El Teorema de Goodstein

Araceli Muñoz Sánchez

Trabajo de fin de grado
Grado en Matemáticas
Curso 2020/2021

Tutor: Francisco Félix Lara Martín

Facultad de Matemáticas

Departamento de Ciencias de la Computación e Inteligencia Artificial

Resumen.

Este trabajo se centra en el Teorema de Goodstein. El primer objetivo será demostrarlo. Para ello, debemos introducir al lector en la Teoría de Conjuntos. Explicaremos sus elementos principales y los axiomas sobre los que se desarrolla. Una vez puestas estas bases, desarrollaremos a partir de ellas la estructura de los números ordinales. Esto será suficiente para poder elaborar una prueba del Teorema de Goodstein.

Una vez probado desde la Teoría de Conjuntos, nos planteamos un nuevo objetivo: expresar el Teorema dentro de otra teoría, la Aritmética de Peano (PA). Para ello, se explicará en qué consiste la teoría PA y se estudiarán las funciones Σ_1-definibles y las funciones demostrablemente totales en PA. Sin embargo, aunque veremos que el Teorema de Goodstein puede ser expresado en PA en términos de una función de este tipo, probaremos que en PA este teorema no tiene demostración. Para este fin será imprescindible la introducción de conceptos como las sucesiones de funciones G_α y H_α (sucesión de Hardy) y los teoremas de Wainer y Cichon.

Por último, para evidenciar el papel tan importante que tiene el concepto de infinito en la demostración del Teorema de Goodstein, veremos que PA y una teoría de conjuntos finitos son *esencialmente equivalentes* como teorías. Para ver esto, definiremos las interpretaciones entre teorías, veremos qué tiene que ocurrir para que dos teorías sean esencialmente equivalentes, concretaremos cuál es exactamente esta teoría de conjuntos finitos y presentaremos la interpretación de Ackermann y su inversa.

Abstract.

The main subject of this work is Goodstein's Theorem and our first objective will be proving it. To this end, we will present Set Theory to the reader. We will explain its key elements and its axioms. Once we have set this basis, we will develop the ordinal numbers. This will be enough to make the proof of Goodstein's Theorem.

After making the proof from Set Theory, we come up with a new objective: expressing the Theorem in a different theory, Peano Arithmetic (PA). To this aim, we will explain PA and we will study Σ_1-definable functions and provable total functions in PA. Nevertheless, although we will be able to express Goodstein's Theorem in PA in terms of these types of functions, we will prove that this theorem has no proof in PA. To this end it will be crucial to present the sequences of functions G_α and H_α (Hardy's sequence) and Cichons's and Wainer's theorems.

Finally, we will reveal how important is the infinite concept in the proof of Goodstein's Theorem by showing that PA and a finite set theory are *definitionally equivalent*. So, we will define interpretations between theories, we will see the exact definition of definitionally equivalent, we will specify which is that finite set theory and we will present Ackermann's interpretation and its inverse.

Índice general

Introducción.

En 1944 el matemático inglés Reuben Louis Goodstein demostraba un resultado que será el tema principal de este trabajo. Para explicar (informalmente) de qué se trata dicho resultado, vamos a ver antes unas nociones necesarias.

La representación de un número natural g en base p es una suma de potencias de p (con exponentes menores que g) y coeficientes menores que la base p. Por ejemplo, la representación de 59057 en base 3 quedaría de la siguiente manera:

$$59057 = 2 \cdot 3^0 + 2 \cdot 3^1 + 3^{10} = 2 + 2 \cdot 3 + 3^{10}.$$

Si ahora representamos todos los exponentes también en base 3, los exponentes de esos exponentes también en base 3 y así sucesivamente hasta que nos quedáramos con exponentes menores o iguales que 3 nos quedaría algo de esta forma:

$$59057 = 2 + 2 \cdot 3 + 3^{3^2+1}.$$

A esto lo llamamos la representación de 59057 en base *pura* 3.

A cualquier g representado en base pura p podemos aplicarle un *salto de base*, es decir, en la representación cambiamos todas las apariciones de p por $p + 1$. Si hacemos un salto de base en el ejemplo anterior obtendríamos algo así:

$$2 + 2 \cdot 4 + 4^{4^2+1} = 17179869194.$$

Pues bien, la *sucesión de Goodstein* en base p empezando por g comienza con la representación de g en base pura p y cada nuevo término se calcula realizando un salto de base al término anterior y restando 1. La sucesión de Goodstein en base 3 empezando por 59057 tendría como primer término a

$$59057 = 2 + 2 \cdot 3 + 3^{3^2+1}.$$

El segundo término sería:

$$2 + 2 \cdot 4 + 4^{4^2+1} - 1 = 1 + 2 \cdot 4 + 4^{4^2+1} = 17179869193.$$

Como tercer término tendríamos a:

$$1 + 2 \cdot 5 + 5^{5^2+1} - 1 = 2 \cdot 5 + 5^{5^2+1},$$

que es un número de 19 cifras. El cuarto término sería:

$$2 \cdot 6 + 6^{6^2+1} - 1 = 5 + 6 + 6^{6^2+1},$$

un número de 29 cifras.

Observamos que las sucesiones de Goodstein crecen bastante rápido. Sin embargo, Goodstein demostró que todas las sucesiones de este tipo comienzan a decrecer en algún momento hasta llegar a 0. Lo curioso de este resultado, además de que parece ir en contra de la intuición es que, a pesar de definirse dentro del conjunto de los números naturales, necesita de conjuntos infinitos para poder probarse. Es decir, aunque en la sucesión sólo intervengan números naturales, es necesario "salirse"de $\mathbb{N}$ para demostrar el Teorema de Goodstein.

Veremos que con "salirnos"de $\mathbb{N}$ nos referimos al uso de los ordinales transfinitos. Aquí entra en juego la Teoría de Conjuntos, que introduciremos en el Capítulo 1. Detallaremos los axiomas sobre los que está fundamentada, tanto los lógicos como los no lógicos. También puntualizaremos que, en realidad, no sólo existe una única teoría de conjuntos. Las diferentes teorías existentes se diferencian en los axiomas que utilizan. Normalmente, la inclusión de un mayor número de axiomas dará como resultado teorías más potentes. En concreto, en este trabajo prestaremos especial atención al *Axioma del Infinito*, que es el que permite la existencia de conjuntos infinitos.

Dentro de la Teoría de Conjuntos se pueden construir las estructuras y objetos matemáticos más importantes utilizando solamente conjuntos. En el Capítulo 2 construiremos una de ellas. Pensemos en los números naturales. Como estamos en la Teoría de Conjuntos, cada número natural se define como un conjunto concreto. Pero, gracias al Axioma del Infinito, existen conjuntos infinitos dentro de nuestra teoría. Es decir, el "infinito" es un objeto que existe y que podemos manejar. Por tanto, ¿por qué no "extender" los números naturales más allá? ¿Y si definiéramos el "infinito" como un número? ¿Y el "infinito"+1, "infinito"+2, ..., etc.? Pues bien, de esto tratan los números ordinales. Los definiremos, veremos muchas de sus propiedades y definiremos también los números naturales como parte de los ordinales. Ayudándonos de los ordinales transfinitos o infinitos expondremos una prueba del Teorema de Goodstein en el Capítulo 5. La haremos como en [1], que es una reformulación de la que hizo Cichon en [3].

En el Capítulo 3 veremos la Aritmética de Peano (PA), una teoría dedicada a la investigación de los números naturales. Presentaremos sus axiomas y probaremos dentro de la teoría algunas propiedades básicas de los números naturales. En el Capítulo 4 estudiaremos varios tipos de funciones definidas sobre los naturales (funciones Σ_1-definibles, funciones demostrablemente totales en PA y funciones recursivas) que son expresables mediante una fórmula del lenguaje de PA cumpliendo ciertas propiedades. Veremos, de vuelta en el Capítulo 5, que la sucesión de Goodstein puede definirse a partir de funciones de este tipo, por lo que será expresable dentro de PA y estará bien definida. Sin embargo, como demostraron Kirby y Paris en 1982, el Teorema de Goodstein no es un teorema de PA. Es

decir, este teorema es independiente de PA. Esto lo probaremos como se hace en [1], que es diferente de cómo lo hicieron Kirby y Paris.

Antes de elaborar la prueba de la independencia, introduciremos dos sucesiones de funciones que nos serán necesarias: G_α y H_α (la sucesión de Hardy). Probaremos también el Teorema de Cichon y enunciaremos el Teorema de Wainer, además de otros resultados de carácter más técnico. Durante esta parte del trabajo, PA y la Teoría de Conjuntos irán de la mano para probar la independencia.

Como acabamos de explicar, los conjuntos infinitos son necesarios en nuestra prueba del Teorema de Goodstein y, en la teoría de números naturales PA el Teorema de Goodstein no puede probarse a pesar de definirse dentro de ellos. Por tanto, queremos resaltar la importancia del Axioma del Infinito para probar este teorema. Para ello, lo último que haremos en el trabajo será definir una teoría de conjuntos en la que no existan los conjuntos infinitos y probar que es esencialmente equivalente a PA.

Veremos entonces en el Capítulo 6 las interpretaciones entre teorías. Las interpretaciones transforman de una manera consistente las fórmulas de una teoría en fórmulas de otra teoría diferente. Es como si nos cambiáramos las gafas con las que miramos los objetos. Definiremos la interpretación de Ackermann de $\mathsf{ZF_{fin}}^*$ (la teoría de conjuntos finitos que comentábamos) en PA. Definiremos también la interpretación inversa de una interpretación y construiremos la inversa de la interpretación de Ackermann. A partir de esto, veremos qué significa exactamente la noción de teorías esencialmente equivalentes y que estas dos teorías lo son.

Por último, aunque este resultado no formará parte del trabajo, cabe destacar que el Teorema de Goodstein tampoco puede probarse en $\mathsf{ZF_{fin}}^*$. Sin embargo, el hecho de que no pueda probarse en PA y PA sea esencialmente equivalente a $\mathsf{ZF_{fin}}^*$ no es suficiente para demostrar esto.

Capítulo 1

Teoría de Conjuntos.

1.1. Introducción.

La Teoría de Conjuntos nació en 1873 y se considera a Georg Cantor su principal creador. Se ocupa, naturalmente, del estudio matemático de los conjuntos y sus propiedades (matemáticamente interesantes). Uno de sus objetivos principales es fundamentar las Matemáticas. Dentro de la Teoría de Conjuntos se pueden desarrollar todos los objetos y estructuras matemáticos más importantes (números naturales, enteros, racionales, reales, relaciones, funciones, etc.).

Pero, ¿qué es exactamente un conjunto? O, mejor dicho, ¿qué tipo de conjuntos exactamente forman parte del universo de la Teoría de Conjuntos? Pues bien, intuitivamente, un conjunto es una *colección* de *objetos*. Y, en concreto, los conjuntos que forman parte de la Teoría son conjuntos cuyos elementos son conjuntos; a su vez, los elementos de estos elementos también son conjuntos; y así sucesivamente. Es lo que se llama *conjuntos hereditarios* o *conjuntos puros*. Sin embargo, ya el mismo Cantor sabía que no toda colección de conjuntos es un conjunto. A estas colecciones las llamaremos *clases propias*. Por ejemplo, la clase que contiene a todos los conjuntos y la clase que contiene a todos los conjuntos que no son elementos de sí mismos son clases propias.

Como veremos a continuación, la Teoría de Conjuntos es un sistema axiomático. Por tanto, debemos determinar las nociones primitivas no definidas por el sistema: por un lado, tenemos los objetos de la Teoría, los *conjuntos*; por otro lado, tenemos la relación existente entre ellos, que será la *pertenencia*. Además, es un sistema formal. Por tanto, para construirlo, se necesita de un lenguaje formal. Todo lo que esté "dentro"de la Teoría debe ser expresable en dicho lenguaje. Éste será el de la lógica de primer orden con igualdad junto con un símbolo no lógico, $\in$, que designa la relación de pertenencia. Denotaremos al lenguaje como $\mathcal{L}_{\varepsilon}$.

Según se avanza en el desarrollo del sistema, aparecen nociones nuevas que son definidas en términos de nociones primitivas o nociones ya definidas. Por ejemplo, la noción de *subconjunto* o *intersección*. Para expresar estas nuevas nociones ampliamos el alfabeto con nuevos símbolos, pero realmente sólo estamos utilizando abreviaturas, ya que estos nuevos

símbolos corresponderán a una fórmula expresable en nuestro lenguaje.

1.2. Axiomas.

Por un lado, los axiomas lógicos y las reglas de inferencia de la Teoría de Conjuntos son los de la lógica de primer orden con igualdad. Se tienen los símbolos lógicos habituales: $\neg, \rightarrow, \wedge, \vee, \leftrightarrow, \forall, \exists, =$; el símbolo no lógico $\in$; símbolos auxiliares: (,) , [,] y variables $(x, y, z, A, B, \alpha, \beta, \dots)$.

$'x = y'$ y $'x \in y'$ son fórmulas de $\mathcal{L}_\varepsilon$. Si φ y ψ son fórmulas de $\mathcal{L}_\varepsilon$, entonces las siguientes expresiones también lo son:

$$\varphi \wedge \psi, \varphi \vee \psi, \varphi \rightarrow \psi, \varphi \leftrightarrow \psi, \neg\varphi.$$

Si $\varphi(x)$ es una fórmula de $\mathcal{L}_\varepsilon$, entonces las siguientes expresiones también lo son:

$$\exists x\varphi(x), \forall x\varphi(x).$$

Sean φ, ψ y η fórmulas de $\mathcal{L}_\varepsilon$. Los *axiomas lógicos* son los siguientes:

1. $\varphi \rightarrow [\psi \rightarrow \varphi]$.
2. $[\varphi \rightarrow [\psi \rightarrow \eta]] \rightarrow [[\varphi \rightarrow \psi] \rightarrow [\varphi \rightarrow \eta]]$.
3. $[\neg\varphi \rightarrow \neg\psi] \rightarrow [\psi \rightarrow \varphi]$.
4. $\forall x[\varphi \rightarrow \psi(x)] \rightarrow [\varphi \rightarrow \forall x\psi(x)]$.
5. $\forall x\varphi(x) \rightarrow \varphi(v)$, donde v es una variable libre que ha reemplazado a la variable ligada x.

Sean φ y ψ fórmulas de $\mathcal{L}_\varepsilon$. Las *reglas de inferencia* son las que siguen:

1. De φ y $\varphi \rightarrow \psi$ se deduce ψ.
2. De φ se deduce $\forall x\varphi(x)$, donde $\varphi(x)$ se obtiene reemplazando en φ todas las apariciones de alguna variable libre por x.

Además, también se añaden los siguientes *axiomas de igualdad*:

1. Axioma de identidad: $\forall x(x = x)$.
2. Esquema de sustitución: Para cada fórmula $\varphi(x)$ de $\mathcal{L}_\varepsilon$ se tiene

$$\forall x\forall y[x = y \rightarrow (\varphi(x) \leftrightarrow \varphi(y))].$$

Por otro lado, los axiomas no lógicos que determinan la teoría son los que presentaremos a continuación.

Axioma de extensionalidad (Ext).

Si dos conjuntos son tales que todo elemento del primero es también elemento del segundo y todo elemento del segundo lo es también del primero, entonces los dos conjuntos son iguales.

En el lenguaje formal:

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y).$$

Axioma del conjunto vacío (Vacío).

Existe un conjunto que no tiene elementos.

$$\exists x \forall y \neg (y \in x).$$

A este conjunto lo llamamos *conjunto vacío* y lo denotamos como '$\varnothing$'.

Axioma-esquema de separación (Sep).

Si $\varphi(x,y_1,\ldots,y_n)$ es una propiedad de conjuntos $x,y_1,\ldots,y_n$ expresable por una fórmula de $\mathcal{L}_\varepsilon$, entonces para cualesquiera conjuntos $b_1,\ldots,b_n$ y para cada conjunto a existe un conjunto b cuyos elementos son los elementos x del conjunto a tales que $\varphi(x,b_1,\ldots,b_n)$.

Formalmente, sea $\varphi(x; y_1, \ldots, y_n)$ una fórmula e y una variable que no ocurre libre en $\varphi(x; y_1, \ldots, y_n)$:

$$\forall y_1, \ldots, \forall y_n (\forall z \exists y \forall x (x \in y \leftrightarrow x \in z \wedge \varphi(x; y_1, \ldots, y_n))).$$

En realidad, es un esquema de axiomas, ya que tenemos un axioma por cada fórmula $\varphi(x; y_1, \ldots, y_n)$. Además, cada fórmula define la *clase* que contiene a todos los conjuntos que la satisfacen. Una clase es una colección de conjuntos que puede ser o no un conjunto. Así,

$$\mathbf{A} = \{x : \varphi(x; y_1, \ldots, y_n)\} \text{ es una clase.}$$

En vez de escribir $\varphi(x; y_1, \ldots, y_n)$, utilizaremos '$x \in \mathbf{A}$' como abreviatura. Como no toda colección de conjuntos es un conjunto, no podemos asegurar que $\mathbf{A}$ lo sea. Por ese motivo decimos que es una clase. $\mathbf{A}$ será un conjunto si $\exists y \forall x (x \in y \leftrightarrow x \in \mathbf{A})$. En caso contrario, si $\mathbf{A}$ no es un conjunto será una *clase propia*, es decir, una colección de conjuntos que no es un conjunto. Por tanto, lo que nos dice **Sep** es que para todo conjunto z, la clase $\{x : x \in \mathbf{A} \wedge x \in z\}$ es un conjunto.

Definición 1.2.1 *Dados dos conjuntos a y b. Diremos que a es subconjunto de b y abreviaremos como '$a \subseteq b$' si se cumple que: $\forall x (x \in a \rightarrow x \in b)$.*

Proposición 1.2.2 *Dados dos conjuntos a y b. Existe un conjunto único cuyos elementos son los elementos comunes de a y b.*

Demostración: Consideremos el conjunto a y la fórmula '$x \in b$'. Por **Sep**, existe c tal que para todo x, $x \in c \leftrightarrow x \in a \wedge x \in b$. Por **Ext** este conjunto es único. ⊠

Definición 1.2.3 *Dados dos conjuntos a y b. Al conjunto cuyos elementos son los comunes de a y b lo llamamos conjunto intersección de a y b y lo denotamos como '$a \cap b$'.*

Axioma del par (Par).

Para cualesquiera conjuntos a y b, existe un conjunto cuyos únicos elementos son a y b.

$$\forall x \forall y \exists z \forall u (u \in z \leftrightarrow u = x \vee u = y).$$

Axioma del conjunto unión (Unión).

Para cada conjunto a existe un conjunto cuyos elementos son los elementos de los elementos de a.

$$\forall x \exists y \forall z (z \in y \leftrightarrow \exists u (u \in x \wedge z \in u)).$$

A este conjunto lo denotamos como '$\cup a$'.

Proposición 1.2.4 *Para cualesquiera conjuntos a y b existe un conjunto único cuyos elementos son los elementos de a y los elementos de b.*

Demostración: Por **Par**, existe el conjunto $\{a, b\}$. Por **Unión**, existe el conjunto $\cup\{a, b\}$, que es el conjunto que buscamos. Es único por **Ext**. ⊠.

Definición 1.2.5 *Dados dos conjuntos a y b, al conjunto cuyos elementos son los elementos de a y los de b lo llamamos unión de a y b y lo denotamos como '$a \cup b$'.*

Proposición 1.2.6 *Dado un conjunto a, existe un conjunto único cuyos elementos son los conjuntos que pertenecen a todos los elementos de a.*

Demostración: La clase $\{x \in \cup a : \forall b (b \in a \to x \in b)\}$ existe por **Unión** y es un conjunto por **Sep**. Además, es único por **Ext**. ⊠.

Definición 1.2.7 *Dado un conjunto a, al conjunto cuyos elementos son los conjuntos que pertenecen a todos los elementos de a lo denotamos como '$\cap a$'.*

Definición 1.2.8 *Para cualesquiera conjuntos a y b, llamaremos par ordenado y denotaremos por $\langle a, b\rangle$ al conjunto $\{\{a\}, \{a, b\}\}$.*

Nótese que el par ordenado de dos conjuntos es un conjunto por **Par**.

