sea pues I un corte maximal que cumple Pr. digamos

$$I : \frac{\Gamma \to \Delta, D \quad D, \Pi \to \Lambda}{\Gamma, \Pi \to \Delta, \Lambda}$$

y sean S_1, S_2 los secuentes superiores de I. Como I cumple Pr tenemos que una de las fórmulas de corte es un dp o un IT-dp. Analicemos primero el caso en que la D en S_1 cumple tal propiedad:

Si $grd(D) > 0$ entonces D es un dp., de manera que S_2 contiene una fórmula con un símbolo lógico (a saber D), por lo tanto por la proposición anterior en S_2 o en un secuente arriba de S_2 figura una fórmula A que es dp. o IT-dp., de donde se derivan dos subcasos:

i) A no figura en S_2.

Como A no figura en S_2, debió desaparecer mediante un corte, en cuyo caso el corte tendría la propiedad Pr, contradiciendo la maximalidad de I.

ii) A figura en S_2.

En este caso A debe ser la misma D, lo que contradice el hecho de que P no contiene un corte adecuado.

Por lo tanto $grd(D) = 0$ y D es de la forma $\xi(t)$.

Supongamos ahora que en S_2 figura un símbolo lógico. En tal caso tenemos que arriba de S_2 figura un dp. o un IT-dp., ya que si estuviera en S_2 no podría ser D y, por lo tanto tendría que figurar en el secuente inferior de I, contradiciendo el hecho de que I cumple Pr. No obstante, si está arriba de S_2 entonces I no es maximal. Concluimos que en S_2 no puede haber símbolos lógicos.

Puesto que I es un corte maximal que cumple Pr, ninguna inferencia frontera ni IT-secuente superior en segfin(P) figura arriba de S_2. Por lo tanto en el segmento de P que va desde S_2 hasta el secuente final está incluido en segfin(P), en el no figuran ni axiomas lógicos (pues P

es previamente reducida) ni IT-secuentes superiores, por lo que es imposible que $\xi(t)$ figure en S_2. Concluimos que D tampoco puede ser $\xi(t)$.
De todo lo anterior concluimos que la D en S_1 no puede ser un descendiente o IT-descendiente principal.
Supongamos ahora que la D en S_2 es un dp. o un IT-dp. Como ya vimos, D no puede ser un IT-dp., así que $grd(D) > 0$ y por lo tanto hay un dp. o IT-dp. en S_1 o arriba de S_1. En ambos casos llegamos a una contradicción, de manera análoga a la que usamos arriba.
En Conclusión: No puede existir un corte con la propiedad Pr, así que en el secuente final de P figura un descendiente principal.$\square$

Resumamos ahora lo que hemos hecho hasta aquí: Sea P una IT-Derivación.
Si P es no-crítica entonces ya la podemos reducir a una IT-Derivación P' con $o(P') < o(P)$ y $nt(P') = nt(P)$, pues lo único que tenemos que hacer es aplicar el método del capítulo 2. Por lo tanto, ahora tenemos que tratar con el caso en el que P es una prueba crítica. Para esto definimos lo que es una reducción crítica.

3.4.2 Reducción Crítica

Sea P una IT-derivación crítica previamente reducida. La proposición anterior garantiza que en P figura un corte adecuado. Por una reducción critica de P entenderemos a una prueba P' construida a partir de P como sigue: Tenemos que el secuente final de P contiene un IT-descendiente principal, digamos $\xi(s_i)$ descendiente de $\xi(t)$ (donde el término cerrado t denota al número s_i).
Sea s un ordinal tal que $s < nt(P)$, de modo que $s < t$, y consideremos la siguiente derivación Q:

$$\cfrac{\cfrac{\cfrac{\rightarrow s < t \quad \xi(s) \rightarrow \xi(s)}{s < t \Rightarrow \xi(s) \rightarrow \xi(s)}\ (IMP\text{-}I)}{\forall x[x < t \Rightarrow \xi(x)] \rightarrow \xi(s)}\ (UNIV\text{-}I)}{\forall x[x < t \Rightarrow \xi(x)] \rightarrow \xi(s), \xi(t)}\ (DIL)$$