Definición 1.2.9 *Dadas dos clases $\boldsymbol{A}$ y $\boldsymbol{B}$. Denotamos por $\boldsymbol{A} \times \boldsymbol{B}$ a la siguiente clase:*

$$\boldsymbol{A} \times \boldsymbol{B} = \{\langle a, b\rangle : a \in \boldsymbol{A} \wedge b \in \boldsymbol{B}\}.$$

Definición 1.2.10 *Decimos que una fórmula $\varphi(x)$ define una relación si se cumple lo siguiente:*

$$\forall x[\varphi(x) \to \exists a \exists b(x = \langle a, b\rangle)].$$

Además, a la clase $\boldsymbol{R} = \{x : \varphi(x)\}$ la llamamos relación.

Definición 1.2.11 *Supongamos que una clase $\boldsymbol{F}$ es una relación. Diremos que $\boldsymbol{F}$ es una función si para cualesquiera conjuntos x, y, z se tiene que: si $\langle x, y\rangle \in \boldsymbol{F}$ y $\langle x, z\rangle \in \boldsymbol{F}$, entonces $y = z$. Si $\langle x, y\rangle \in \boldsymbol{F}$ escribiremos que $\boldsymbol{F}(x) = y$.*

Axioma-esquema de Reemplazamiento (Reemp).

Sea $\mathbf{F}$ una función, entonces para todo conjunto a, la clase:

$$\mathbf{F}[a] = \{y : \exists x(x \in a \wedge \mathbf{F}(x) = y)\}.$$

es un conjunto.

En realidad, **Reemp** es un esquema de axiomas, ya que tenemos un axioma por cada clase que es una función.

Llegados a este punto, debemos aclarar que no existe una única Teoría de Conjuntos. Dependiendo de los axiomas que incluyamos podemos obtener teorías diferentes en las que surgen resultados distintos. Hasta ahora, los axiomas que llevamos conforman lo que llamamos la teoría EST, por sus sigas en inglés ('Elementary Set Theory' o 'Teoría de Conjuntos Elemental').

$$\mathsf{EST} = \textbf{Ext} + \textbf{Vacío} + \textbf{Sep} + \textbf{Par} + \textbf{Unión} + \textbf{Reemp}.$$

(En realidad, **Sep** es redundante en presencia de **Reemp**, por lo que se podría prescindir de incluirlo).

Sigamos presentando nuevos axiomas.

Axioma de las Partes o del Conjunto Potencia (Pot).

Para cada conjunto a existe un conjunto que denotaremos $\mathcal{P}(a)$ cuyos elementos son los subconjuntos de a.

$$\forall x \exists y(z \in y \leftrightarrow z \subseteq x).$$

Teorema 1.2.12 *Para dos conjuntos cualesquiera A y B, la clase $A \times B$ es un conjunto.*

Demostración: Sean $a \in A$ y $b \in B$ cualesquiera. Por **Par**, $\{a\}$ y $\{a, b\}$ son conjuntos. Además, $\{a\}, \{a, b\} \subseteq A \cup B$, que existe por **Unión**. Por tanto, $\{a\}, \{a, b\} \in \mathcal{P}(A \cup B)$, que es un conjunto según **Pot**. Así, el conjunto $\{\{a\}, \{a, b\}\} = \langle a, b\rangle$ está contenido en $\mathcal{P}(A \cup B)$. Por consiguiente, $\langle a, b\rangle \in \mathcal{P}(\mathcal{P}(A \cup B))$. Se tiene entonces que:

$$A \times B = \{x \in \mathcal{P}(\mathcal{P}(A \cup B)) : \exists a \exists b(a \in A \wedge b \in B \wedge x = \langle a, b\rangle)\},$$

que es un conjunto por **Sep**. ⊠

Axioma del Infinito (Inf).

Existe un conjunto que tiene al conjunto vacío como elemento y es tal que si x es un elemento suyo, entonces $x \cup \{x\}$ también lo es.

$$\exists y(\varnothing \in y \wedge \forall x(x \in y \rightarrow x \cup \{x\} \in y)).$$

A los conjuntos que satisfacen lo anterior se les denomina *conjuntos inductivos.*

Axioma de Regularidad (Reg).

$$x \neq \varnothing \rightarrow \exists y(y \in x \wedge x \cap y = \varnothing).$$

En este punto, debemos destacar una teoría importante que incluye a todos los axiomas que llevamos hasta ahora: la teoría ZF (por Zermelo y Fraenkel).

$$\mathsf{ZF} = \textbf{Ext} + \textbf{Vacío} + \textbf{Sep} + \textbf{Par} + \textbf{Unión} + \textbf{Reemp} + \textbf{Pot} + \textbf{Inf} + \textbf{Reg}.$$

Otra teoría importante que utilizaremos al final de este trabajo es $\mathsf{ZF}_{\mathsf{fin}}$. Incluirá todos los axiomas que incluye ZF salvo que en lugar de **Inf**, tenemos $\neg$**Inf**. Será una teoría de conjuntos finitos.

$$\mathsf{ZF}_{\mathsf{fin}} = \textbf{Ext} + \textbf{Vacío} + \textbf{Sep} + \textbf{Par} + \textbf{Unión} + \textbf{Reemp} + \textbf{Pot} + \neg\textbf{Inf} + \textbf{Reg}.$$

Por último, queda presentar el axioma de elección, que apareció en forma de un principio de elección en una demostración del teorema del buen orden que publicó Zermelo en el año 1904. Este principio de elección fue el origen de una considerable polémica durante los años siguientes. Añadido a la teoría ZF constituye la teoría ZFC .

Definición 1.2.13 *Sea $\boldsymbol{F}$ una clase que es además una función. Se denomina dominio de $\boldsymbol{F}$ y se denota como 'dom($\boldsymbol{F}$)' a la siguiente clase:*

$$dom(\boldsymbol{F}) = \{x : \exists y(\langle x, y\rangle \in \boldsymbol{F})\}.$$

Nótese que si F es un conjunto, entonces $dom(F) = \{x \in \cup F : \exists y(\langle x, y\rangle \in F)\}$, que es un conjunto por **Unión** y **Sep**.

Si $\mathbf{A}$ y $\mathbf{B}$ son dos clases y f es una función contenida en $\mathbf{A} \times \mathbf{B}$ tal que $dom(f) = \mathbf{A}$, diremos que f es una función de $\mathbf{A}$ en $\mathbf{B}$ y lo notaremos como $f : \mathbf{A} \to \mathbf{B}$.

Axioma de Elección (AC).

Para todo conjunto a existe un conjunto F tal que

$$F \text{ es una función } \wedge\, dom(F) = a \wedge \forall x \in a(x \neq \varnothing \to F(x) \in x).$$

Por tanto, ZFC=ZF+**AC**.

Capítulo 2

Ordinales y números naturales.

Una vez introducida la Teoría de Conjuntos y sus axiomas más importantes, ya estamos listos para exponer, a lo largo de este capítulo, una construcción de gran utilidad dentro de la Teoría de Conjuntos: los números ordinales. En particular, en este trabajo, necesitaremos la Forma Normal de Cantor (sección 2.4.4) para definir la sucesión de Goodstein. Además, también requeriremos los ordinales para la demostración del Teorema de Goodstein y para la construcción de toda la artillería empleada en la demostración de la independencia de la teoría PA del Teorema de Goodstein.

Veremos también los números naturales, que son una parte de los números ordinales, y haremos hincapié en el papel que juega **Inf** a la hora de definirlos. A lo largo del presente capítulo trabajaremos fundamentalmente dentro de la teoría ZF. Sin embargo, nos detendremos a observar qué ocurre cuando cambiamos **Inf** por su negación (cambiando a la teoría $\mathsf{ZF_{fin}}$).

2.1. Ordinales. Definición y propiedades.

En primer lugar, será necesario establecer la noción de *clase bien ordenada* y algunas de sus propiedades.

Definición 2.1.1 *Sean $\boldsymbol{A}$ una clase y $<$ una relación sobre $\boldsymbol{A}$; es decir, $< \subseteq \boldsymbol{A} \times \boldsymbol{A}$. Sean $x, y \in \boldsymbol{A}$. Notaremos:*

- $x < y$ *si* $\langle x, y\rangle \in <$.
- $x \leq y$ *si* $x < y \vee x = y$.
- $x \not< y$ *si* $\langle x, y\rangle \notin <$.

Diremos que $<$ es un buen orden sobre $\boldsymbol{A}$, o que $\boldsymbol{A}$ está bien ordenado por $<$, si:

1. *$<$ es irreflexiva:* $\forall x \in \boldsymbol{A}(x \not< x)$.
2. *$<$ es transitiva:* $\forall x, y, z \in \boldsymbol{A}(x < y \wedge y < z \to x < z)$.

3. $\forall x, y \in \boldsymbol{A}(x \leq y \vee y \leq x)$.

4. $<$ *es adecuada a izquierda:* $\forall x \in \boldsymbol{A}(\{y \in \boldsymbol{A} : y < x\}$ *es un conjunto).*

5. $\forall B[B \subseteq \boldsymbol{A} \wedge B \neq \varnothing \rightarrow \exists x(x \in B \wedge \forall y \in B(y \not< x))]$.

Definición 2.1.2 *Sea* $\boldsymbol{A}$ *una clase,* $<$ *un buen orden sobre* $\boldsymbol{A}$ *y* $a \in \boldsymbol{A}$*. Una* ***sección inicial*** *de* $\boldsymbol{A}$ *determinada por* a *y* $<$ *es el conjunto de los elementos de* $\boldsymbol{A}$ *que son* $<$*-estrictamente menores que* a*:*

$$sec(a, \boldsymbol{A}, <) = \{x \in \boldsymbol{A} : x < a\}$$

Definición 2.1.3 *Sean* $\boldsymbol{A}$ *y* $\boldsymbol{B}$ *dos clases y* $<, <'$ *dos buenos órdenes sobre* $\boldsymbol{A}$ *y* $\boldsymbol{B}$ *respectivamente. Decimos que una función* $\boldsymbol{F} : \boldsymbol{A} \rightarrow \boldsymbol{B}$ *es biyectiva si cumple:*

- $\boldsymbol{F}$ *inyectiva:* $\forall a, a' \in \boldsymbol{A}(\boldsymbol{F}(a) = \boldsymbol{F}(a') \rightarrow a = a')$.
- $\boldsymbol{F}$ *sobreyectiva:* $\forall b \in \boldsymbol{B}(\exists a \in \boldsymbol{A}(\boldsymbol{F}(a) = b))$.

Definición 2.1.4 *Sean* $\boldsymbol{A}$ *y* $\boldsymbol{B}$ *dos clases y* $<, <'$ *dos buenos órdenes sobre* $\boldsymbol{A}$ *y* $\boldsymbol{B}$ *respectivamente. Decimos que una función* $\boldsymbol{F} : \boldsymbol{A} \rightarrow \boldsymbol{B}$ *es creciente si para todos* $a, a' \in \boldsymbol{A}$ *tales que* $a < a'$ *se cumple que* $\boldsymbol{F}(a) <' \boldsymbol{F}(a')$.

Definición 2.1.5 *Sean* $\boldsymbol{A}$ *y* $\boldsymbol{B}$ *dos clases y* $<, <'$ *dos buenos órdenes sobre* $\boldsymbol{A}$ *y* $\boldsymbol{B}$ *respectivamente. Decimos que una función* $\boldsymbol{F} : \boldsymbol{A} \rightarrow \boldsymbol{B}$ *es un isomorfismo* ($\boldsymbol{F} : \boldsymbol{A} \cong \boldsymbol{B}$) *si* $\boldsymbol{F}$ *es biyectiva y creciente.*

Si entre dos clases $\mathbf{A}$ y $\mathbf{B}$ existe un isomorfismo, diremos que $\mathbf{A}$ y $\mathbf{B}$ son isomorfas y escribiremos $\mathbf{A} \cong \mathbf{B}$.

Teorema 2.1.6 (Comparación de clases bien ordenadas.) *Sean* $\boldsymbol{A}$ *y* $\boldsymbol{B}$ *dos clases bien ordenadas. Entonces, se cumple una y sólo una de las tres posibilidades siguientes:*

1. $\boldsymbol{A} \cong \boldsymbol{B}$.
2. $\boldsymbol{A}$ *es isomorfa a una sección inicial de* $\boldsymbol{B}$.
3. $\boldsymbol{B}$ *es isomorfa a una sección inicial de* $\boldsymbol{A}$.

⊠

Una vez vistas estas nociones de clases bien ordenadas que nos serán necesarias, ya casi estamos listos para definir los números ordinales. Primero, otra definición.

Definición 2.1.7 *Un conjunto* A *es* ***transitivo*** *si cumple una cualquiera de las condiciones equivalentes siguientes:*

1. *Todo elemento de cada elemento de* A *es elemento de* A

2. *Cada elemento de A es un subconjunto de A*

3. $\cup A \subseteq A$

4. $A \subseteq \mathcal{P}(A)$

Definición 2.1.8 *Para una clase $\boldsymbol{A}$, la relación de pertenencia sobre $\boldsymbol{A}$ será la clase $\in_{\boldsymbol{A}} = \{\langle x, y\rangle \in \boldsymbol{A} \times \boldsymbol{A} \mid x \in y\}$. Teniendo esto en cuenta, se dice que un conjunto es un* ***número ordinal*** *(u ordinal a secas) si es transitivo y está bien ordenado por la relación de pertenencia.*

Ahora, vamos a ver algunas propiedades de los ordinales para empezar a entender cómo se comportan.

Proposición 2.1.9 *Todo elemento de un ordinal es un ordinal.*

Demostración: Sea α un ordinal y sea a un elemento de α.

Por un lado, supongamos que c pertenece a un elemento b de a. Como α es transitivo y $b \in a$, entonces $b \in \alpha$. Además, como $c \in b$, entonces también $c \in \alpha$. Se tiene que $a, b, c \in \alpha$ y α está bien ordenado por $\in_\alpha$. Por tanto, por la propiedad transitiva de $\in_\alpha$, como $c \in b$ y $b \in a$ resulta que $c \in a$ y a es un conjunto transitivo.

Veamos ahora que $\in_a$ es un buen orden de a. Como $a \in \alpha$ y α es transitivo, entonces $a \subseteq \alpha$ y la restricción $\in_\alpha \cap (a \times a)$ de $\in_\alpha$ a a es un buen orden de a. Pero $\in_\alpha \cap (a \times a)$ es precisamente $\in_a$. ⊠

Proposición 2.1.10 *Sea α un ordinal y sea δ un elemento de α. Entonces, $sec(\delta, \alpha, \in_\alpha)$ es igual a δ.*

Demostración: Veámoslo por doble inclusión. Como $\delta \in \alpha$ y α es transitivo, entonces $\delta \subseteq \alpha$, luego $\delta \subseteq \{x \in \alpha \mid x \in \delta\} = sec(\delta, \alpha, \in_\alpha)$. Por otro lado, claramente si $b \in sec(\delta, \alpha, \in_\alpha)$, entonces $b \in \delta$. ⊠

Proposición 2.1.11 *Sean α y β dos ordinales (bien ordenados por las relaciones de pertenencia $\in_\alpha, \in_\beta$ respectivamente) tales que $\alpha \cong \beta$. Entonces $\alpha = \beta$.*

Demostración: Sea f un isomorfismo entre los conjuntos bien ordenados α y β. Queremos ver que f es la función identidad sobre α, es decir, que $f(x) = x$ para todo $x \in \alpha$.

Sea $B = \{x \in \alpha \mid f(x) \neq x\}$. Veamos que B es el conjunto vacío. Por reducción al absurdo, supongamos que no es vacío. Como subconjunto de α, B tiene un elemento mínimo (en el sentido del buen orden $\in_\alpha$) que llamaremos γ. Entonces, para cada $\delta \in \alpha$, si $\delta \in \gamma$, $\delta \notin B$ y $f(\delta) = \delta$. Luego

$$sec(\gamma, \alpha, \in_\alpha) = \{\delta \in \alpha \mid \delta \in \gamma\} = \{\delta \in \alpha \mid f(\delta) \in f(\gamma)\} = \{y \in \beta \mid y \in f(\gamma)\} = sec(f(\gamma), \beta, \in_\beta)$$

por las propiedades de los isomorfismos.

Por la Proposición 2.1.10, $\gamma = sec(\gamma, \alpha, \in_\alpha)$ y $f(\gamma) = sec(f(\gamma), \beta, \in_\beta)$. Y, por la cadena de igualdades que acabamos de deducir, tenemos que $\gamma = f(\gamma)$, lo cual es una contradicción ya que $\gamma \in B$. Por tanto, B es el conjunto vacío y, en consecuencia, el isomorfismo f es único y es la función identidad. Por consiguiente, tiene que ser $\alpha = \beta$. ⊠

A continuación, veremos que dos ordinales cualesquiera siempre son comparables por la relación de pertenencia.

Proposición 2.1.12 (Propiedad de tricotomía.) *Dados dos ordinales cualesquiera α y β, se cumple una y sólo una de las tres posibilidades siguientes: $\alpha \in \beta, \alpha = \beta$ ó $\beta \in \alpha$.*

Demostración: Por el Teorema 2.1.6, podemos afirmar que α y β, al ser conjuntos bien ordenados por la relación de pertenencia, se tiene que o son isomorfos o uno es isomorfo a una sección inicial del otro. Según esto, distinguimos tres casos excluyentes:

- $\alpha \cong \beta$. Lo que implica, según la Proposición 2.1.11 que $\alpha = \beta$.
- Existe $\delta \in \alpha$ tal que $\text{sec}(\delta, \alpha, \in_\alpha) \cong \beta$. Por tanto, como $\delta = sec(\delta, \alpha, \in_\alpha)$ por la Proposición 2.1.10, entonces $\delta = \beta$ y $\beta \in \alpha$.
- Existe $\delta \in \beta$ tal que $sec(\delta, \beta, \in_\beta) \cong \alpha$. Por un razonamiento análogo al anterior, obtenemos que $\alpha \in \beta$.

⊠

Ahora, veremos que todo conjunto no vacío de ordinales tiene elemento mínimo en el sentido de $\in$.

Proposición 2.1.13 *Sea A un conjunto no vacío de ordinales. Entonces A tiene un elemento único α tal que $\alpha \in \beta$ para todo $\beta \in A$ distinto de α. Decimos que dicho α es el elemento mínimo de A.*

Demostración: Como A es no vacío, sea γ un elemento de A. Se distinguen dos casos:

- $\gamma \cap A = \varnothing$.

  En este caso, para cada $\beta \in A$ distinto de γ, $\beta \notin \gamma$, y por la tricotomía de ordinales tiene que ser $\gamma \in \beta$.

- $\gamma \cap A \neq \varnothing$.

  Entonces $\gamma \cap A$ es un subconjunto no vacío del ordinal γ. Como γ está bien ordenado por la relación de pertenencia, existe un α en $\gamma \cap A$ tal que para cada $\beta \in \gamma \cap A$, si $\beta \neq \alpha$, entonces $\alpha \in \beta$. Este α es el elemento buscado:

  Sea $\beta \in A$ distinto de α. Si $\beta \notin \gamma$ entonces $\gamma \in \beta$ ó $\gamma = \beta$, luego $\gamma \subseteq \beta$ y $\alpha \in \beta$. En el caso de que $\beta \in \gamma$ se tendría que $\beta \in \gamma \cap A$, con lo que $\alpha \in \beta$.