el ordinal de esta derivación es $o(Q) = 3 < 7 = o_P(\forall x[x < t \Rightarrow \xi(x)] \rightarrow \xi(t))$. Al substituir en P el IT-Secuente superior $\forall x[x < t \Rightarrow \xi(x)] \rightarrow \xi(t)$ con la derivación Q, y agregando la fórmula $\xi(s)$ en toda la derivación (aplicando quizás algunos intercambios) obtenemos una derivación P' con secuente final

$$\xi(0) \rightarrow \xi(s), \xi(s_1), ..., \xi(s_k)$$

Por último es obvio que:

$$o(P') < o(P) \text{ y } nt(P') = s < nt(P)$$

De esta manera termina la construcción de una reducción crítica de P.

Así que ahora, que podemos reducir cualquier IT-derivación a otra con menor ordinal, estamos a punto de concluir la no-demostrabilidad de $IT(\varepsilon_0)$, que será nuevamente consecuencia de un lema fundamental.

3.4.3 El Lema Fundamental para IT-Derivaciones

Hasta este momento todo nuestro formalismo ha podido ser encajado dentro de AP. No obstante, para probar el lema fundamental, necesitamos efectuar una inducción transfinita hasta ε_0, así que jamás podrá ser formalizada en AP.

LEMA FUNDAMENTAL. Para cualquier IT-derivación P se cumple que:

$$nt(P) \leq o(P)$$

<u>Dem</u>: (Inducción **<u>Transfinita</u>** sobre $o(P)$)

Sea P una IT-derivación con $o(P) = \mu$ y $nt(P) = \sigma$. Usemos inducción transfinita fuerte. Hipótesis de Inducción: Para cualquier IT-derivación Q con $o(Q) < \mu$, se cumple que:

$$nt(Q) \leq o(Q)$$

Debemos considerar dos casos:

I) P es no-crítica.

En este caso aplicando el método de reducción obtenemos una IT-derivación P' con las siguientes propiedades:

$$o(P') < \mu \ \ y \ \ nt(P') = \sigma$$

de donde, usando la hipótesis de inducción, concluimos que:

$$\sigma \underset{H.I.}{\leq} o(P') < \mu$$

II) P es crítica.

En este caso procedemos por reducción al absurdo. Supongamos que $\sigma > \mu$. En tal caso podemos aplicar una reducción crítica a P con lo que obtenemos una IT-derivación P' tal que:

$$nt(P') = \mu < \sigma \ \ y \ \ o(P') < o(P) = \mu$$

y esto implica que

$$o(P') < \mu = nt(P')$$

lo cual contradice a la hipótesis de inducción. En cualquier caso concluimos

$$nt(P) \leq o(P).$$

Con esto damos por terminada esta sección y pasamos a la parte central del capítulo, la prueba directa de no demostrabilidad.

3.5 Prueba Directa

Lo primero que haremos en esta sección es demostrar que la inducción transfinita hasta cualquier ordinal menor que ε_0 es demostrable en AP, probando que los secuentes $IT(\omega_n)$ son derivables para cualquier $n \in \mathbb{N}$. Esto es suficiente para asegurar que $IT(\mu)$ es demostrable para cualquier $\mu \in ORD$, puesto que cualquier ordinal menor que ε_0 es menor que algún ω_n, y si bien solamente probamos la existencia de IT-derivaciones para los números ω_n, podemos, a partir de una derivación de este tipo, construir otra con número terminal menor que el original simplemente reemplazando $\xi(x)$ por $\xi^*(x)$ en toda la derivación y modificando de manera adecuada el secuente final y los IT-secuentes superiores. Formalicemos esto en la siguiente

PROPOSICIÓN. Para cualquier $n \in \mathbb{N}$, la inducción transfinita hasta el ordinal ω_n es demostrable en AP, es decir, para cualquier fórmula A de AP y cualquier $n \in \mathbb{N}$, el secuente

$$\forall\alpha[\forall\beta[\beta < \alpha \Rightarrow A(\beta)] \Rightarrow A(\alpha)] \rightarrow \forall\alpha[\alpha \leq \omega_n \Rightarrow A(\alpha)]$$

es demostrable en AP.

<u>Dem</u>: (Inducción para Naturales sobre n)
Basta ver que en $AP(\xi)$ el secuente

$$\forall\alpha[\forall\beta[\beta < \alpha \Rightarrow \xi(\beta)] \Rightarrow \xi(\alpha)] \rightarrow \forall\alpha[\alpha \leq \omega_n \Rightarrow \xi(\alpha)] \qquad (*)$$

es demostrable para cualquier $n \in \mathbb{N}$.
$n = 1$) Cierto, pues en AP vale la inducción matemática.
Hipótesis de inducción: Supongamos que el secuente $(*)$ es demostrable para ω_n.
P.D. $(*)$ es valido para ω_{n+1}
Llamemos φ a la fórmula en el antecedente de $(*)$ y $\psi(\alpha)$ a la fórmula $\forall\gamma[\xi^*(\gamma) \Rightarrow \xi^*(\gamma + \omega^\alpha)]$, probaremos varias cosas:
1) Mediante un argumento parecido a la parte a) de la prueba de existencia de IT-derivaciones, se tiene que el secuente

$$\varphi \rightarrow \xi^*(0)$$

es demostrable.
2) Para cualquier ordinal α, el secuente

$$\forall\gamma[\gamma < \alpha \Rightarrow \psi(\gamma)] \rightarrow \psi(\alpha)$$

es demostrable (cfr. lema de la sección 3.3).
3) Por hipótesis de inducción, tenemos una derivación de $\varphi \rightarrow \xi^*(\omega_n)$ a partir de la cual obtenemos, usando las partes d) y e) de la demostración de la existencia de IT-derivaciones (sección 3.3), primero una derivación de $\rightarrow \psi(\omega_n)$ y segundo una prueba del secuente

$$\xi^*(0) \rightarrow \xi^*(\omega_{n+1})$$

Por lo que mediante el siguiente corte y usando la parte 1)

$$\frac{\varphi \rightarrow \xi^{*}(0) \quad \xi^{*}(0) \rightarrow \xi^{*}(\omega_{n+1})}{\varphi \rightarrow \xi^{*}(\omega_{n+1})}$$

De donde resulta que el secuente (*) es demostrable para ω_{n+1}.

Conclusión: $IT(\omega_n)$ es demostrable para cualquier $n \in \mathbb{N}$.□

Hemos llegado a la culminación del capítulo y de todo el trabajo. Si bien en la sección 3.1 hemos probado que la inducción transfinita hasta ε_0 no es demostrable en AP, ahora daremos una prueba directa, para lo cual utilizaremos el lema fundamental para IT-derivaciones.

PROPOSICIÓN. La inducción transfinita hasta ε_0 no es demostrable en AP.

Dem: (Reducción al Absurdo) supongamos lo contrario. En tal caso el secuente

$$\forall\alpha[\forall\beta[\beta < \alpha \Rightarrow \xi(\beta)] \Rightarrow \xi(\alpha)] \rightarrow \forall\alpha[\alpha \leq \varepsilon_0 \Rightarrow \xi(\alpha)]$$

es demostrable en $AP(\xi)$ (ver la observación al final de esta demostración), por lo tanto mediante el uso de RDU, RDI y un corte obtenemos el secuente

$$\forall\alpha[\forall\beta[\beta < \alpha \Rightarrow \xi(\beta)] \Rightarrow \xi(\alpha)] \rightarrow \xi(\varepsilon_0)$$

A partir de la derivación de este secuente construimos la siguiente prueba P :

$$\dfrac{\dfrac{\dfrac{\forall\beta[\beta < \gamma \Rightarrow \xi(\beta)] \rightarrow \xi(\gamma)}{\rightarrow \forall\beta[\beta < \gamma \Rightarrow \xi(\beta)] \Rightarrow \xi(\gamma)}\,(IMP\text{-}D)}{\rightarrow \forall\alpha[\forall\beta[\beta < \alpha \Rightarrow \xi(\beta)] \Rightarrow \xi(\alpha)]}\,(UNIV\text{-}D) \quad \forall\alpha[\forall\beta[\beta < \alpha \Rightarrow \xi(\beta)] \Rightarrow \xi(\alpha)] \rightarrow \xi(\varepsilon_0)}{\rightarrow \xi(\varepsilon_0)}$$