Con lo cual, en todo caso encontramos el elemento buscado (único por tricotomía) y queda demostrada la proposición. ⊠

Hasta ahora, hemos visto que la clase que contiene a todos los números ordinales es transitiva, ya que los elementos de los ordinales son ordinales. Además, la relación $\in$ de pertenencia entre ordinales es un buen orden de dicha clase, ya que:

1. Para todo ordinal α: $\alpha \notin \alpha$ por la propiedad de tricotomía.
2. Para cualesquiera ordinales α, β y γ: si $\alpha \in \beta$ y $\beta \in \gamma$, entonces $\alpha \in \gamma$ por ser γ transitivo.
3. Para cualesquiera ordinales α y β : $\alpha \in \beta, \alpha = \beta$ ó $\beta \in \alpha$ por la propiedad de tricotomía.
4. Para todo ordinal α, $\{x : x \text{ es ordinal} \wedge x \in \alpha\} = \alpha$, ya que todos los elementos de α son ordinales por la Proposición 2.1.9. Por tanto, es un conjunto.
5. Cada conjunto no vacío de ordinales tiene elemento mínimo por la Proposición 2.1.13.

Según estas propiedades, si la clase de todos los ordinales es un conjunto, entonces es también un ordinal, por lo que es elemento de sí mismo, pero un ordinal no puede ser elemento de sí mismo. Obtenemos una contradicción conocida como la **Paradoja de Burali-Forti** o **Paradoja de Cantor**. Por este motivo, la clase de todos los ordinales no es un conjunto, no está "dentro" de nuestro universo.

A esta clase propia la denominaremos a partir de ahora **On**.

$$\mathbf{On} = \{x \mid x \text{ es un ordinal}\}.$$

Como acabamos de ver, la pertenencia entre ordinales tiene las propiedades características de un buen orden, y a partir de ahora, para dos ordinales cualesquiera α y β, en vez de $\alpha \in \beta$ podemos escribir $\alpha < \beta$. Así pues, un ordinal será el conjunto de todos los ordinales menores que él.

Teorema 2.1.14 (Principio del elemento mínimo para On) *Sea $\boldsymbol{A}$ una clase no vacía de ordinales. Entonces $\boldsymbol{A}$ tiene mínimo, es decir, existe un ordinal $\alpha \in \boldsymbol{A}$ tal que $\alpha \leq \beta$ para todo $\beta \in \boldsymbol{A}$.*

Demostración: Como $\mathbf{A} \neq \varnothing$, hay un ordinal $\alpha \in \mathbf{A}$. Si $\alpha \leq \beta$ para todo $\beta \in \mathbf{A}$ hemos terminado. En caso contrario, existe $\beta \in \mathbf{A}$ tal que $\beta < \alpha$.

Consideremos el conjunto $\alpha \cap \mathbf{A}$, que es un conjunto por ser subconjunto de α y es distinto del vacío porque tiene a β como elemento. Por la Proposición 2.1.13, $\alpha \cap \mathbf{A}$ tiene elemento mínimo, sea δ. Veamos que δ es también el elemento mínimo de $\mathbf{A}$. Imaginemos, por reducción al absurdo, que existe $\gamma \in \mathbf{A}$ tal que $\gamma < \delta$. Entonces, por transitividad, $\gamma \in \alpha$ y δ no sería el elemento mínimo. Se llega por tanto a una contradicción. ⊠

Lema 2.1.15 *Todo conjunto transitivo de ordinales es un ordinal.*

Demostración: Si A es un conjunto de ordinales, ya hemos visto que $\in_A$ es un buen orden de A. Como además A es transitivo, es un ordinal. ⊠

Lema 2.1.16 *Para cualesquiera ordinales α y β, $\alpha \in \beta$ si y sólo si $\alpha \subset \beta$ (estrictamente).*

Demostración: Si $\alpha \in \beta$, como β es transitivo, $\alpha \subseteq \beta$, y al ser $\alpha \neq \beta$, entonces $\alpha \subset \beta$. Para el recíproco, si $\alpha \subset \beta$, entonces $\alpha \neq \beta$ y $\beta \notin \alpha$ (ya que si $\beta \in \alpha$ entonces $\beta \in \beta$). Luego, por tricotomía $\alpha \in \beta$. ⊠

A continuación, daremos algunos métodos para obtener nuevos ordinales a partir de otros ya dados.

Proposición 2.1.17 *Sea α un ordinal. Entonces, $\alpha^+ = \alpha \cup \{\alpha\}$ es también un ordinal y es además el menor ordinal mayor que α. A α^+ se le denomina el ordinal sucesor o el siguiente de α.*

Demostración: Todos los elementos de α^+ son ordinales. Los elementos de los elementos de α^+ son ordinales menores que α, por lo que son elementos de α y también de α^+. Por tanto, α^+ es un conjunto transitivo de ordinales, es decir, un ordinal.

Por otro lado, $\alpha < \alpha^+$ claramente. Supongamos que β es un ordinal mayor que α. Entonces, $\alpha \in \beta$ y $\alpha \subset \beta$, con lo que $\alpha^+ \subseteq \beta$ y $\alpha^+ \leq \beta$. ⊠

Proposición 2.1.18 *Si A es un conjunto de ordinales, entonces $\cup A$ es un ordinal y, además, $\cup A = sup A$. Es decir, es el menor ordinal que es mayor o igual que todos los elementos de A.*

Demostración: Por un lado, $\cup A$ es claramente un conjunto de ordinales. Supongamos ahora que $\alpha \in \cup A$. Entonces, existe $\beta \in A$ tal que $\alpha \in \beta$. Por tanto, también $\alpha \subset \beta$. Como $\beta \subseteq \cup A$, entonces $\alpha \subset \cup A$ y $\cup A$ es un conjunto transitivo de ordinales.

Ya hemos visto que es un ordinal. Ahora toca ver que es el supremo: Sea $\alpha \in A$. Entonces $\alpha \subseteq \cup A$ y por tanto $\alpha \leq \cup A$. Sea ahora β un ordinal mayor o igual que todos los elementos de A. Entonces, todos los elementos de A están contenidos en β, y por tanto, $\cup A$ está contenido en β y β es mayor o igual que $\cup A$. ⊠

Proposición 2.1.19 *Si A es un conjunto de ordinales, entonces $\cap A$ es un ordinal y, además, $\cap A = inf A$. Es decir, es el mayor ordinal que es menor o igual que todos los elementos de A. Además, como pertenece a A también es el mínimo de A.*

Demostración: A, al ser un conjunto no vacío de ordinales, tiene elemento mínimo, sea α, que está en A. Veamos que $\alpha = \cap A$ por doble inclusión.

Por un lado, $\alpha \in \beta$ para todo $\beta \in A$ tal que $\beta \neq \alpha$. Por tanto, $\alpha \subseteq \beta$ para todo $\beta \in A$ y $\alpha \subseteq \cap A$.

Por otro lado, sea $x \in \cap A$. Como $x \in \beta$ para todo $\beta \in A$, en particular $x \in \alpha$. Por consiguiente, $\cap A \subseteq \alpha$. ⊠

Para terminar esta sección, es conveniente presentar un resultado importante que no probaremos aquí pero muestra que los ordinales cumplen efectivamente su función de representantes de los conjuntos bien ordenados.

Teorema 2.1.20 *Sea A un conjunto bien ordenado. Existe un ordinal único α tal que*

$$A \cong \alpha.$$

$\boxtimes$

2.2. Tipos de ordinales y números naturales.

Una vez vistas algunas de las propiedades básicas de los ordinales, uno podría empezar a preguntarse qué forma tienen estos conjuntos tan característicos. Por ello, vamos a dar los primeros ejemplos:

El conjunto vacío es un conjunto transitivo y está bien ordenado por la relación de pertenencia. Por ello, es un ordinal. Además, por la propiedad de tricotomía de los ordinales, todo ordinal es mayor o igual que $\varnothing$. Por consiguiente, $\varnothing$ es el *menor* de todos los números ordinales o el *primer* ordinal.

Según la Proposición 2.1.17, siguiendo el buen orden $\in$, el ordinal siguiente a $\varnothing$ es $\varnothing^+ = \{\varnothing\}$. El siguiente a éste sería $\{\varnothing\}^+ = \{\varnothing, \{\varnothing\}\}$. Aplicando esto sucesivamente obtenemos los primeros ordinales:

$$\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, \ldots$$

Ahora, vamos a distinguir las tres categorías excluyentes en las que se dividen los ordinales:

- El ordinal $\varnothing$.
- Ordinal **sucesor**: se dice que α es un ordinal sucesor si existe un ordinal β tal que $\beta^+ = \beta \cup \{\beta\} = \alpha$.
- Ordinal **límite**: son aquellos ordinales distintos de $\varnothing$ y que no son sucesores.

Como apunte, si α es un ordinal sucesor tal que $\beta^+ = \alpha$, también notaremos β^+ como $\beta + 1$. Además, se dirá que β es el predecesor de α y escribiremos $\alpha - 1 = \beta$.

El siguiente lema nos ayudará a caracterizar a los ordinales límite.

Lema 2.2.1 *Sea α un ordinal distinto del vacío. Son equivalentes:*

1. *α es límite.*
2. *$\forall \beta < \alpha (\beta^+ < \alpha)$.*
3. *$\alpha = \bigcup \alpha$.*

Demostración: ($1 \Rightarrow 2$): Sea $\beta < \alpha$. Como β^+ es el menor ordinal mayor que β, entonces $\beta^+ \leq \alpha$. Por hipótesis, α no es sucesor, por tanto, $\beta^+ < \alpha$.

($2 \Rightarrow 3$): Por doble inclusión. Por ser α transitivo, $\bigcup \alpha \subseteq \alpha$. Veamos la inclusión en el otro sentido. Sea $\beta \in \alpha$. Por hipótesis, $\beta^+ \in \alpha$. Como $\beta \in \beta^+$, entonces $\beta \in \bigcup \alpha$.

($3 \Rightarrow 1$): Supongamos que α es sucesor. Entonces, existe un ordinal β tal que $\alpha = \beta^+$ y:

$$\bigcup \alpha = \bigcup (\beta \cup \{\beta\}) = \beta \neq \alpha,$$

lo cual contradice nuestra hipótesis. Por reducción al absurdo, α debe ser límite. ⊠

Ahora vamos a definir los *números naturales*, lo que nos permitirá darle nombre a los primeros ordinales.

Definición 2.2.2 *Un conjunto n es un **número natural** u ordinal finito si satisface:*

$$n \in \mathbf{On} \wedge [n = \varnothing \vee (n \text{ es sucesor} \wedge \forall x < n (x \text{ es sucesor} \vee x = \varnothing))].$$

Por tanto, al ordinal $\varnothing$ le llamamos ordinal 0. Como es natural, al siguiente de 0, que es $0^+ = \{\varnothing\}$ le llamamos 1. El ordinal $1^+ = \{\varnothing, \{\varnothing\}\}$ es el 2. $2^+ = 3 = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$. Y así sucesivamente. Como hemos dicho, los números naturales son los primeros ordinales, pero a continuación de los números naturales hay más ordinales que no son números naturales. Antes de ver cuáles son, notemos que hasta ahora, hemos definido los ordinales y los naturales sin la intervención de **Inf**. Sin embargo, para probar la existencia de ordinales mayores que los números naturales sí necesitamos este axioma.

Lema 2.2.3 *La clase $\mathbb{N}$ que contiene a todos los números naturales es un conjunto.*

Demostración: Sea A un conjunto inductivo, que existe por **Inf**. Veamos que $\mathbb{N}$ es subconjunto de A. Si A es un conjunto inductivo y existe $n \in \mathbb{N}$ tal que $n \notin A$, entonces el conjunto $B = \{x \in \mathbb{N} : x \leq n \wedge x \notin A\}$ es un conjunto de ordinales no vacío. Sea m su menor elemento, entonces $m \neq \emptyset$ luego, por ser un número natural $m = k \cup \{k\}$ para algún $k < m \leq n$. Puesto que $m \notin A$ y A es inductivo, necesariamente $k \notin A$, lo que nos da un contradicción, ya que tendríamos $k \in B$ y $k < m$. Hemos probado así que $B = \emptyset$ y, por tanto, no existe $n \in \mathbb{N}$ tal que $n \notin A$. Por tanto, $\mathbb{N} \subseteq A$ y, por **Sep**, $\mathbb{N}$ es un conjunto. ⊠

Proposición 2.2.4 *El conjunto $\mathbb{N}$ de los números naturales es un ordinal.*

Demostración: Sea $p \in \mathbb{N}$ y m, n dos conjuntos tales que $m \in n$ y $n \in p$. Como $p \in \mathbf{On}$, es transitivo y $m \in p$. Es decir, m es un ordinal (todos los elementos de los ordinales son ordinales) y $m < p$. Por ser p natural, m es el vacío o sucesor. Por tanto, $m \in \mathbb{N}$ y $\mathbb{N}$ resulta ser un conjunto transitivo de ordinales y por consiguiente un ordinal. ⊠

Proposición 2.2.5 *El conjunto de los números naturales es el menor ordinal límite.*

Demostración: Ya hemos visto que $\mathbb{N}$ es un ordinal. Claramente es distinto de 0. Si fuese un ordinal sucesor, entonces $\mathbb{N}$ sería un número natural y por tanto elemento de sí mismo, cosa que no es posible. Por tanto, $\mathbb{N}$ tiene que ser límite y además el menor porque todos los ordinales menores que él son números naturales, que son 0 o sucesores. ⊠

A $\mathbb{N}$ visto como ordinal, se le designa con la letra griega ω.

Por definición, un conjunto x es finito si existe un número natural n y una función biyectiva $f : n \to x$. Pues bien, el ordinal ω es infinito (es decir, no es finito). Los **números naturales** son los **ordinales finitos**. Claramente, todos los números naturales son conjuntos finitos. Pero además, si suponemos que existe un ordinal α que es finito pero no es natural, entonces $\alpha \notin \omega$, y por tricotomía $\omega \leq \alpha$, por lo que α contendrá a ω que es un conjunto infinito y α tiene que ser infinito.

De esta manera, ω también es el menor ordinal infinito. Por lo que hasta el momento, ya podemos decir que conocemos los siguientes ordinales: 0,1,2,3, ..., ω , ω^+,$(\omega^+)^+$, ...

Si nos encontráramos en $\mathsf{ZF_{fin}}$, el ordinal ω no existiría por ser un conjunto inductivo. Es decir, ω sería una clase propia. Además, por la tricotomía de los ordinales, cualquier ordinal mayor que ω tampoco existiría. En particular, como ω es el menor ordinal límite, en $\mathsf{ZF_{fin}}$ no existe ningún ordinal límite.

Por tanto, en $\mathsf{ZF_{fin}}$ sólo existen los ordinales finitos, es decir, los números naturales. Así, si queremos definir los números naturales en $\mathsf{ZF_{fin}}$ basta con dar la definición de número ordinal.

Teorema 2.2.6 $\mathsf{ZF_{fin}} \vdash \forall x(x \in \mathbf{On} \leftrightarrow x = \varnothing \vee \exists y \in \mathbf{On}(x = y \cup \{y\}))$.

⊠

Corolario 2.2.7 $\mathsf{ZF_{fin}} \vdash \forall x \subseteq \mathbf{On}(x \neq \varnothing \to \cup x \in x)$.

Demostración: Vamos a probar que $\cup x \in \mathbf{On}$.

Supongamos que $z \in y$ e $y \in \cup x$. Entonces, $\exists \alpha \in x$ tal que $y \in \alpha$. Como $\alpha \in \mathbf{On}$, entonces α es transitivo. Por tanto, $z \in \alpha$, y en consecuencia, $z \in \cup x$. Así, podemos afirmar que $\cup x$ es transitivo.

Por otro lado, todo elemento de $\cup x$ es elemento de un ordinal. Como los elementos de los ordinales son ordinales, $\cup x$ es un conjunto transitivo de ordinales y, por tanto, $\cup x \in \mathbf{On}$.

Supongamos que $\cup x \neq \varnothing$. Entonces, $\cup x$ es sucesor y existirá $\alpha \in x$ tal que $\cup x - 1 \in \alpha$. Entonces no existe ningún ordinal mayor que $\cup x - 1$ que pertenezca a $\cup x$, y podemos afirmar que $\cup x = \alpha \in x$.

Si $\cup x = \varnothing$, será $x = \{\varnothing\}$ y claramente $\cup x \in x$. ⊠

Una vez que sabemos cómo definir los números naturales en $\mathsf{ZF}_{\mathsf{fin}}$, vamos a probar el principio de inducción para los números naturales.

Teorema 2.2.8 *Sea φ una propiedad (expresable en $\mathsf{ZF}_{\mathsf{fin}}$). Entonces:*

$$\mathsf{ZF}_{\mathsf{fin}} \vdash [\varphi(0) \wedge \forall n(n \textit{ natural} \wedge \varphi(n) \rightarrow \varphi(n+1))] \rightarrow \forall n(n \textit{ natural} \rightarrow \varphi(n)).$$

Demostración: Razonemos en $\mathsf{ZF}_{\mathsf{fin}}$. Supongamos que:

$$\varphi(0) \wedge \forall n(\text{n natural} \wedge \varphi(n) \rightarrow \varphi(n+1)).$$

Por reducción al absurdo, supondremos que existe un n natural tal que $\neg\varphi(n)$. Entonces, el conjunto $A = \{n \in \mathbb{N} : \neg\varphi(n)\} \neq \varnothing$. Por **Reg**, existe $n^* \in A$ tal que $n^* \cap A = \varnothing$. Sabemos que $n^* \neq \varnothing$ porque $0 \notin A$ por hipótesis. Por tanto, existe $m \in \mathbb{N}$ tal que $n^* = m \cup \{m\}$. Como $n^* \cap A = \varnothing$, sabemos que $m \notin A$, por lo que se satisface $\varphi(m)$. Por hipótesis, también se satisface $\varphi(m+1) = \varphi(n^*)$. Con esto llegamos a una contradicción y queda probado el teorema. ⊠

Nótese que en la demostración de este último teorema, **Inf** no juega ningún papel y, de hecho, puede probarse también sin hacer uso de **Reg**. Por tanto, si estamos en la teoría ZF, la demostración del teorema del principio de inducción también se cumpliría.

2.3. Inducción transfinita y aritmética ordinal.

Otra vez de vuelta en ZF y tomando como antesala el Principio de inducción sobre los números naturales que vimos en el Teorema 2.2.8, ahora vamos a ver los principios de inducción y recursión primero sobre un ordinal cualquiera y luego sobre la clase propia de los ordinales, **On**. Estos principios son de muchísima utilidad para demostrar propiedades de los ordinales y definir funciones sobre ellos. Son una extensión del Principio de inducción sobre los números naturales a la clase **On** y casos particulares de los principios de inducción y recursión para clases bien ordenadas.

Teorema 2.3.1 (Principio de inducción completa hasta un ordinal α.) *Sea α un ordinal y A un subconjunto de α con la siguiente propiedad:*

$$\forall\beta < \alpha(\forall\delta < \beta(\delta \in A) \rightarrow \beta \in A).$$

Entonces $A = \alpha$.

⊠

Teorema 2.3.2 (Principio de inducción hasta un ordinal α) *Sea α un ordinal. Sea A un subconjunto de α con las propiedades siguientes:*

1. Si $0 < \alpha$, entonces $0 \in A$.
2. Para cada $\beta < \alpha$, si $\beta \in A$ y $\beta^+ < \alpha$, entonces $\beta^+ \in A$.
3. Para cada ordinal límite $\gamma < \alpha$, si $\delta \in A$ para todo $\delta < \gamma$, entonces $\gamma \in A$.

Entonces $A = \alpha$. ⊠

Teorema 2.3.3 (Principio de inducción completa) *Sea $\boldsymbol{A}$ una clase de ordinales tal que*

$$(\forall \beta < \alpha\ (\beta \in \boldsymbol{A})) \rightarrow \alpha \in \boldsymbol{A}$$

*Entonces, $\boldsymbol{A}$=**On**.*

⊠

Teorema 2.3.4 (Principio de inducción transfinita sobre On) *Sea $\boldsymbol{A}$ una clase de ordinales tal que*

1. $0 \in \boldsymbol{A}$.
2. *Para cada ordinal β, si $\beta \in \boldsymbol{A}$, entonces $\beta^+ \in \boldsymbol{A}$.*
3. *Para cada ordinal límite γ, si $\delta \in \boldsymbol{A}$ para todo $\delta < \gamma$, entonces $\gamma \in \boldsymbol{A}$.*

*Entonces, $\boldsymbol{A}$=**On**.* ⊠

Proposición 2.3.5 *Sea $\boldsymbol{V}$ la clase que contiene a todos los conjuntos y sea $\mathbf{G} : \boldsymbol{V} \times \boldsymbol{V} \rightarrow \boldsymbol{V}$ una función. Existe una única función $\boldsymbol{F} : \mathbf{On} \times \boldsymbol{V} \rightarrow \boldsymbol{V}$ tal que:*

$$\boldsymbol{F}(\alpha, x) = \boldsymbol{G}(\boldsymbol{F}_{|\alpha}(x), x),$$

donde $\boldsymbol{F}_{|\alpha} = \boldsymbol{F} \cap (\alpha \times \{x\} \times \boldsymbol{F}[\alpha \times \{x\}])$.

Teorema 2.3.6 (Recursión.) *Sean a un conjunto y $\boldsymbol{G}$,$\boldsymbol{H}$: $\boldsymbol{V} \times \boldsymbol{V} \rightarrow \boldsymbol{V}$ funciones. Existe una única función $\boldsymbol{F} : \mathbf{On} \times \boldsymbol{V} \rightarrow \boldsymbol{V}$ tal que:*

- $\boldsymbol{F}(0,x)=a$
- $\boldsymbol{F}(\alpha^+,x)=\boldsymbol{G}(\boldsymbol{F}(\alpha,x),x)$.
- $\boldsymbol{F}(\alpha,x)=\boldsymbol{H}(\{\boldsymbol{F}(\beta,x)\ :\ \beta < \alpha\ \},x)$ *si α es límite*

Gracias al Teorema de Recursión podemos justificar la existencia de las funciones suma, producto y exponenciación para ordinales. A continuación, vamos a definir recursivamente todas ellas y enumerar sus propiedades principales.

La suma.

Sean α y β dos ordinales cualesquiera, se define su suma como sigue:

$$\alpha + \beta = \begin{cases} \alpha & \text{si } \beta = 0 \\ (\alpha + (\beta - 1))^+ & \text{si } \beta \text{ es ordinal sucesor} \\ \bigcup\{\alpha + \delta \mid \delta < \beta\} & \text{si } \beta \text{ es ordinal límite} \end{cases}$$

(Si β es un ordinal sucesor con $\beta = \alpha^+$ para otro ordinal α, entonces se entiende $\beta - 1 = \alpha$).

Tenemos las siguientes propiedades para la suma:

- Asociativa: Para tres ordinales cualesquiera α, β y γ, tenemos que
$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$$
- La adición NO es conmutativa.
- Para dos ordinales cualesquiera α y β, $\alpha < \beta$ si y sólo si existe un ordinal $\delta > 0$ tal que $\alpha + \delta = \beta$.
- Para tres ordinales cualesquiera α, β y β': si $\beta < \beta'$ entonces $\alpha + \beta < \alpha + \beta'$.
- Para tres ordinales cualesquiera α, β y β': si $\alpha + \beta = \alpha + \beta'$ entonces $\beta = \beta'$.
- Sean $\alpha \leq \gamma$ ordinales. Entonces, existe un único ordinal β tal que $\alpha + \beta = \gamma$.
- Para tres ordinales cualesquiera α, α' y β: si $\alpha \leq \alpha'$, entonces $\alpha + \beta \leq \alpha' + \beta$.
- Para un ordinal β y un ordinal límite γ cualesquiera, entonces
$$\gamma + \beta \geq sup\{\delta + \beta \mid \delta < \gamma\}.$$

La multiplicación.

Sean α y β dos ordinales cualesquiera, se define su multiplicación como sigue:

$$\alpha \cdot \beta = \begin{cases} 0 & \text{si } \beta = 0 \\ (\alpha \cdot (\beta - 1)) + \alpha & \text{si } \beta \text{ es ordinal sucesor} \\ \bigcup\{\alpha \cdot \delta \mid \delta < \beta\} & \text{si } \beta \text{ es ordinal límite} \end{cases}$$

Tenemos las siguientes propiedades para la multiplicación:

- Asociativa: Para tres ordinales cualesquiera α, β y γ, tenemos que
$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$
- Distributiva respecto de la adición: Para tres ordinales cualesquiera α, β y γ, tenemos que
$$\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$$
- La multiplicación NO es conmutativa.
- La propiedad distributiva de la multiplicación respecto de la adición NO se cumple por la derecha.
- Para cualesquiera ordinales $\alpha > 0, \beta$ y β': si $\beta < \beta'$ entonces $\alpha \cdot \beta < \alpha \cdot \beta'$.
- Para cualesquiera ordinales $\alpha > 0, \beta$ y β': si $\alpha \cdot \beta = \alpha \cdot \beta'$ entonces $\beta = \beta'$.
- Para tres ordinales cualesquiera α, α' y β : si $\alpha \leq \alpha'$, entonces $\alpha \cdot \beta \leq \alpha' \cdot \beta$.
- Para un ordinal β y un ordinal límite γ cualesquiera, entonces
$$\gamma \cdot \beta \geq sup\{\delta \cdot \beta \mid \delta < \gamma\}.$$

La exponenciación.

Sean α y β dos ordinales cualesquiera, se define la exponenciación como sigue:

$$\alpha^{\beta} = \begin{cases} 1 & \text{si } \beta = 0 \\ \alpha^{\beta - 1} \cdot \alpha & \text{si } \beta \text{ es ordinal sucesor} \\ \bigcup\{\alpha^{\delta} \mid \delta < \beta\} & \text{si } \beta \text{ es ordinal límite} \end{cases}$$

Tenemos las siguientes propiedades para la exponenciación:

- Para tres ordinales cualesquiera α, β y γ, tenemos que $\alpha^{\beta+\gamma} = \alpha^{\beta} \cdot \alpha^{\gamma}$

- Para tres ordinales cualesquiera α, β y γ, tenemos que $(\alpha^\beta)^\gamma = \alpha^{\beta\cdot\gamma}$
- Para tres ordinales $\alpha > 1$, y $\beta < \beta'$, tenemos que $\alpha^\beta < \alpha^{\beta'}$.
- Para tres ordinales $\alpha > 1$, y β y β', si $\alpha^\beta = \alpha^{\beta'}$, entonces $\beta = \beta'$.
- Para tres ordinales cualesquiera α, α' y β: si $\alpha \leq \alpha'$, entonces $\alpha^\beta \leq \alpha'^\beta$
- Para β ordinal cualquiera y γ ordinal límite, entonces

$$\gamma^\beta \geq sup\{\delta^\beta | \delta < \gamma\}$$

Una vez que conocemos cómo funcionan las operaciones podemos dar una breve descripción del comienzo de la clase de los ordinales:

$0, 1, 2, 3, \ldots, \omega, \omega+1, \omega+2, \ldots, \omega+\omega = \omega\cdot 2, \omega\cdot 2+1, \omega\cdot 2+2, \ldots, \omega\cdot 2+\omega = \omega\cdot 3,$

$\omega\cdot 3+1, \ldots, \omega\cdot 3+\omega = \omega\cdot 4, \ldots, \omega\cdot\omega = \omega^2, \omega^2+1, \ldots, \omega^2+\omega, \omega^2+\omega+1, \ldots,$

$\omega^2+\omega\cdot 2, \ldots, \omega^2+\omega\cdot\omega = \omega^2\cdot 2, \ldots, \omega^3, \ldots, \omega^\omega, \ldots, \omega^{\omega+1}, \ldots, \omega^{\omega\cdot 2}, \ldots, \omega^{\omega^2}, \ldots, \omega^{\omega^\omega}, \ldots$

2.4. Forma Normal de Cantor.

En esta sección vamos a ver el Teorema de la Forma Normal de Cantor que nos será necesario para poder construir las sucesiones de Goodstein. Primero, varios resultados.

Proposición 2.4.1 (División) *Sean α cualquiera y $\beta > 0$ dos ordinales. Entonces, existen γ y δ únicos tales que $\alpha = \beta\cdot\gamma + \delta$, con $\delta < \beta$.*

Demostración: Si $\alpha < \beta$: $\alpha = \beta\cdot 0 + \alpha$.

Si $\alpha \geq \beta$: Sea $\gamma = \sup\{\delta : \beta\cdot\delta \leq \alpha\}$. Entonces, $\gamma \geq 1$ ya que 1 está en el conjunto. Por tanto, γ será ordinal sucesor o límite. Veamos ahora que para todo $\delta < \gamma$, $\beta\cdot\delta \leq \alpha$:

En el caso de que $\beta\cdot\gamma \leq \alpha$ se tiene claramente por la monotonía estricta del producto en el segundo argumento. En el caso de que $\beta\cdot\gamma > \alpha$, si $\beta\cdot\delta > \alpha$, por la monotonía del producto tendríamos que γ no sería el supremo y llegaríamos a contradicción.

Veamos ahora que $\beta\cdot\gamma \leq \alpha$:

Si existe τ tal que $\gamma = \tau + 1$, entonces $\tau < \gamma$ y $\tau \in \{\delta : \beta\cdot\delta \leq \alpha\}$. Por tanto, por fuerza γ debe estar también en el conjunto, ya que si no, τ sería el supremo.

Si γ es ordinal límite: $\beta\cdot\gamma = \bigcup_{\delta<\gamma} \beta\cdot\delta \leq \bigcup_{\delta<\gamma} \alpha = \alpha$.

Como ya podemos afirmar que $\beta\cdot\gamma \leq \alpha$, entonces sabemos que existe δ único tal que $\alpha = \beta\cdot\gamma + \delta$. Si δ fuera mayor o igual que β, existiría μ con $\beta + \mu = \delta$. De esta manera,

$\alpha = \beta \cdot \gamma + \beta + \mu = \beta \cdot (\gamma + 1) + \mu$, con lo que $\beta \cdot (\gamma + 1) \leq \alpha$ y γ no sería el supremo. Así, $\delta < \beta$.

La unicidad la probaremos de la siguiente manera:

Si $\alpha = \beta\gamma_1 + \delta_1$ entonces $\beta\gamma_1 \leq \alpha$, luego $\gamma_1 \leq \gamma$ (recordemos la definición de γ como un supremo).

Si $\beta\gamma_2 \leq \alpha$ y $\gamma_2 > \gamma_1$ entonces, teniendo en cuenta que $\delta_1 < \beta$, resulta

$$\alpha \geq \beta\gamma_2 \geq \beta(\gamma_1 + 1) = \beta\gamma_1 + \beta > \beta\gamma_1 + \delta_1 = \alpha$$

lo cual es absurdo. Por tanto, si $\beta\gamma_2 \leq \alpha$ entonce $\gamma_2 \leq \gamma_1$ lo que (usando la defínción de γ como supremo) prueba que $\gamma_1 = \gamma_2$. Hemos probado así que

$$\beta\gamma_2 + \delta_2 = \alpha = \beta\gamma_1 + \delta_1 = \beta\gamma_2 + \delta_1$$

y por tanto $\delta_2 = \delta_1$. ⊠

Proposición 2.4.2 *Si $\alpha > 1$ y β es un ordinal cualquiera: $\beta \leq \alpha^\beta$.*

Demostración: Por inducción transfinita sobre β.

- $\beta = 0 : 0 \leq \alpha^0 = 1$.
- Suponemos cierto para β: Por hipótesis de inducción y las propiedades de la suma se tiene que $\beta + 1 \leq \alpha^\beta + 1 < \alpha^{\beta+1} + 1$. Así, $\beta + 1 \leq \alpha^{\beta+1}$.
- Supongamos que β es límite y se cumple la propiedad para todo $\gamma < \beta$: Por hipótesis de inducción, $\gamma \subseteq \alpha^\gamma$ para todo $\gamma < \beta$. Por consiguiente,

$$\bigcup\{\gamma | \gamma < \beta\} = \beta \subseteq \bigcup\{\alpha^\gamma | \gamma < \beta\} = \alpha^\beta.$$

Por lo que sigue que $\beta \leq \alpha^\beta$. ⊠

Proposición 2.4.3 *Sean $\alpha > 1$ y $\beta > 0$ dos ordinales cualesquiera. Entonces, existe un único δ tal que $\alpha^\delta \leq \beta < \alpha^{\delta+1}$.*

Demostración: Por la Proposición 2.4.2, $\beta \leq \alpha^\beta < \alpha^{\beta+1}$. Por tanto, el conjunto

$$\mathrm{A} = \{\delta : \beta < \alpha^\delta\} \neq \varnothing$$

y tiene elemento mínimo, sea γ.

Claramente $\gamma \neq 0$, ya que 0 no puede estar en A porque tendría que ser $\beta < \alpha^0 = 1$.

Veamos que γ es sucesor: Supongamos que es un ordinal límite. Entonces, $\alpha^\gamma = \bigcup_{\delta<\gamma} \alpha^\delta$.

Por ser el mínimo de A, para todo $\delta < \gamma$ se cumple que $\alpha^\delta \leq \beta$ o, equivalentemente, $\alpha^\delta \subseteq \beta$. Por tanto, $\bigcup_{\delta<\gamma} \alpha^\delta = \alpha^\gamma \subseteq \beta$ y $\alpha^\gamma \leq \beta$, lo cual no puede ser porque $\gamma \in$ A. De esta manera, podemos afirmar que γ es sucesor.

Sea δ tal que $\gamma = \delta + 1$, entonces $\delta \notin$ A y $\alpha^\delta \leq \beta < \alpha^{\delta+1}$. Con esto queda probada la existencia. Probemos ahora la unicidad:

Supongamos que $\alpha^\delta \leq \beta < \alpha^{\delta+1}$ y $\alpha^\gamma \leq \beta < \alpha^{\gamma+1}$ con $\delta < \gamma$. Entonces, $\delta + 1 \leq \gamma$. Por tanto, $\beta < \alpha^{\delta+1} \leq \alpha^\gamma \leq \beta$ y sería $\beta < \beta$, lo cual es una contradicción y, así, $\delta = \gamma$. ⊠

Teorema 2.4.4 (Forma Normal de Cantor) *Sea $\alpha > 1$. Para todo $\beta > 0$ existen $n \in \omega$ y ordinales $\beta_0, \ldots, \beta_n, \gamma_0, \ldots, \gamma_n$ únicos tales que*

$$\beta = \alpha^{\beta_n} \cdot \gamma_n + \cdots + \alpha^{\beta_0} \cdot \gamma_0$$

con $0 \leq \beta_0 < \beta_1 < \ldots < \beta_n$ y $0 < \gamma_i < \alpha$ para $i = 0, \ldots, n$.

Demostración: Por inducción transfinita (completa) en β.

Por la Proposición 2.4.3, existe un único δ tal que

$$\alpha^\delta \leq \beta < \alpha^{\delta+1} \tag{2.1}$$

Por la Proposición 2.4.1, existen ordinales τ y μ únicos tales que

$$\beta = \alpha^\delta \cdot \tau + \mu \text{ con } \mu < \alpha^\delta \tag{2.2}$$

De (2.1) y (2.2) obtenemos que $\alpha^\delta \leq \alpha^\delta \cdot \tau + \mu < \alpha^{\delta+1}$. Además, veamos que $0 < \tau < \alpha$:

Si $\tau = 0$: $\mu \geq \alpha^\delta$, lo cual es una contradicción.

Si $\tau \geq \alpha$: $\alpha^\delta \cdot \tau + \mu \geq \alpha^{\delta+1} + \mu \geq \alpha^{\delta+1}$, que es una contradicción.

Por tanto, si $\mu = 0$ entonces $\beta = \alpha^\delta \cdot \tau$ y ya tendríamos la Forma Normal de Cantor de β.

Si $\mu > 0$: Claramente $\mu \leq \beta$. Pero al ser $\alpha^\delta \cdot \tau \geq 1$, entonces $\mu < \beta$. Por consiguiente, podemos aplicar la hipótesis de inducción a μ. Podemos encontrar pues $\beta_0, \ldots, \beta_n, \gamma_0, \ldots, \gamma_n$ únicos tales que $\mu = \alpha^{\beta_n} \cdot \gamma_n + \cdots + \alpha^{\beta_0} \cdot \gamma_0$. Si sustituimos en (2.2) obtenemos:

$$\beta = \alpha^\delta \cdot \tau + \alpha^{\beta_n} \cdot \gamma_n + \cdots + \alpha^{\beta_0} \cdot \gamma_0.$$

Con esto y con las propiedades de las operaciones ordinales, podemos asegurar que existe una Forma Normal de Cantor para β.

A continuación, hay que ver la unicidad. Primero, probaremos que si

$$\beta = \alpha^{\beta_n}\gamma_n + \cdots + \alpha^{\beta_0}\gamma_0 \text{ con } \beta_n > \cdots > \beta_0 \text{ y cada } \gamma_j < \alpha,$$

entonces $\alpha^{\beta_n} \leq \beta < \alpha^{\beta_n+1}$.

$\alpha^{\beta_n} \leq \beta$ es obvio mientras que $\beta < \alpha^{\beta_n+1}$ puede probarse fácilmente por inducción: Para $n = 0$ es directo y supuesto para n,tenemos que, aplicando la hipótesis de inducción:

$$\alpha^{\beta_{n+1}}\gamma_{n+1}+\alpha^{\beta_n}\gamma_n+\cdots+\alpha^{\beta_0}\gamma_0 < \alpha^{\beta_{n+1}}\gamma_{n+1}+\alpha^{\beta_n+1} \leq \alpha^{\beta_{n+1}}(\gamma_{n+1}+1) \leq \alpha^{\beta_{n+1}}\alpha = \alpha^{\beta_{n+1}+1}$$

La unicidad de la forma normal se obtiene ahora por inducción completa utilizando la Proposición 2.4.2. ⊠

Capítulo 3

La aritmética de Peano.

3.1. Axiomas y primeros resultados.

Consideremos la estructura algebraica $\mathbb{N} = \langle \mathrm{N}; +, \cdot, 0, 1\rangle$, donde N es el conjunto de los números naturales (enteros no negativos). Esta estructura es el modelo estándar de la teoría de números naturales llamada *Aritmética de Peano* (PA). El lenguaje de esta teoría es el lógico de primer orden con igualdad:

$$\mathcal{L}_{\mathsf{PA}} = \{+, \cdot, \mathbf{0}, \mathbf{1}\},$$

donde $+$ y $\cdot$ son símbolos de función de aridad dos y $\mathbf{0}$ y $\mathbf{1}$ son símbolos de constante. En general, además del modelo estándar se pueden considerar otros modelos de la forma

$$\mathbb{M} = \langle \mathrm{M}; +^{\mathbb{M}}, \cdot^{\mathbb{M}}, \mathbf{0}^{\mathbb{M}}, \mathbf{1}^{\mathbb{M}}\rangle,$$

donde M es el universo; $+^{\mathbb{M}}$ y $\cdot^{\mathbb{M}}$ son dos símbolos de función que resultan de interpretar los símbolos $+$ y $\cdot$ de $\mathcal{L}_{\mathsf{PA}}$. Por convenio, para cualquier modelo $\mathbb{M}$ escribiremos simplemente $+$ y $\cdot$ omitiendo el símbolo del modelo. Igualmente, $\mathbf{0}^{\mathbb{M}}$ y $\mathbf{1}^{\mathbb{M}}$ son dos elementos del universo que resultan de interpretar los símbolos $\mathbf{0}$ y $\mathbf{1}$ de $\mathcal{L}_{\mathsf{PA}}$. De nuevo, simplificaremos la notación y escribiremos 0 y 1 en cualquier modelo en lugar de $\mathbf{0}^{\mathbb{M}}$ y $\mathbf{1}^{\mathbb{M}}$.