De esta forma, hemos construido una IT-derivación P con número terminal $nt(P) = \varepsilon_0$. Esto implica que

$$o(P) < \varepsilon_0 = nt(P)$$

lo cual es una contradicción directa al lema fundamental para IT-derivaciones. Por lo tanto

$IT(\varepsilon_0)$ es no demostrable en AP.$\square$

OBSERVACIÓN IMPORTANTE: El lector seguramente ya se habrá preguntado como es qué estamos haciendo uso del número ε_0 , si el sistema $AP(\xi)$ solo contempla a los ordinales estrictamente menores que él. Según esto, en $AP(\xi)$, el secuente $IT(\varepsilon_0)$ ni siquiera podría ser formulado. Lo que sucede es que nuestro teorema, bien interpretado significa: Si $IT(\varepsilon_0)$ pudiera ser formulado en $AP(\xi)$ entonces sería indemostrable en $AP(\xi)$.

Pese a todo, este detalle no tiene ninguna importancia, pues podríamos haber aceptado desde un principio al ordinal ε_0 como parte de nuestro dominio numérico, ya que todas las derivaciones que hemos desarrollado son completamente independientes de él. De hecho podemos agregar un número cualquiera de ordinales al dominio numérico, siempre y cuando se den expresiones precisas (términos) para designarlos y que todas las funciones y predicados continúen siendo decidibles, (para que los axiomas permanezcan validos en este sentido de decidibilidad).

A partir de esta aclaración concluimos que si la inducción transfinita en este dominio restringido es no demostrable, de acuerdo a nuestros resultados, no podrá ser demostrable mediante una extensión consistente del dominio numérico. Es en este sentido en el que debe entenderse el teorema anterior.

Bibliografía

[End1] Enderton H.B. Elements of Set Theory. Academic Press. 1977.

[End2] Enderton H.B. Una Introducción Matemática a la Lógica. UNAM 1987.

[Gen1] Gentzen G. Die Widerspruchsfreiheit der reinen Zahlentheorie. Traducción al ingles en [Sza]

[Gen2] Gentzen G. Neue Fassung des Widerspruchsfreiheitsbeweises für die reine Zahlentheorie. Traducción al ingles en [Sza]

[Gen3] Gentzen G. Beweisbarkeit und Unbeweisbarkeit von Anfangsfällen der transfiniten Induktion in der reinen Zahlentheorie. Traducción al ingles en [Sza]

[Hrb] Hrbacek J. & Jech T. Introduction to Set Theory. Marcel Dekker 1984.

[Kle] Kleeen S. Introducción a la Metamatemática. Editorial Tecnos 1974.

[Men] Mendelson Elliot. Introduction to Mathematical Logic. 3a. Edición. Wadsworth & Brooks 1987

[Ro] Rojas D. La Naturaleza de la Matemática en Gödel y su relación con los Teoremas Limitativos. Tesis de Licenciatura, Facultad de Ciencias UNAM. Abril 1997.

[Ru] Ruiz F. Acerca de una Extensión Gödeliana del Punto de Vista Finitista y de la Consistencia de la Aritmética. Tesis de Licenciatura, Facultad de Ciencias UNAM 1997 (Por aparecer).

[Sch] Schütte Kurt. Proof Theory. Springer Verlag 1977.

[Sza] Szabo M.E. The Collected Papers of Gerhard Gentzen, Studies in Logic and The Foundations of Mathematics, North Holland 1969.

[Tak] Takeuti G. Proof Theory, Studies in Logic and The Foundations of Mathematics Vol. 81, North Holland 1987.

[To1] Torres A. Carlos, La Filosofía y el Programa de Hilbert. En Mathesis Vol. V, No. 1, Departamento de Matemáticas Facultad de Ciencias UNAM 1989

[To2] Torres A. Carlos, Los Teoremas de Gödel, Tesis de Maestria, Facultad de Ciencias UNAM, 1989.

[To3] Torres A. Carlos, El Segundo Problema de Hilbert, Conferencia presentada en el XXVII congreso nacional de la Sociedad Matemática Mexicana, Queretaro, Qro. 1994. Sin publicar.