De esta manera, los axiomas de PA se definen como los cierres universales de las fórmulas que siguen:

1. Conmutatividad, asociatividad, distributividad y propiedades de los elementos neutros.

$$x + y = y + x,\ x \cdot y = y \cdot x,$$

$$(x + y) + z = x + (y + z),\ (x \cdot y) \cdot z = x \cdot (y \cdot z),$$

$$(x + y) \cdot z = x \cdot z + y \cdot z,$$

$$x + \mathbf{0} = x,\ x \cdot \mathbf{1} = x.$$

2. La ley de la resta.
$$x + z = y + z \to x = y.$$

3. Todo número excepto el cero es un sucesor.
$$x \neq \mathbf{0} \leftrightarrow \exists y[x = y + \mathbf{1}].$$

4. El axioma de inducción. Sea $F(x)$ una fórmula y x una variable:
$$(F(\mathbf{0}) \wedge \forall x[F(x) \to F(x + \mathbf{1})]) \to \forall x F(x).$$

Observemos que para poder aplicar el principio de inducción sobre un conjunto, dicho conjunto tiene que ser definible por una fórmula $F(x)$.

Lema 3.1.1 *Las siguientes fórmulas son teoremas de* PA*:*

1. $x \cdot \mathbf{0} = \mathbf{0}$.
2. $x + y = \mathbf{0} \to x = \mathbf{0}$.

Demostración: Por el Teorema de Completitud de Gödel, la condición $\mathsf{PA} \vdash F$ es equivalente con la validez de la fórmula F en cualquier modelo de PA. Por tanto, consideramos un modelo arbitario $\mathbb{M} = \langle \mathrm{M}; +, \cdot, 0, 1\rangle$.

1. Sea $a \in M$. Aplicando los axiomas tenemos que
$$a + 0 = a = a \cdot 1 = a \cdot (0 + 1) = a \cdot 0 + a \cdot 1 = a \cdot 0 + a.$$
Por tanto, por el axioma de conmutatividad y el de la resta, obtenemos que $a \cdot 0 = 0$. De esta manera, $\mathbb{M} \vDash (a \cdot 0 = 0)$ para todo $a \in \mathrm{M}$.

2. Sean $a, b \in \mathrm{M}$ con $a \neq 0$. Entonces, $a = a_0 + 1$ para algún $a_0 \in \mathrm{M}$ de acuerdo con el tercer axioma. De esta manera, $a + b = a_0 + 1 + b = a_0 + b + 1$, por lo que $a + b$ es un sucesor y no puede ser 0. ⊠

3.2. El orden.

El orden usual $\leq$ de $\mathbb{N}$ se puede caracterizar por la equivalencia

$$n \leq m \leftrightarrow \exists k \in \mathrm{N}\ [n + k = m] \ \text{ para } n, m \in \mathrm{N}.$$

Además,
$$n < m \leftrightarrow \exists k \in \mathrm{N}\ [n + k + 1 = m] \ \text{ para } n, m \in \mathrm{N}.$$

Vamos a introducir en PA el nuevo símbolo $\leq$ que definimos como sigue:

$$\forall x, y[x \leq y \leftrightarrow \exists z(x + z = y)]$$

Además,
$$x < y \leftrightarrow x \leq y \wedge x \neq y$$

Teorema 3.2.1 *La fórmula $x \leq y$ define un orden lineal del universo, es decir, los cierres universales de las siguientes fórmulas son teoremas de* PA.

1. $x \leq x$.
2. $(x \leq y \wedge y \leq x) \to x = y$.
3. $(x \leq y \wedge y \leq z) \to x \leq z$.
4. $x \leq y \vee y \leq x$.

Demostración: Sea $\mathbb{M}$ un modelo arbitrario de PA.

1. Para $a \in \mathrm{M}$ cualquiera tenemos $a + 0 = a$, de lo que sigue $a \leq a$.
2. Supongamos que $a \leq b$ y $b \leq a$ para $a, b \in \mathrm{M}$ cualesquiera. Entonces existen $u, w \in \mathrm{M}$ tales que $a + u = b$ y $b + w = a$. Así, $a + u + w = a$. Por el axioma de la resta, $u + w = 0$ y por el Lema 3.1.1 $u = 0$. Por tanto, $a = b$.
3. Supongamos que $a \leq b$ y $b \leq c$ para $a, b, c \in \mathrm{M}$ cualesquiera. Entonces existen $u, w \in \mathrm{M}$ tales que $a + u = b$ y $b + w = c$. Por tanto, $a + u + w = c$ y $a \leq c$.
4. Por inducción: Sea $F(x, y)$ la fórmula $x \leq y \vee y \leq x$.

   Sea $a \in \mathrm{M}$ arbitrario pero fijo. Como $0 + a = a$, $0 \leq a$ y $\mathbb{M} \vDash F(a, 0)$.

   Supongamos ahora que $\mathbb{M} \vDash F(a, b)$ para un $b \in \mathrm{M}$ cualquiera. Entonces tenemos $a \leq b \vee b \leq a$.

   Si $a \leq b$: Como claramente $b \leq b + 1$, entonces $a \leq b + 1$.

   Si $b \leq a$: Existe $u \in \mathrm{M}$ tal que $b + u = a$. Si $u = 0$, entonces $b = a$ y $a \leq b + 1$. Si $u > 0$, entonces $u = w + 1$ para algún $w \in \mathrm{M}$ y $b + w + 1 = a$. Por tanto, $b + 1 \leq a$.

   En todo caso vemos que se cumple $\mathbb{M} \vDash F(a, b + 1)$. ⊠.

Veamos ahora algunas propiedades simples de $\leq$.

Lema 3.2.2 *En* PA *se satisface lo siguiente:*

$$\forall x(\mathbf{0} \leq x).$$

⊠

Lema 3.2.3 *En* PA *se satisface lo siguiente:*

$$\mathbf{0} < \mathbf{1}.$$

Demostración: Sea $\mathbb{M}$ un modelo arbitrario de PA. Ya sabemos que $0 \leq 1$. Supongamos que $0 = 1$. Entonces, $0 + 1 = 1 = 0$ y 0 sería sucesor, lo cual está en contradicción con uno de los axiomas. ⊠

Lema 3.2.4 *No hay elementos intermedios entre un elemento y su sucesor. Es decir:*

$$\mathsf{PA} \vdash \forall x, y((x < y + \mathbf{1}) \leftrightarrow (x \leq y)).$$

Demostración: Para un modelo cualquiera $\mathbb{M}$, con $a, b \in \mathrm{M}$ cualesquiera se tiene que

$$a < b + 1 \leftrightarrow \exists w(w \in M \wedge a + w + 1 = b + 1) \leftrightarrow \exists w(w \in M \wedge a + w = b) \leftrightarrow a \leq b.$$

⊠

Teorema 3.2.5 (Inducción completa) *Para toda fórmula F se cumple lo siguiente:*

$$\mathsf{PA} \vdash \forall x[(\forall y < xF(y)) \rightarrow F(x)] \rightarrow \forall xF(x).$$

Demostración: Sea $G(x)$ la fórmula $\forall y \leq xF(y)$. Sea $\mathbb{M}$ un modelo arbitrario de PA. Supongamos que se cumple

$$\mathbb{M} \vDash \forall x[(\forall y < xF(y)) \rightarrow F(x)]. \tag{3.1}$$

Sea $Z = \{a \in \mathrm{M} : \mathbb{M} \vDash G(a)\}$. De (3.1) sigue que $\mathbb{M} \vDash F(0)$. Por tanto, también se cumple $\mathbb{M} \vDash G(0)$, con lo que $0 \in Z$.

Supongamos que $a \in Z$: $\mathbb{M} \vDash F(b)$ para todo $b \leq a$. Por tanto, por (3.1), tenemos que $\mathbb{M} \vDash F(a + 1)$. Con lo que $G(a + 1)$ se satisface también. Así, $a + 1 \in Z$ y $Z = \mathrm{M}$ por el axioma de inducción. Por consiguiente, $\mathbb{M} \vDash \forall xF(x)$. ⊠.

Teorema 3.2.6 (Esquema del mínimo) *Para toda fórmula F se cumple lo siguiente:*

$$\mathsf{PA} \vdash \exists xF(x) \rightarrow \exists x[F(x) \wedge \forall y < x \neg F(y)]$$

Demostración: Supongamos que se cumple la negación del consecuente de la implicación, es decir,

$$\forall x[\neg F(x) \vee \neg(\forall y < x \neg F(y))]$$

Entonces, por equivalencia lógica se cumple que

$$\forall x[(\forall y < x \neg F(y)) \rightarrow \neg F(x)]$$

Aplicando el Teorema 3.2.5 a $\neg F$ obtenemos

$$\forall x[(\forall y < x \neg F(y)) \rightarrow \neg F(x)] \rightarrow \forall x \neg F(x),$$

que nos da la negación del antecedente de la implicación que queríamos demostrar. ⊠

Lema 3.2.7 $\mathsf{PA} \vdash (x \leq y \rightarrow \exists! z(x + z = y))$.

Demostración: Sea $\mathbb{M}$ un modelo dado y $a, b, u, w \in \mathrm{M}$ tales que $a + u = b = a + w$, entonces $u = w$. ⊠

Podemos introducir, por tanto, la **resta** como una operación $y - x$ en PA:

$$(y - x = z) \leftrightarrow ((x \leq y \wedge x + z = y) \vee (x > y \wedge z = \mathbf{0}))$$

A continuación, vamos a introducir también el **valor absoluto**:

$$(|x - y| = z) \leftrightarrow ((x \leq y \wedge x + z = y) \vee (y \leq x \wedge y + z = x)).$$

3.3. Numerales.

Los numerales son términos de la teoría PA que definimos por inducción para $n \in \mathbb{N}$ como:

- $\Lambda_0 = \mathbf{0}$.
- $\Lambda_1 = \mathbf{1}$.
- $\Lambda_{n+1} = \Lambda_n + \mathbf{1}$.

Es decir, para un $n > 0$, el numeral Λ_n será $\mathbf{1} + \cdots + \mathbf{1}$ n veces.

En particular, en el modelo estándar $\mathbb{N}$, el término Λ_n corresponde al número natural n. Veamos ahora algunas propiedades:

Lema 3.3.1 $\mathsf{PA} \vdash (\Lambda_n + \Lambda_m = \Lambda_{n+m})$

Demostración: Por inducción en m.

$$\Lambda_n + \Lambda_0 = \Lambda_n.$$

Supongamos que $\Lambda_n + \Lambda_m = \Lambda_{n+m}$. Entonces,

$$\Lambda_n + \Lambda_{m+1} = \Lambda_n + (\Lambda_m + \Lambda_1) = \Lambda_{n+m} + \Lambda_1 = \Lambda_{n+m+1}.$$

⊠

Lema 3.3.2 $\mathsf{PA} \vdash (\Lambda_n \cdot \Lambda_m = \Lambda_{n \cdot m})$

Demostración: Por inducción en m.

$$\Lambda_n \cdot \Lambda_0 = \Lambda_0.$$

Supongamos que $\Lambda_n \cdot \Lambda_m = \Lambda_{n \cdot m}$. Entonces,

$$\Lambda_n \cdot \Lambda_{m+1} = \Lambda_n \cdot (\Lambda_m + \Lambda_1) = \Lambda_n \cdot \Lambda_m + \Lambda_n \cdot \Lambda_1 = \Lambda_{n \cdot m} + \Lambda_n = \Lambda_{n \cdot m + n} = \Lambda_{n \cdot (m+1)}.$$

⊠

Lema 3.3.3 $\mathsf{PA} \vdash \forall x (x \leq \Lambda_n \to x = \Lambda_0 \vee \cdots \vee x = \Lambda_n)$.

Demostración: Por inducción en n.

Si $x \leq \Lambda_0$, como $x \geq \Lambda_0$ debe ser $x = \Lambda_0$.

Supongamos que se cumple para Λ_n. Si $x \leq \Lambda_{n+1}$, entonces se cumple que $x < \Lambda_{n+1} \vee x = \Lambda_{n+1}$. Según el Lema 3.2.4, ésto equivale a $x \leq \Lambda_n \vee x = \Lambda_{n+1}$. Por tanto, por hipótesis de inducción, $x = \Lambda_0 \vee \cdots \vee x = \Lambda_n \vee x = \Lambda_{n+1}$. ⊠

Capítulo 4

Funciones Σ_1-definibles y funciones demostrablemente totales.

4.1. Funciones Σ_1-definibles en $\mathbb{N}$.

Definición 4.1.1 *Sean F(x) y t una fórmula y un término del lenguaje $\mathcal{L}_{\mathsf{PA}}$ tales que t no contiene a la variable x.*

1. *La fórmula definida por cuantificación existencial acotada a partir de F y t es la fórmula $\exists x(x \leq t \wedge F(x))$. Para referirnos a esta fórmula utilizaremos la notación $\exists x \leq tF(x)$ y la expresión $\exists x \leq t$ se denomina cuantificador existencial acotado.*

2. *La fórmula definida por cuantificación universal acotada a partir de F y t es la fórmula $\forall x(x \leq t \rightarrow F(x))$. Para referirnos a esta fórmula utilizaremos la notación $\forall x \leq tF(x)$ y la expresión $\forall x \leq t$ se denomina cuantificador universal acotado.*

Definición 4.1.2 *Decimos que una fórmula está **acotada** si pertenece a la menor clase de fórmulas que contiene a las fórmulas atómicas y que es cerrada bajo conectivas lógicas y bajo cuantificación acotada.*

Definición 4.1.3 *A las fórmulas de la forma $\exists xF$ donde F es una fórmula acotada las llamaremos Σ_1-fórmulas. A la clase que contiene a todas las Σ_1-fórmulas la llamaremos Σ_1. Además, si una Σ_1-fórmula F_f define una función $f : N^k \rightarrow N$, es decir,*

$$f(x_1, \ldots, x_k) = y \Leftrightarrow \mathbb{N} \vDash F_f(x_1, \ldots, x_k, y)$$

diremos que la función f es Σ_1-definible.

A continuación vamos a ver unos ejemplos de funciones Σ_1-definibles importantes:

1. Las *funciones polinómicas*. Una función $f : N^k \rightarrow N$ es polinómica si existe un término $t(x_1, \ldots, x_k)$ de $\mathcal{L}_{\mathsf{PA}}$ tal que para todo $n_1, \ldots, n_k, m \in \mathbb{N}$ se tiene:

$$f(n_1, \ldots, n_k) = m \Leftrightarrow \mathbb{N} \vDash t(n_1, \ldots, n_k) = m.$$

Por tanto, por estar definida por una fórmula atómica es Σ_1-definible (téngase en cuenta que las fórmulas acotadas son equivalentes a una fórmula Σ_1).

2. Las funciones *cociente* y *resto*. Sean $q(a,b)$ y $r(a,b)$ el cociente y resto de dividir a entre b, con $a, b \in N$. Entonces, si $b \neq 0$ tenemos $a = b \cdot q(a,b) + r(a,b)$ con $r(a,b) < b$. Además, establecemos que $q(a,0) = 0$ y $r(a,0) = 0$. Veamos que ambas son Σ_1-definibles. Dados $a, b, c \in N$ se tiene:

   $q(a,b) = c \Leftrightarrow \mathbb{N} \vDash F(a,b,c)$, siendo $F(x,y,z)$ la siguiente fórmula acotada (y, por tanto, Σ_1):

   $$(y = \mathbf{0} \wedge z = \mathbf{0}) \vee [y \neq \mathbf{0} \wedge \exists v < y(x = y \cdot z + v)].$$

   $r(a,b) = c \Leftrightarrow \mathbb{N} \vDash G(a,b,c)$, siendo $G(x,y,z)$ la siguiente fórmula acotada (y, por tanto, Σ_1):

   $$(y = \mathbf{0} \wedge z = \mathbf{0}) \vee [y \neq \mathbf{0} \wedge \exists u \leq x(x = y \cdot u + z \wedge z < y)].$$

3. La función $J : N \times N \to N$. Es una función biyectiva (aunque no lo probaremos aquí) que se define de la siguiente manera:

   $$J(x,y) = z \Leftrightarrow \mathbb{N} \vDash 2 \cdot z = (x+y) \cdot (x+y+1) + 2 \cdot x$$

   Al ser biyectiva, existen además dos funciones que componen la *inversa* de J. Es decir, existen $K : N \to N$ y $L : N \to N$ tales que:

   $$J(x,y) = z \Leftrightarrow K(z) = x \wedge L(z) = y.$$

   Las siguientes fórmulas acotadas definen a K y L:

   $$\exists x \leq z[\Lambda_2 \cdot z = (x+y) \cdot (x+y+\Lambda_1) + \Lambda_2 \cdot x].$$
   $$\exists y \leq z[\Lambda_2 \cdot z = (x+y) \cdot (x+y+\Lambda_1) + \Lambda_2 \cdot x].$$

Lema 4.1.4 *Sea F una fórmula acotada. Entonces, la fórmula $\exists x_1, \ldots, \exists x_k F$ es equivalente a una Σ_1-fórmula.*

Demostración: Por inducción en k.

Si $k = 1$ se cumple obviamente por definición de Σ_1-fórmula.

Supongamos que se cumple para cierto k. Entonces, existe una fórmula acotada F' tal que:

$$\mathbb{N} \vDash \exists x_1, \ldots, \exists x_k F \Leftrightarrow \exists y F'$$

Se tiene entonces que:

$$\mathbb{N} \vDash \exists x_1, \ldots, \exists x_k \exists x_{k+1} F \Leftrightarrow \exists y \exists x_{k+1} F'$$

Por la biyectividad de la función J, sea $z \in N$ tal que $J(y, x_{k+1}) = z$, entonces

$$\mathbb{N} \vDash \exists y \exists x_{k+1} F' \Leftrightarrow \exists z[y = K(z) \wedge x_{k+1} = L(z) \wedge F'],$$

donde $'y = K(z)'$ y $'x_{k+1} = L(z)'$ son reemplazadas por sus fórmulas acotadas correspondientes y se obtiene una Σ_1-fórmula. De esta manera, se cumple para todo k. ⊠

Lema 4.1.5 *Sea $F(x, y)$ una fórmula acotada. Entonces:*

$$\mathbb{N} \vDash \forall x \leq u \exists y F(x, y) \Leftrightarrow \exists w \forall x \leq u \exists y \leq w F(x, y).$$

Como consecuencia, la clase Σ_1 es cerrada bajo cuantificación universal acotada.

Demostración: La implicación de derecha a izquierda es trivial. Veamos la contraria. Sea $u \in N$ tal que $\mathbb{N} \vDash \forall x \leq u \exists y F(x, y)$. Tomemos entonces para cada $j \leq u$ un $k_j \in \mathbb{N}$ tal que $\mathbb{N} \vDash F(j, k_j)$. Entonces, sea k el máximo de $\{k_0, \ldots, k_u\}$. Se satisface lo siguiente:

$$\mathbb{N} \vDash \forall x \leq u \exists y \leq k F(x, y).$$

⊠

A la clase de las funciones Σ_1-definibles la denotamos por $\mathcal{F}\Sigma_1(\mathbb{N})$.

Lema 4.1.6 *$\mathcal{F}\Sigma_1(\mathbb{N})$ es cerrada bajo composición.*

Demostración: Si una fórmula $F(y_1, \ldots, y_k, y)$ define una función f y $G_i(x_1, \ldots, x_l, y_i)$ definen funciones g_i para $i = 1, \ldots, k$, entonces la fórmula

$$\exists y_1, \ldots, y_k[G_1(x_1, \ldots, x_l, y_1) \wedge \cdots \wedge G_k(x_1, \ldots, x_l, y_k) \wedge F(y_1, \ldots, y_k, y)]$$

define la composición $f(g_1, \ldots, g_k)$. Por tanto, si $F, G_1, \ldots, G_k \in \Sigma_1$, dicha fórmula es equivalente a una Σ_1-fórmula y la función $f(g_1, \ldots, g_k)(x_1, \ldots, x_l)$ es de la clase $\mathcal{F}\Sigma_1(\mathbb{N})$. ⊠

Antes de introducir el siguiente Teorema debemos indicar que para cualesquiera $a, b, m \in N$, diremos que $a \equiv b \mod m$ sii $r(a, m) = r(b, m)$ sii $\exists u(a - b = m \cdot u)$. Esto último lo denotaremos como $m|(a - b)$ y diremos que m divide a $a - b$.

Teorema 4.1.7 (Teorema Chino del Resto) *Sean $m_0, \ldots, m_k \in N$ coprimos dos a dos. Entonces, para cualesquiera $a_0, \ldots, a_k \in N$ el sistema de congruencias*

$$x \equiv a_i \mod m_i \text{ para } i = 0, \ldots, k$$

tiene una solución $x \in N$ con $x < m_0 \cdots m_k$.

Demostración: Procedemos por inducción en k.

Si $k = 0 : x = r(a_0, m_0)$.

Supongamos que tenemos una solución x del sistema para un cierto $k > 0$. Bastará entonces con encontrar y que satisfaga

$$\begin{aligned} y &\equiv x \quad \text{mod } m' \\ y &\equiv a_{k+1} \quad \text{mod } m \end{aligned}$$

donde $m' = m_0 \cdots m_k$ y $m = m_{k+1}$.

En efecto, si $y \equiv x \bmod m'$, entonces $m'|(y-x)$, por lo que $m_i|(y-x)$ para $i = 0, \ldots, k$. Por tanto, $y \equiv x \equiv a_i \bmod m_i$ para $i = 0, \ldots, k$.

Por hipótesis, tenemos que m' y m son coprimos. Por tanto, existen $u, w \in$ N tales que $|um' - wm| = 1$ por la Identidad de Bezout. Supongamos que $um' - wm = 1$ (para el otro caso es similar). Entonces se tiene:

$$\begin{aligned} um' &\equiv 1 \quad \text{mod m} \\ (um' - w)m &\equiv 1 \quad \text{mod m}' \end{aligned}$$

Multiplicando ambas congruencias se obtiene:

$$\begin{aligned} um'a_{k+1} &\equiv a_{k+1} \quad \text{mod m} \\ (um' - w)mx &\equiv x \quad \text{mod m}' \end{aligned}$$

Y, por último, $y = um'a_{k+1} + (um' - w)mx$ es solución del sistema como puede comprobarse fácilmente. Como buscamos una solución menor que $m' \cdot m$, podemos escoger entonces $r(y, m'm)$.

En efecto, para un cierto $q \in$ N se tiene que $y = qm'm + r(y, m'm)$. Así, $m'|(y - r(y, m'm))$ y por tanto $y \equiv r(y, m'm) \bmod m'$. Para m se hace de manera similar. ⊠

Definición 4.1.8 *$\beta(a, b, i) = r(a, (i + 1)b + 1)$ para a,b,i $\in$ N.*

Proposición 4.1.9 *Para toda sucesión finita $\langle a_0, \ldots, a_n \rangle$ de números naturales existen $a, b \in N$ tales que $\beta(a, b, i) = a_i$ para todo $i = 0, \ldots, n$.*

Demostración: Sea $m =$máx$\{n, a_0, \ldots, a_n\}$ y sea $b = m!$. Entonces, es fácil comprobar que los números $m_i = (i + 1)b + 1$ son coprimos dos a dos para $i = 0, \ldots, n$.

Por el Teorema Chino del Resto, existe $a < m_0 \cdots m_n = \prod_{i \leq n} [(i + 1)b + 1]$ tal que $a \equiv a_i \bmod m_i$ para $i = 0, \ldots, n$. Como $a_i \leq m \leq b < m_i \; \forall i \leq n$, tenemos que $r(a, m_i) = a_i$ para $i = 0, \ldots, n$. Es decir, $\beta(a, b, i) = a_i$ para $i = 0, \ldots, n$. ⊠

Teorema 4.1.10 *Sean g y h funciones Σ_1-definibles y sea f la función definida por recursión primitiva como sigue:*

$$f(0, n_1, \ldots, n_k) = g(n_1, \ldots, n_k)$$
$$f(n+1, n_1, \ldots, n_k) = h(f(n, n_1, \ldots, n_k), n, n_1, \ldots, n_k),$$

entonces f es Σ_1-definible.

Demostración: Sean F_g y F_h las Σ_1-fórmulas que definen g y h respectivamente. La condición $f(n, n_1, \ldots, n_k) = m$ es equivalente a que exista una sucesión finita $\langle a_0, \ldots, a_n\rangle$ tal que $a_0 = g(n_1, \ldots, n_k)$, $a_n = m$ y para todo $i < n$, $a_{i+1} = h(a_i, i, n_1, \ldots, n_k)$.

Además, tenemos que

$$a_0 = g(n_1, \ldots, n_k) \Leftrightarrow \mathbb{N} \vDash F_g(n_1, \ldots, n_k, a_0) \text{ y}$$

$$a_{i+1} = h(a_i, i, n_1, \ldots, n_k) \Leftrightarrow \mathbb{N} \vDash F_h(n_1, \ldots, n_k, i, a_i, a_{i+1}).$$

La existencia de los $a_0, \ldots, a_n$ es, por la **Proposición 4.1.9**, equivalente a la existencia de $a, b \in N$ tales que $\beta(a, b, i) = a_i$ para $i = 0, \ldots, n$. Pero la función β es Σ_1-definible mediante la fórmula acotada $\Gamma(a, b, i, c)$:

$$\exists q \leq a\{a = q \cdot [(i + \mathbf{1}) \cdot b + \mathbf{1}] + c \wedge c < (i + \mathbf{1}) \cdot b + \mathbf{1}\}$$

Por tanto, $\beta(a, b, i) = c \Leftrightarrow \mathbb{N} \vDash \Gamma(a, b, i, c)$.

De esta manera, $f(n, n_1, \ldots, n_k) = m \Leftrightarrow \mathbb{N} \vDash F(n_1, \ldots, n_k, n, m)$, donde $F(x_1, \ldots, x_k, x, y)$ es la fórmula:

$\exists a, b\{\exists z \leq a[F_g(x_1, \ldots, x_k, z) \wedge \Gamma(a, b, \mathbf{0}, z)] \wedge \Gamma(a, b, x, y) \wedge$
$\wedge \forall i < x \exists u, w \leq a[\Gamma(a, b, i, u) \wedge \Gamma(a, b, i + \mathbf{1}, w) \wedge F_h(x_1, \ldots, x_k, i, u, w)]\}$.

Gracias al Lema 4.1.5, es sencillo comprobar que F es equivalente a una Σ_1-fórmula. ⊠

Definición 4.1.11 *La clase de las funciones **primitivas recursivas** es la menor clase que contiene a las funciones polinómicas y es cerrada bajo composición y bajo definición por recursión primitiva. Denotamos por* PR *a la clase de las funciones primitivas recursivas.*

Definición 4.1.12 *Sea g una función tal que $\forall n_1, \ldots, n_k \exists m(g(m, n_1, \ldots, n_k) = 0)$. Sea f la función definida como sigue:*

$$f(n_1, \ldots, n_k) = \mathit{mín}\{m : g(m, n_1, \ldots, n_k) = 0\}.$$

Decimos que f está definida por minimización a partir de g.

Si cerramos la clase PR bajo minimización obtenemos una clase mayor: la clase de las funciones **recursivas totales**.

Proposición 4.1.13 *Toda función recursiva es Σ_1-definible.*

Demostración: Las funciones polinómicas son claramente Σ_1-definibles. Ya vimos también que la clase $\mathcal{F}\Sigma_1(\mathbb{N})$ es cerrada bajo composición (Lema 4.1.6) y bajo definición por recursión primitiva (Teorema 4.1.10). Por tanto, quedaría ver que $\mathcal{F}\Sigma_1(\mathbb{N})$ es cerrada bajo minimización y ya estaría probado que la clase de las funciones recursivas totales está contenida en $\mathcal{F}\Sigma_1(\mathbb{N})$.

Sea g una función Σ_1-definible tal que $\forall n_1, \ldots, n_k \exists m(g(m, n_1, \ldots, n_k) = 0)$ y sea G la Σ_1-fórmula tal que

$$g(m, n_1, \ldots, n_k) = u \Leftrightarrow \mathbb{N} \vDash G(m, n_1, \ldots, n_k, u).$$

Sea f la función definida por minimización a partir de g. Entonces:

$$f(n_1, \ldots, n_k) = n \Leftrightarrow \mathbb{N} \vDash G(n, n_1, \ldots, n_k, 0) \wedge \forall m < n \neg G(m, n_1, \ldots, n_k, 0) \tag{4.1}$$

Observemos que:

$$\forall m < n \neg G(m, n_1, \ldots, n_k, 0) \Leftrightarrow \forall m < n \neg \forall z(G(m, n_1, \ldots, n_k, z) \rightarrow z = 0) \Leftrightarrow$$
$$\forall m < n \exists z(G(m, n_1, \ldots, n_k, z) \wedge z \neq 0),$$

lo cual es equivalente a una Σ_1-fórmula por los lemas 4.1.5 y 4.1.4. En consecuencia, (4.1) también es Σ_1. ⊠

4.2. Funciones demostrablemente totales en PA.

Definición 4.2.1 *Decimos que una función $f : N^k \to N$ es **demostrablemente total** en* PA *si hay una Σ_1-fórmula $F_f(x_1, \ldots, x_k, y)$ tal que:*

1. *Para todo $n_1, \ldots, n_k, m \in N$: $f(n_1, \ldots, n_k) = m \Leftrightarrow \mathbb{N} \vDash F_f(n_1, \ldots, n_k, m)$.*
2. *$\mathsf{PA} \vdash \forall x_1, \ldots, x_k \exists! y F_f(x_1, \ldots, x_k, y)$.*

Lema 4.2.2 *La composición de funciones demostrablemente totales es una función demostrablemente total.*

Demostración: Si a las funciones $f, g_1, \ldots, g_k$ corresponden las fórmulas totales definitorias $F_f, F_{g_1}, \ldots, F_{g_k}$, entonces la composición $f(g_1, \ldots, g_k)$ es definible por la fórmula $F(x_1, \ldots, x_l, y)$ siguiente:

$$\exists y_1, \ldots, y_k [F_{g_1}(x_1, \ldots, x_l, y_1) \wedge \cdots \wedge F_{g_k}(x_1, \ldots, x_l, y_k) \wedge F_f(y_1, \ldots, y_k, y)].$$

$F(x_1, \ldots, x_l, y)$ es Σ_1 por el Lema 4.1.6 y es inmediato verificar que es demostrablemente total. ⊠

Lema 4.2.3 *La función β es demostrablemente total.*

Demostración: Bastará con probar el *Teorema de división con resto* en PA:

$$\mathsf{PA} \vdash \forall a, b[b \neq \mathbf{0} \rightarrow \exists! q, r(a = q \cdot b + r \wedge r < b)].$$

Efectivamente, sea $\mathbb{M}$ un modelo arbitrario, $b \in \mathrm{M}$ con $b \neq 0$ y sea

$$Y = \{a \in M : \exists! q, r(a = q \cdot b + r \wedge r < b)\}.$$

$0 \in Y$: con $q = r = 0$ claramente.

Supongamos que $a \in Y$: entonces, $a + 1 = q \cdot b + r + 1$ con q, r únicos. Como $r < b$, entonces $r + 1 \leq b$. Si $r + 1 < b$ ya lo tenemos, y si $r + 1 = b$, entonces $a + 1 = (q + 1)b$.

Por lo tanto, $Y = M$, la función *resto* es total y en consecuencia β también lo es. $\boxtimes$.

Lema 4.2.4 *Sea $G(x, y)$ la fórmula $\forall z[z|x \wedge z|y \rightarrow z = \mathbf{1}]$, donde $z|x$ denota la fórmula $\exists u > 0[x = z \cdot u]$. Claramente, se tiene que $\mathbb{N} \vDash G(a, b)$ sii a y b son primos entre sí.*

Entonces, se cumple la siguiente propiedad:

$$\mathsf{PA} \vdash \forall x_1, x_2, y[G(x_1, y) \wedge G(x_2, y) \rightarrow G(x_1 \cdot x_2, y)]$$

Demostración: Sea $\mathbb{M}$ un modelo arbitrario y $m_1, m_2 \in \mathrm{M}$ tales que $0 < m_2 < m_1$. Sea d el menor elemento z tal que:

$$\exists u \leq m_1 \exists v \leq m_1(u \neq 0 \wedge v \neq 0 \wedge m_2 v < m_1 u \wedge z = m_1 u - m_2 v).$$

Veamos que $d = mcd(m_1, m_2)$:

1. $d|m_1$: Por el Teorema de división con resto, existen q y r tales que $m_1 = d \cdot q + r$ con $r < d$. Puesto que $d < m_1$ como puede observarse fácilmente, entonces $q > 0$. Si $r > 0$ se tiene que:

   $$r = m_1 - dq = m_1 - (m_1 u - m_2 v)q = m_1(1 + em_2 - uq) - m_2(m_1 e - vq),$$

   siendo e el menor elemento tal que $1 + em_2 \geq uq$ y $m_1 e \geq vq$. Entonces, es fácil ver que $1 + m_2 e - uq \leq m_1$ (por reducción al absurdo y por la propia definición de e) y que $m_1 e - vq \leq m_1$ (de manera análoga). Por tanto, se produce una contradicción ya que $r < d$.

2. Análogamente se prueba que $d|m_2$.

3. Si $k|m_1$ y $k|m_2$ entonces $k|d$, ya que existirían q_1 y q_2 tales que

   $$d = um_1 - vm_2 = uq_1 k - vq_2 k = (uq_1 - vq_2)k$$

Supongamos ahora que para cierto $m \in \mathrm{M}$, $\mathbb{M} \vDash G(m_1, m) \wedge G(m_2, m)$. Entonces tenemos que:

$$mcd(m_1, m) = 1 \wedge mcd(m_2, m) = 1$$

Supongamos que $m_2 < m_1 < m < m_1 m_2$ (otras disposiciones respecto al orden se tratarían de manera similar). Entonces, existen $u, v, u', v' \in \mathrm{M}$ y menores o iguales que m tales que :

$$1 = um - vm_1 \qquad \text{y} \qquad 1 = u'm - v'm_2$$

Multiplicando ambas expresiones obtendríamos:

$$1 = vv'm_1m_2 - (uv'm_2 + u'vm_1 - uu'm)m.$$

Por tanto, $mcd(m_1m_2, m) = 1$, es decir, $\mathbb{M} \vDash G(m_1m_2, m)$. ⊠

Con el siguiente lema veremos que se puede expresar el *Teorema Chino del Resto* en un modelo $\mathbb{M}$ de PA cualquiera.

Lema 4.2.5 *Si $\varphi, \psi : \mathrm{M} \to \mathrm{M}$ son funciones definibles en $\mathbb{M}$ tales que $mcd(\psi(i), \psi(j)) = 1$ para $i \neq j$. Entonces, para todo $l \in \mathrm{M}$ existe $a \in \mathrm{M}$ tal que $a \equiv \varphi(i)$ mod $\psi(i)$ para todo $i \leq l$.*

Demostración: Consideremos el siguiente conjunto definible:

$$Y = \{l \in \mathrm{M} : \exists a \forall i \leq l (a \equiv \varphi(i) \bmod \psi(i))\}.$$

- $0 \in Y$: para $a = \varphi(0)$.
- Supongamos que $l \in Y$: Sea a_l una solución correspondiente a l. Primero, debemos probar que existe $m' \in \mathrm{M}$ tal que $\psi(i) | m'$ $\forall i \leq l$ y $mcd(m', m) = 1$ con $m = \psi(l+1)$.

  Para ello, consideramos el siguiente conjunto definible

  $Z = \{l \in M : \forall w[\forall i \leq l \ \mathrm{mcd}(\psi(i), w) = 1 \to \exists m' \forall i \leq l (\psi(i) | m') \wedge (mcd(m', w) = 1)]\}$.

  - $0 \in Z$: para $m' = \psi(0)$.
  - Si $l \in Z$: Sea w tal que $\forall i \leq l + 1$ $\mathrm{mcd}(\psi(i), w) = 1$. Por hipótesis de inducción, como w es coprimo con $\psi(0), \ldots, \psi(l)$, existe m'_l que es divisible entre $\psi(0), \ldots, \psi(l)$ y tal que $\mathrm{mcd}(m'_l, w) = 1$. Por tanto, en virtud del **Lema 4.2.4**, $m' = m'_l \cdot \psi(l+1)$ es el elemento correspondiente a $l+1$ y $l+1 \in Z$. Así, $Z = M$.

  Una vez probado que existe m' con esas características, lo escogemos de manera que $\psi(i) | m'$ con $i \leq l$ y $\mathrm{mcd}(m', m) = 1$. Recordemos que $m = \psi(l+1)$, que es coprimo con $\psi(0), \ldots, \psi(l)$.

Por hipótesis de inducción, $a_l \equiv \varphi(i) \bmod \psi(i)$ para todo $i \leq l$. Por tanto, basta con encontrar una solución del sistema:

$$\begin{aligned} y &\equiv a_l && \bmod \mathrm{m}' \\ y &\equiv \varphi(l+1) && \bmod \mathrm{m} \end{aligned} \tag{4.2}$$

Efectivamente, si $y \equiv a_l \bmod m'$, entonces $m'|(y - a_l)$. Como $\psi(i)|m'$ para $i \leq l$, se tiene que $\psi(i)|(y - a_l)$ para $i \leq l$ e $y \equiv a_l \equiv \varphi(i) \bmod \psi(i)$ para $i \leq l$.

Como $\mathrm{mcd}(m', m) = 1$, entonces (por la prueba del **Lema 4.2.4**) existen $u, w \in \mathrm{M}$ tales que $|um' - wm| = 1$. Supongamos que $um' - wm = 1$ (para el otro caso se procede de manera similar). Entonces, se tiene:

$$\begin{aligned} um' &\equiv 1 && \bmod m \\ (um' - w)m &\equiv 1 && \bmod m' \end{aligned}$$

Multiplicando ambas congruencias obtenemos:

$$\begin{aligned} um'\varphi(l+1) &\equiv \varphi(l+1) && \bmod m \\ (um' - w)ma_l &\equiv a_l && \bmod m' \end{aligned}$$

Y, por último, $y = um'\varphi(l+1) + (um' - w)ma_l$ es solución del sistema (4.2) como puede comprobarse fácilmente. Por lo tanto, $l + 1 \in Y$ e $Y = M$. ⊠.

Teorema 4.2.6 *Toda función $f \in PR$ es demostrablemente total.*

Demostración: Ya sabemos que las funciones polinómicas y la composición de funciones demostrablemente totales son funciones demostrablemente totales. Por tanto, tenemos que probar que si g y h son funciones demostrablemente totales y f está definida por recursión primitiva de la siguiente manera:

$$\begin{aligned} f(0, n_1, \ldots, n_k) &= g(n_1, \ldots, n_k) \\ f(n+1, n_1, \ldots, n_k) &= h(f(n, n_1, \ldots, n_k), n, n_1, \ldots, n_k), \end{aligned}$$

entonces f es demostrablemente total.

Sea $F(x_1, \ldots, x_k, x, y)$ la fórmula que define la función f como en la demostración del Teorema 4.1.10 ($f(n, n_1, \ldots, n_k) = m \Leftrightarrow \mathbb{N} \vDash F(n_1, \ldots, n_k, n, m)$). Recordemos que la fórmula F contiene a la fórmula $\Gamma(a, b, i, c)$, que define la función $\beta(a, b, i) = c$. Pero, por el Lema 4.2.3, sabemos que la función β es demostrablemente total en PA.

Para un modelo arbitrario $\mathbb{M}$ de PA y para cualesquiera $d_1, \ldots, d_k \in \mathrm{M}$ tenemos:

$\mathbb{M} \vDash F(d_1, \ldots, d_k, l, d) \Leftrightarrow (\exists a, b \in M\{\beta(a, b, 0) = g(d_1, \ldots, d_k) \wedge \beta(a, b, l) = d \wedge$
$\wedge \forall i < l[\beta(a, b, i+1) = h(\beta(a, b, i), i, d_1, \ldots, d_k)]\})$.

Hay que probar que $\mathbb{M} \vDash \forall x \exists! y F(d_1, \ldots, d_k, x, y)$. Para ello, consideraremos el conjunto paramétricamente definible $Y = \{l \in M : \mathbb{M} \vDash \exists! y F(d_1, \ldots, d_k, l, y)\}$.

- $0 \in Y$: Para $a = g(d_1, \ldots, d_k)$ y $b = a$.
- Supongamos que $l \in Y$: Sean a_l, b_l los elementos correspondientes a l; sea $d = h(\beta(a_l, b_l, l), l, d_1, \ldots, d_k)$ y sea φ la función definida como:

  $$\varphi(i) = \beta(a_l, b_l, i) \text{ para } i \in M \text{ con } i < l + 1$$
  $$\varphi(l + 1) = d.$$

  Nótese que φ es definible en $\mathbb{M}$.

  Ahora, debemos encontrar un elemento $c \in$ M tal que $l + 1 < c, d < c$ y $\varphi(i) < c$ para todo $i \leq l$. A continuación, elegiremos un $b \in$ M tal que $e|b\ \forall e \leq c$.

  La función $\psi(i) = (i + 1)b + 1$ para $i \in$ M es definible en $\mathbb{M}$ y $mcd(\psi(i), \psi(j)) = 1$ para $i < j \leq l + 1$.

  Efectivamente, supongamos que p es el menor primo mayor que 1 tal que $p|\psi(i)$ y $p|\psi(j)$ con $i < j$. Entonces, $p|(\psi(j) - \psi(i))$ implica $p|(j - i)b$. Como $j - i < c$, entonces $(j - i)|b$, por lo que podemos asegurar que $p|b$. Por tanto, $p|b(i + 1)$. Pero entonces $p|1$ y llegamos a una contradicción.

  Aplicando el **Lema 4.2.5**, encontramos un $a \in$ M tal que para todo $i \leq l + 1$ $a \equiv \varphi(i) \bmod \psi(i)$. Esto es,

  $$\beta(a, b, i) = \beta(a_l, b_l, i) \text{ para } i \leq l$$
  $$\beta(a, b, l + 1) = d = h(\beta(a, b, l), l, d_1, \ldots, d_k)$$

  Por consiguiente, $l + 1 \in Y$.

$\boxtimes$.

Por último, vamos a definir la función exponencial en $\mathbb{N}$ y vamos a probar que es demostrablemente total en PA. Además de servirnos de ejemplo, nos será necesaria más adelante.

Sea $exp : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ la función definida como:

$$exp(x, y) = \begin{cases} 0 & \text{si } x = 0 \\ 1 & \text{si } x \neq 0 \wedge y = 0 \\ x^y & \text{si } x \neq 0 \wedge y \neq 0 \end{cases}$$

Consideremos la fórmula $Exp(x, y, z)$ equivalente a una Σ_1-fórmula:

$$[x = \mathbf{0} \wedge z = \mathbf{0}] \vee [x \neq \mathbf{0} \wedge y = \mathbf{0} \wedge z = \mathbf{1}] \vee$$
$$[x \neq \mathbf{0} \wedge y \neq \mathbf{0} \wedge \exists u \exists v(\beta(u, v, 0) = 1 \wedge \forall j < y(\beta(u, v, j + 1) = \beta(u, v, j) \cdot x) \wedge \beta(u, v, y) = z)],$$

donde las referencias a la función β deben ser expresadas utilizando la fórmula acotada $\Gamma(u, v, i, w)$ vista anteriormente. Vamos a utilizar a continuación la inducción en PA .

Es claro que:

$$\mathsf{PA} \vdash \forall x \exists z Exp(x, \mathbf{0}, z).$$

Además, también se cumple que:

$$\mathsf{PA} \vdash \forall x \forall y (\exists z Exp(x, y, z) \rightarrow \exists w Exp(x, y + \mathbf{1}, w)).$$

Lo último es sencillo de probar. Sean u, v los correspondientes a la fórmula $Exp(x, y, z)$. Entonces sólo tenemos que considerar la secuencia $\langle \beta(u, v, 0), \ldots, \beta(u, v, y), \beta(u, v, y) \cdot x \rangle$ y, razonando como en la prueba del Teorema 4.2.6, sigue que $\exists w Exp(x, y+\mathbf{1}, w)$ se satisface. Por tanto,

$$\mathsf{PA} \vdash \forall x \forall y \exists z Exp(x, y, z).$$

La unicidad también se prueba (sin mucha dificultad) por inducción. Por tanto, finalmente se obtiene:

$$\mathsf{PA} \vdash \forall x \forall y \exists! z Exp(x, y, z),$$

con lo que la función $exp(x, y)$ es total.

Capítulo 5

El Teorema de Goodstein y su independencia de PA.

5.1. El Teorema de Goodstein.

Sean $g, p \in N$ con $p > 1$. Podemos representar g en base p de la siguiente manera:

$$g = a_{k_1} p^{k_1} + \cdots + a_{k_n} p^{k_n}$$

con $a_{k_i} < p$ para todo i y $0 \leq k_1 < \ldots < k_n < g$. Sabemos que estos coeficientes existen y son únicos por el Teorema de la Forma Normal de Cantor. Si sustituimos p por una variable x obtenemos la función $f_1(x) = a_{k_1} x^{k_1} + \cdots + a_{k_n} x^{k_n}$.

Si representamos a continuación los exponentes $k_1, \ldots, k_n$ también en base p, los exponentes de todas estas representaciones también los representamos en base p y así sucesivamente un número finito de pasos K hasta que todos los exponentes sean menores o iguales que p, obtendríamos lo que se conoce como la representación de g en base pura p.

Ejemplo 5.1.1 *Representación de 100 en base pura 3:* $100 = 3^{3+1} + 3^2 \cdot 2 + 1$.

Como hacíamos con $f_1(x)$, definimos de una manera análoga $f_{g,p}(x)$, que es la representación de g en base pura p, donde cada p la cambiamos por la variable x. Es decir,

$$f_{g,p}(x) = a_{k_1} x^{f_{k_1,p}(x)} + \cdots + a_{k_n} x^{f_{k_n,p}(x)}$$

Observemos que para todo $g, p > 1$, $f_{g,p}(p) = g$.

Lema 5.1.2 *Sea $p > 1$ y k=máx$\{k : p^k | g\ \}$ y $j = g - p^k$. Entonces:*

$$f_{g,p}(x) = f_{j,p}(x) + x^{f_{k,p}(x)}$$

Demostración: Sabemos que $g = p^k \cdot d$ para un cierto $d \in N$. Entonces, claramente

$$g = p^k \cdot f_{d,p}(p) = p^k \cdot (a_k + a_{k+1} \cdot p + a_{k+2} \cdot p^2 + \cdots + a_{k+r} \cdot p^r)$$

para un cierto r. Además, $a_k > 0$ por definición de k. De esta manera, $g = \sum_{i=k}^{k+r} a_i \cdot p^i$.

Como $j = g - p^k$ y $a_k \geq 1$:

$$f_{j,p}(p) = (a_k - 1) \cdot p^k + a_{k+1} \cdot p^{k+1} + \cdots + a_{k+r} \cdot p^{k+r} = f_{g,p}(p) - p^k = f_{g,p}(p) - p^{f_{k,p}(p)}.$$

⊠

Lema 5.1.3 *Si $x \geq p > 1$, entonces $f_{g,p}(x) < f_{g+1,p}(x)$.*

Demostración: Lo probaremos por inducción en g. Por hipótesis de inducción suponemos que $f_{j,p}(x) < f_{j+1,p}(x)$ para todo $j < g$ y para todo $x \geq p$. En particular, podemos suponer que $f_{i,p}(x) < f_{j,p}(x)$ para todo $j < g$, para todo $i < j$ y para todo $x \geq p$.

Dado g, sea $k = \text{máx}\{i : p^i | g\}$. Distinguimos varios casos:

Si $k \neq 0$, entonces, $g + 1 = 1 + \sum_{j=k}^{j=k+r} a_j p^j$, para algún $r \in N$. Luego, para todo x:

$$f_{g,p}(x) < f_{g,p}(x) + 1 = f_{g+1,p}(x).$$

El mismo razonamiento nos sirve si $k = 0$ y $a_0 < p - 1$.

Si en cambio, $k = 0$ y $a_0 = p - 1$, sea $m = \text{máx}\{i : \forall j < i \, (a_j = p - 1)\}$. Entonces,

$$g + 1 = 1 + (a_0 + a_1 p + \cdots + a_r p^r) = (a_m + 1)p^m + \sum_{j=m+1}^{r} a_j p^j = p^m + \sum_{j=m}^{r} a_j p^j$$

De este modo, dado x, $f_{g,p}(x) = \sum_{j=0}^{r} a_j x^{f_{j,p}(x)}$, mientras que

$$f_{g+1,p}(x) = x^{f_{m,p}(x)} + \sum_{j=m}^{r} a_j x^{f_{j,p}(x)}.$$

Por tanto, dado $x \geq p$,

$$f_{g,p}(x) < f_{g+1,p}(x) \Leftrightarrow \sum_{j=0}^{m-1} a_j x^{f_{j,p}(x)} < x^{f_{m,p}(x)}$$

con $a_j = p - 1$ para todo $j = 0, \ldots, m - 1$. Si $x = p$, el resultado es directo, ya que

$$\sum_{j=0}^{m-1} a_j p^{f_{j,p}(p)} = \sum_{j=0}^{m-1} a_j p^j < p^m = p^{f_{m,p}(p)}$$

Si $x > p$ tenemos, usando que $m < g$ y la hipótesis de inducción:

$$\sum_{j=0}^{m-1} a_j x^{f_{j,p}(x)} = (p-1)\sum_{j=0}^{m-1} x^{f_{j,p}(x)} \leq (p-1)\sum_{j=0}^{f_{m-1,p}(x)} x^j \leq \frac{p-1}{x-1}(x^{f_{m-1,p}(x)+1}-1) < x^{f_{m,p}(x)}$$

como queríamos demostrar.

⊠

Definición 5.1.4 *Sean $g, p \in N$ con $p > 1$. La sucesión de Goodstein en base p empezando por g es la sucesión $g_0, g_1, \ldots$ donde $g_0 = g$ y, si $g_n \neq 0$, entonces*

$$g_{n+1} = f_{g_n,p+n}(p+n+1) - 1.$$

Si en caso contrario $g_n = 0$, acaba la sucesión.

Teorema 5.1.5 (Goodstein) *Sean $g, p \in N$ con $p > 1$. Sea g_n la sucesión de Goodstein en base p empezando por g. Entonces existe un $n \in N$ tal que $g_n = 0$.*

Demostración: Sea $g_0, g_1, \ldots$ la sucesión de Goodstein en base p empezando por g. Entonces, a cada g_n le vamos a asignar un ordinal α_n. Sea $\alpha_n = f_{g_n,p+n}(\omega)$, donde f se define de la misma manera que antes pero extendemos su dominio a la clase **On**.

Entonces, por un lado tenemos que $f_{g_n,p+n}(\omega) = a_{k_1}\omega^{k_1} + \cdots + a_{k_n}\omega^{k_n}$ para ciertos $a_{k_i} < p+n$ y ciertos $k_i < g_n$ para todo $i = 1, \ldots, n$.

Por otro lado, consideremos

$$g_{n+1}+1 = f_{g_n,p+n}(p+n+1) = a_{k_1}(p+n+1)^{k_1}+\cdots+a_{k_n}(p+n+1)^{k_n} = f_{g_{n+1}+1,p+n+1}(p+n+1),$$

ya que $a_{k_i} < p+n < p+n+1$ y $k_i < g_n \leq g_{n+1}+1$ para todo $i = 1, \ldots, n$.

Por consiguiente, tenemos que

$$f_{g_{n+1}+1,p+n+1}(\omega) = a_{k_1}\omega^{k_1} + \cdots + a_{k_n}\omega^{k_n} = f_{g_n,p+n}(\omega) = \alpha_n.$$

Además, $\alpha_{n+1} = f_{g_{n+1},p+n+1}(\omega)$. Por tanto, por el lema anterior (que se verifica también para **On**), tenemos que $\alpha_{n+1} < \alpha_n$. Por el Teorema 2.1.14, sabemos que

$$\{\alpha_n \mid n \in N\} = \{a_{k_1}\omega^{k_1} + \cdots + a_{k_n}\omega^{k_n} | a_{k_1}(p+n)^{k_1} + \cdots + a_{k_n}(p+n)^{k_n} = g_n \ \forall n \in N\}$$

tiene un elemento mínimo, sea α_m. Si existiera un elemento α_{m+1}, entonces $\alpha_{m+1} < \alpha_m$, lo cual no es posible por ser α_m el elemento mínimo. Por tanto, tiene que ser el último elemento de la sucesión, con lo que la sucesión $\{\alpha_n\}_{n\in N}$ tiene $m+1$ elementos.

Veamos ahora que $\{g_n\}_{n\in N}$ también tiene $m+1$ elementos. Supongamos que α_m es el último elemento de su sucesión pero existe un elemento g_{m+1}. Entonces, podemos expresar

g_{m+1} en base $p+m+1$ y por tanto existiría $f_{g_{m+1},p+m+1}(\omega)$, que no es otra cosa que α_{m+1}. Como no existe tal elemento, g_{m+1} tampoco puede existir y g_m es el último elemento de la sucesión de Goodstein, que es finita por tener $m+1$ elementos. ⊠

Ahora, debemos expresar la sucesión de Goodstein en el lenguaje de PA.

Primero, definamos la función $f(p,u,q)$, que expresa el cambio de base p a q en la representación de u en base pura p con $p>1$.

$$f(p,u,q) = \begin{cases} u & \text{si } u < p \\ \sum_{k<u} c(u,p,k) \cdot q^{f(p,k,q)} & \text{si } u \geq p \end{cases},$$

donde $c(u,p,k)$ representa el k-ésimo coeficiente de la representación de u en base p. La definimos de la siguiente manera:

$$c(u,p,0) = r(u,p)$$

$$c(u,p,k) = r(q(u,p^k),p) \quad \text{si } k > 0$$

Las funciones q y r son las funciones cociente y resto que definimos en el capítulo anterior. Recordemos que ambas eran Σ_1-definibles.

Por tanto, $c(u,p,k)$ será Σ_1-definible por ser composición de funciones Σ_1-definibles. Además, c también es PR.

Volviendo a la función f, vemos que está definida por recursión sobre todos sus valores anteriores, no únicamente sobre el valor inmediatamente anterior. Por ello, vamos a ver la recursión de curso de valores, un recurso para poder expresar f de otra manera.

Definición 5.1.6 *Decimos que s codifica una sucesión de longitud n, $\langle a_0,\ldots,a_{n-1}\rangle$, si s es el menor número tal que tomando $a = K(s)$ y $b = L(s)$ se tiene que $\beta(a,b,0) = n$ y para todo $i = 1,\ldots,n$, $a_i = \beta(a,b,i+1)$. En este caso, para cada $i = 0,\ldots,n-1$, utilizaremos la notación $(s)_i$ para denotar al elemento a_i. La sucesión vacía (de longitud 0) se denotará por $\langle\rangle$.*

Definición 5.1.7 *Sean $a = \langle a_0,\ldots,a_n\rangle$ y $b = \langle b_0,\ldots,b_n\rangle$. Entonces, la función concatenación se define como $a * b = \langle a_0,\ldots,a_n,b_0,\ldots,b_n\rangle$.*

Puede probarse que la función '*' es PR.

Definición 5.1.8 *Sea $f(n,n_1,\ldots,n_k)$ una función. Definimos recursivamente:*

$$f^*(0,n_1,\ldots,n_k) = \langle\rangle$$
$$f^*(n+1,n_1,\ldots,n_k) = f^*(n,n_1,\ldots,n_k) * \langle f(n,n_1,\ldots,n_k)\rangle$$

Por tanto, para $n \geq 1$ tenemos:

$$f^*(n,n_1,\ldots,n_k) = \langle f(0,n_1,\ldots,n_k),\ldots,f(n-1,n_1,\ldots,n_k)\rangle.$$

Proposición 5.1.9 *Si $h \in PR$ y la función f se define por recursión como*

$$f(n, n_1, \ldots, n_k) = h(f^*(n, n_1, \ldots, n_k), n, n_1, \ldots, n_k),$$

entonces $f \in PR$.

Demostración: Se tiene que

$$f^*(0, n_1, \ldots, n_k) = \langle\rangle$$
$$f^*(n+1, n_1, \ldots, n_k) = f^*(n, n_1, \ldots, n_k) * \langle h(f^*(n, n_1, \ldots, n_k), n, n_1, \ldots, n_k)\rangle,$$

por lo que $f^* \in$ PR. Por último, como $f(n, n_1, \ldots, n_k) = (f^*(n+1, n_1, \ldots, n_k))_n$, entonces también $f \in$ PR. ⊠

Según lo que acabamos de ver, tenemos que

$$f^*(p, 0, q) = \langle\rangle \text{ y } f^*(p, u, q) = \langle f(p, 0, q), \ldots, f(p, u-1, q)\rangle \text{ para } u > 0.$$

Así, podemos redefinir f como:

$$f(p, u, q) = \begin{cases} u & \text{si } u < p \\ \sum_{k<u} c(u, p, k) \cdot q^{(f^*(p,u,q))_k} & \text{si } u \geq p \end{cases},$$

y f será PR por la Proposición 5.1.9.

A partir de f se define la sucesión de Goodstein en base $p > 1$ empezando por g_0 de manera recursiva como:

$$g(0, g_0, p) = g_0$$
$$g(i+1, g_0, p) = f(p+i, g(i, g_0, p), p+i+1) - 1$$

Recordemos que en PA $0 - 1 = 0$, por lo que no hace falta distinguir los casos en los que $g(i, g, p)$ es igual o distinto de 0.

Por consiguiente, como se define por recursión a partir de una función PR, entonces $g \in$ PR. Además, según el Teorema 4.2.6, g es demostrablemente total.

Como consecuencia, tenemos que g es Σ_1-definible (recordemos que toda función recursiva es Σ_1-definible y la clase PR está contenida en la clase de las funciones recursivas); y al ser además demostrablemente total, g está bien definida en PA para todo g_0 y para todo $p > 1$.

5.2. El Teorema de Cichon.

A continuación, vamos a definir algunas nociones que nos serán útiles de aquí en adelante. Sea ε_0 el límite de la sucesión de ordinales $\{\omega_n : n \in \mathbb{N}\}$, donde $\omega_0 = 1$ y $\omega_{n+1} = \omega^{\omega_n}$. Tenemos:

$$\omega_0 = 1, \omega_1 = \omega\ , \omega_2 = \omega^{\omega}, \omega_3 = \omega^{\omega^{\omega}}, \omega_4 = \omega^{\omega^{\omega^{\omega}}}, \ldots$$

ε_0 es el primer ordinal α tal que $\alpha = \omega^{\alpha}$. Cada ordinal $\lambda < \varepsilon_0$ puede ser expresado de la siguiente forma única por el Teorema de la Forma Normal de Cantor:

$$\lambda = \omega^{\lambda_1} + \cdots + \omega^{\lambda_m},$$

donde $\lambda > \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m \geq 0$.

Definición 5.2.1 *Sea λ un ordinal límite menor que ε_0. Vamos a definir la* ***sucesión canónica*** *$\{\lambda_n : n \in \mathbb{N}\}$ de ordinales menores que λ convergiendo a λ. Si*

$$\lambda = \omega^{\lambda_1} + \cdots + \omega^{\lambda_m} \text{ con } \lambda > \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m \geq 0$$

y sea $\lambda = \beta + \omega^{\lambda_m}$. Entonces:

$$\lambda_n = \{\lambda\}(n) = \begin{cases} \beta + \omega^{\lambda_m - 1} \cdot n & \text{si } \lambda_m \text{ sucesor} \\ \beta + \omega^{\{\lambda_m\}(n)} & \text{si } \lambda_m \text{ límite} \end{cases}$$

y $\{0\}(n) = 0$.

Definición 5.2.2 *Sea $\alpha < \varepsilon_0$ y $x \in \mathbb{N}$. Se define la siguiente operación:*

$$P_x(\alpha) = \begin{cases} \alpha - 1 & \text{si } \alpha \text{ sucesor} \\ 0 & \text{si } \alpha = 0 \\ P_x(\{\alpha\}(x)) & \text{si } \alpha \text{ límite} \end{cases}$$

Lema 5.2.3 *Sean $g, p \in \mathbb{N}$ con $p > 1$. Entonces, $P_p(f_{g+1,p}(\omega)) = f_{g,p}(\omega)$.*

Demostración: En primer lugar debemos probar un par de resultados. Para el primero, supongamos que $\alpha = \omega^{\lambda_1} + \cdots + \omega^{\lambda_m} = \beta + \omega^{\lambda_m}$ con $\lambda > \lambda_1 \geq \cdots \geq \lambda_m \geq 0$. Entonces, por inducción en λ_m vamos a ver que se cumple lo siguiente:

$$P_x(\alpha) = \beta + P_x(\omega^{\lambda_m}). \tag{5.1}$$

- $\lambda_m = 0 : P_x(\alpha) = P_x(\beta + 1) = \beta = \beta + P_x(1) = \beta + P_x(\omega^{\lambda_m})$.

- λ_m sucesor: Supongamos que se cumple el resultado para $\lambda_m - 1$. Entonces tenemos:

  $$P_x(\alpha) = P_x(\beta + \omega^{\lambda_m}) = P_x(\{\beta + \omega^{\lambda_m}\}(x)) = P_x(\beta + \omega^{\lambda_m - 1} \cdot x) =$$
  $$= P_x((\beta + \omega^{\lambda_m - 1} \cdot (x-1)) + \omega^{\lambda_m - 1}) = \beta + \omega^{\lambda_m - 1} \cdot (x-1) + P_x(\omega^{\lambda_m - 1}) =$$
  $$= \beta + P_x(\omega^{\lambda_m - 1} \cdot (x-1) + \omega^{\lambda_m - 1}) = \beta + P_x(\omega^{\lambda_m - 1} \cdot x) = \beta + P_x(\{\omega^{\lambda_m}\}(x)) =$$
  $$= \beta + P_x(\omega^{\lambda_m}).$$

- λ_m límite: Supongamos que se cumple el resultado para todo $\beta < \lambda_m$:

  $$P_x(\alpha) = P_x(\beta + \omega^{\lambda_m}) = P_x(\{\beta + \omega^{\lambda_m}\}(x)) = P_x(\beta + \omega^{\{\lambda_m\}(x)}) = \beta + P_x(\omega^{\{\lambda_m\}(x)}) =$$
  $$= \beta + P_x(\omega^{\lambda_m}).$$

A continuación, por inducción en $\lambda \geq 1$ probaremos el segundo resultado:

$$P_x(\omega^\lambda) = \omega^{P_x(\lambda)} \cdot (x-1) + P_x(\omega^{P_x(\lambda)}). \tag{5.2}$$

- $\lambda = 1$: Se tiene $P_x(\omega^\lambda) = P_x(\{\omega\}(x)) = P_x(x) = x - 1$. Por otro lado:

  $$\omega^{P_x(\lambda)} \cdot (x-1) + P_x(\omega^{P_x(\lambda)}) = x - 1 + P_x(1) = x - 1.$$

- λ sucesor: Se tiene

  $$P_x(\omega^\lambda) = P_x(\{\omega\}(x)) = P_x(\omega^{\lambda-1} \cdot x) = \omega^{\lambda-1} \cdot (x-1) + P_x(\omega^{\lambda-1}) = \omega^{P_x(\lambda)} \cdot (x-1) + P_x(\omega^{P_x(\lambda)}).$$

  Aquí hemos hecho uso de (5.1).

- λ límite: Supongamos que se cumple el resultado para todo $\beta < \lambda$.
  $P_x(\omega^\lambda) = P_x(\{\omega^\lambda\}(x)) = P_x(\omega^{\{\lambda\}(x)}) = \omega^{P_x(\{\lambda\}(x))} \cdot (x-1) + P_x(\omega^{P_x(\{\lambda\}(x))}) =$
  $= \omega^{P_x(\lambda)} \cdot (x-1) + P_x(\omega^{P_x(\lambda)})$.

Ahora ya disponemos de las herramientas para demostrar el lema. Lo hacemos por inducción sobre g. Asumimos que se cumple para todo $g' < g$.

Sea k el mayor entero tal que $p^k | (g+1)$ y sea $j = g + 1 - p^k$.

Si $k = 0$: Por el **Lema 5.1.2**, $f_{g+1,p}(\omega) = f_{g,p}(\omega) + 1$ y claramente se cumple por definición de P_p.

Si $k > 0$: $g + 1 = \sum_{i=k}^{r} a_i \cdot p^i$ para ciertos $a_i \in \mathbb{N}$, con $a_k \neq 0$ y $a_i < p$ para todo i (como en la prueba del Lema 5.1.2).
Además, $j = g + 1 - p^k = \sum_{i=k}^{r} a_i \cdot p^i - p^k = (a_k - 1) \cdot p^k + \sum_{i=k+1}^{r} a_i \cdot p^i$. Por lo que podemos expresar g de la siguiente manera:

$$g = j + p^k - 1 + p^{k-1} - p^{k-1} = j + p^{k-1} \cdot (p-1) + (p^{k-1} - 1) =$$
$$= (a_k - 1) \cdot p^k + \sum_{i=k+1}^{r} a_i \cdot p^i + p^{k-1} \cdot (p-1) + \sum_{i=0}^{k-2} b_i \cdot p^i$$

para ciertos $b_i < p \in \mathbb{N}$.

Esto es, como podemos observar, la expresión de g en base p. Por tanto:

$$g = f_{g,p}(p) = f_{j,p}(p) + p^{f_{k-1,p}(p)} \cdot (p-1) + f_{p^{k-1}-1,p}(p)$$

De lo que sigue:

$$g = f_{g,p}(\omega) = f_{j,p}(\omega) + \omega^{f_{k-1,p}(\omega)} \cdot (p-1) + f_{p^{k-1}-1,p}(\omega)$$

Por otro lado, por el **Lema 5.1.2** , los resultados que hemos demostrado y aplicando la hipótesis de inducción tenemos que :

$$P_p(f_{g+1,p}(\omega)) = P_p(f_{j,p}(\omega) + \omega^{f_{k,p}(\omega)}) = f_{j,p}(\omega) + P_p(\omega^{f_{k,p}(\omega)}) =$$
$$= f_{j,p}(\omega) + \omega^{P_p(f_{k,p}(\omega))} \cdot (p-1) + P_p(\omega^{P_p(f_{k,p}(\omega))}) =$$
$$= f_{j,p}(\omega) + \omega^{f_{k-1,p}(\omega)} \cdot (p-1) + P_p(\omega^{f_{k-1,p}(\omega)}) =$$
$$= f_{j,p}(\omega) + \omega^{f_{k-1,p}(\omega)} \cdot (p-1) + P_p(f_{p^{k-1},p}(\omega)) =$$
$$= f_{j,p}(\omega) + \omega^{f_{k-1,p}(\omega)} \cdot (p-1) + f_{p^{k-1}-1,p}(\omega).$$

⊠

Sea α_n como en la prueba del Teorema de Goodstein. Recordemos que

$$\alpha_n = f_{g_{n+1}+1,p+n+1}(\omega) \text{ para todo } n.$$

Por el Lema 5.2.3 inferimos:

$$P_{p+n+1}(\alpha_n) = P_{p+n+1}(f_{g_{n+1}+1,p+n+1}(\omega)) = f_{g_{n+1},p+n+1} = \alpha_{n+1}.$$

Corolario 5.2.4 $\alpha_{n+1} = P_{p+n+1}(\alpha_n)$.

Definición 5.2.5 *La* ***sucesión de Hardy*** $\{H_\alpha\}_{\alpha<\varepsilon_0}$ *es una sucesión de funciones que se define recursivamente de la siguiente manera:*

$$H_\alpha(x) = \begin{cases} x & \text{si } \alpha = 0 \\ H_{\alpha-1}(x+1) & \text{si } \alpha \text{ sucesor} \\ H_{\{\alpha\}(x)}(x) & \text{si } \alpha \text{ límite} \end{cases}$$

Se puede probar que si $\alpha < \beta$, entonces $H_\alpha(x) < H_\beta(x)$ para casi todo x. Sin embargo, la velocidad de crecimiento de estas funciones va aumentando muy lentamente a medida que α crece. Veamos algunos ejemplos:

$$
\begin{aligned}
&H_1(x) = H_0(x+1) = x+1\\
&H_2(x) = H_1(x+1) = x+2\\
&\quad\vdots\\
&H_n(x) = x+n\\
&\quad\vdots\\
&H_\omega(x) = H_x(x) = 2x\\
&\quad\vdots\\
&H_{\omega+n}(x) = H_x(x) = 2(x+n)\\
&\quad\vdots\\
&H_{\omega\cdot 2}(x) = H_{\omega+x}(x) = 2(x+x) = 4x\\
&\quad\vdots\\
&H_{\omega\cdot n}(x) = 2^n\cdot x\\
&\quad\vdots\\
&H_{\omega^2}(x) = 2^x\cdot x
\end{aligned}
$$

Lema 5.2.6 *Para todo $x, n \in N$, α y $\beta \leq \omega^\alpha$ cualesquiera se tiene que:*

$$H_{\omega^\alpha n+\beta}(x) = H_{\omega^\alpha n}(H_\beta(x)).$$

Demostración: Procedemos por inducción en β.

- $\beta = 0$: Se cumple claramente, ya que $H_0(x) = x$.
- Supongamos que se cumple el resultado para β: Sea $\beta + 1 \leq \omega^\alpha$.

$$H_{\omega^\alpha n+\beta+1}(x) = H_{\omega^\alpha n+\beta}(x+1) = H_{\omega^\alpha n}(H_\beta(x+1)) = H_{\omega^\alpha n}(H_{\beta+1}(x))$$

- Sea β límite: Supongamos que se cumple el resultado para todo $\gamma < \beta$.

$$H_{\omega^\alpha n+\beta}(x) = H_{\{\omega^\alpha n+\beta\}(x)}(x) = H_{\omega^\alpha n+\{\beta\}(x)}(x) = H_{\omega^\alpha n}(H_{\{\beta\}(x)}(x)) = H_{\omega^\alpha n}(H_\beta(x))$$

⊠

A continuación, presentaremos un importante resultado que no probaremos pero será crucial para probar que el Teorema de Goodstein no puede demostrarse en PA. Este resultado fue obtenido por S.S. Wainer en [8] y [9] y nos permite acotar toda función demostrablemente total en PA mediante una función de la sucesión de Hardy.

Teorema 5.2.7 (Wainer) *Sea $f : N \to N$ una función Σ_1-definible. Sea $F(x, y)$ una Σ_1-fórmula que define a f en $\mathbb{N}$. Supongamos que PA $\vdash \forall x \exists! y F(x, y)$. Entonces, hay un $\alpha < \varepsilon_0$ y un $n_0 \in N$ tales que para $x \in N$ con $x \geq n_0$ se cumple que $f(x) \leq H_\alpha(x)$.*

⊠

El siguiente resultado, probado por E.A. Cichon en [3] será también fundamental para nuestro objetivo. Establece una conexión directa entre la sucesión de Goodstein y las funciones de la sucesión de Hardy.

Teorema 5.2.8 (Cichon) *Sea* $h : N \times N \to N$, $h(g,p) = mín\{m : g_m(g,p) = 0\}$, *donde* $\{g_i(g,p) : i \in N\}$ *es la sucesión de Goodstein en base* p *empezando por* g. *Sea* $\alpha = f_{g,p}(\omega)$. *Entonces,*

$$h(g,p) = H_\alpha(p+1) - (p+1).$$

Demostración: Por el Corolario 5.2.4 tenemos:

$$h(g,p) = mín\{n : \alpha_n = 0\} = mín\{n : P_{p+n}(P_{p+n-1}(\dots P_{p+2}(P_{p+1}(\alpha))\dots) = 0\}.$$

Recordemos que $\alpha_0 = f_{g_0,p}(\omega) = f_{g,p}(\omega) = \alpha$.

Sea $Y(p,\alpha) = \text{mín}\{y : P_{p+y}(P_{p+y-1}(\dots P_{p+2}(P_{p+1}(\alpha))\dots) = 0\} = h(g,p)$.

Bastará con probar que la igualdad

$$Y(p,\alpha) = H_\alpha(p+1) - (p+1) \text{ es cierta para todo } \alpha.$$

Lo probaremos por inducción en α:

- $\alpha = 0$: $Y(p,0) = 0 = p + 1 - (p+1) = H_0(p+1) - (p+1)$.
- α sucesor: Suponemos el resultado cierto para $\alpha - 1$ y para todo p. Entonces, en particular:

  $Y(p+1,\alpha-1) = H_{\alpha-1}(p+2) - (p+2)$ se cumple para todo p por hipótesis de inducción.

  Pero $H_{\alpha-1}(p+2) = H_\alpha(p+1)$ e $Y(p+1,\alpha-1) = Y(p,\alpha)-1$, ya que $P_{p+1}(\alpha) = \alpha - 1$.

  Por tanto,

  $$Y(p,\alpha) - 1 = H_{\alpha-1}(p+2) - (p+2) = H_\alpha(p+1) - (p+2)$$

  Así, $Y(p,\alpha) = H_\alpha(p+1) - (p+1)$.
- α límite: Suponemos el resultado cierto para todo $\beta < \alpha$ y para todo p.

  Tenemos que $Y(p,\alpha) = Y(p,\{\alpha\}(p+1))$ por definición de P_{p+1}.

  Pero, por hipótesis de inducción,

  $$Y(p,\{\alpha\}(p+1)) = H_{\{\alpha\}(p+1)}(p+1) - (p+1) = H_\alpha(p+1) - (p+1).$$

⊠

5.3. Independencia del Teorema de Goodstein de PA.

Definición 5.3.1 *Vamos a definir la sucesión de funciones $G_\alpha : N \to N$ para $\alpha < \varepsilon_0$.*

$$G_\alpha(x) = \begin{cases} 0 & \text{si } \alpha = 0 \\ G_{\alpha-1}(x) + 1 & \text{si } \alpha \text{ sucesor} \\ G_{\{\alpha\}(x)}(x) & \text{si } \alpha \text{ límite} \end{cases}$$

El siguiente resultado nos será útil más adelante y también le dará sentido a la sucesión de funciones que acabamos de definir.

Proposición 5.3.2 *Para todo $\alpha < \varepsilon_0$ se tiene que $G_\alpha(x) = f_{\alpha,\omega}(x)$, donde $f_{\alpha,\omega}(x)$ es la expresión que obtenemos al cambiar cada aparición de ω por x en la representación de α en base pura ω. Por otro lado, sea $g = G_\alpha(x)$ dado, entonces $\alpha = f_{g,x}(\omega)$ siempre que x sea mayor que los coeficientes de la representación de α en base pura ω.*

Demostración: La primera parte la probaremos por inducción en α:

- $\alpha = 0 : G_0(x) = 0 = f_{0,\omega}(x)$.
- Suponemos que se cumple para α :

  $$G_{\alpha+1}(x) = G_\alpha(x) + 1 = f_{\alpha,\omega}(x) + 1 = x^{f_{k_n,\omega}(x)} a_{k_n} + \cdots + x^{f_{k_0,\omega}(x)} a_{k_0} + 1$$

  para ciertos $n < \omega; 0 < a_{k_i} < \omega; k_0 < \ldots < k_n < \alpha$.

  Si α es sucesor, entonces $k_0 = 0$ y

  $$f_{\alpha,\omega}(x) + 1 = x^{f_{k_n,\omega}(x)} a_{k_n} + \cdots + (a_{k_0} + 1) = f_{\alpha+1,\omega}(x)$$

  Si α es límite, entonces $k_0 > 0$ y

  $$f_{\alpha,\omega}(x) + 1 = x^{f_{k_n,\omega}(x)} a_{k_n} + \cdots + x^{f_{k_0,\omega}(x)} a_{k_0} + 1 = f_{\alpha+1,\omega}(x).$$

  Si $\alpha = 0$ está claro.

- Sea α límite : Supongamos que se cumple para todo $\beta < \alpha$.
  Sea $f_{\alpha,\omega}(x) = x^{f_{k_n,\omega}(x)} a_{k_n} + \cdots + x^{f_{k_0,\omega}(x)} a_{k_0}$. Entonces:

  $$\alpha = \omega^{k_n} a_{k_n} + \cdots + \omega^{k_0}(a_{k_0} - 1) + \omega^{k_0} = \beta + \omega^{k_0}.$$

  (con $k_0 > 0$ por ser α límite).
  Por otro lado, $G_\alpha(x) = G_{\{\alpha\}(x)}(x) = f_{\{\alpha\}(x),\omega}(x)$. Hay dos opciones:

- k_0 es sucesor : $\{\alpha\}(x) = \beta + \omega^{k_0-1}x$.
  $f_{\{\alpha\}(x),\omega}(x) = x^{f_{k_n,\omega}(x)}a_{k_n} + \cdots + x^{f_{k_0,\omega}(x)}(a_{k_0} - 1) + x^{f_{k_0-1,\omega}(x)}x =$
  $= x^{f_{k_n,\omega}(x)}a_{k_n} + \cdots + x^{f_{k_0,\omega}(x)}(a_{k_0} - 1) + x^{f_{k_0-1,\omega}(x)+1} =$
  $= x^{f_{k_n,\omega}(x)}a_{k_n} + \cdots + x^{f_{k_0,\omega}(x)}(a_{k_0} - 1) + x^{f_{k_0,\omega}(x)} = f_{\alpha,\omega}(x)$.

- k_0 límite: $\{\alpha\}(x) = \beta + \omega^{\{k_0\}(x)}$.

  $$f_{\{\alpha\}(x),\omega}(x) = x^{f_{k_n,\omega}(x)}a_{k_n} + \cdots + x^{f_{k_0,\omega}(x)}(a_{k_0} - 1) + x^{f_{\{k_0\}(x),\omega}(x)}.$$

  Por hipótesis de inducción, $f_{\{k_0\}(x),\omega}(x) = G_{\{k_0\}(x)}(x) = G_{k_0}(x) = f_{k_0,\omega}(x)$. Por tanto, $f_{\{\alpha\}(x),\omega}(x) = f_{\alpha,\omega}(x)$.

La segunda parte del resultado es clara. Sólo hay que tener en cuenta que $g = f_{\alpha,\omega}(x)$. Así, como estamos considerando x lo suficientemente grande, $f_{\alpha,\omega}(x) = f_{g,x}(x)$. Por tanto, si sustituimos x por ω en esa expresión, se obtiene $f_{g,x}(\omega) = \alpha$. ⊠

Definición 5.3.3 *Sean $\beta \leq \alpha < \varepsilon_0$ y $x \in N$. Escribiremos $\alpha \Rightarrow_x \beta$ si existe $n \in N$ y una sucesión finita $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_n = \beta$ tal que $\alpha_{i+1} = \{\alpha_i\}(x)$ para todo $i = 0, \ldots, n-1$. Además, establecemos que para $\gamma > 0$ no límite, $\{\gamma\}(x) = \gamma - 1$ y $\{0\}(x) = 0$.*

Proposición 5.3.4 *Sean $x, y, z \in N$ con $z \geq y$ y $x > 0$ y sea $\lambda < \varepsilon_0$. Entonces:*

1. $\lambda \Rightarrow_x 0$
2. $\{\lambda\}(z) \Rightarrow_x \{\lambda\}(y)$

Demostración:

1. Por inducción en λ.
   - $\lambda = 0$: $0 \Rightarrow_x 0$ claramente.
   - Suponemos que $\lambda \Rightarrow_x 0$: Sea $\lambda = \alpha_0, \alpha_1, \ldots, \alpha_n = 0$ la secuencia correspondiente. Entonces, como $\{\lambda + 1\}(x) = \lambda$, $\lambda + 1 \Rightarrow_x 0$ para la secuencia $\lambda + 1, \lambda = \alpha_0, \alpha_1, \ldots, \alpha_n = 0$.
   - Sea λ límite: Suponemos que $\beta \Rightarrow_x 0$ para todo $\beta < \lambda$. Entonces, $\lambda \Rightarrow_x \{\lambda\}(x) \Rightarrow_x 0$ por hipótesis de inducción.
2. Por inducción en λ.
   - $\lambda = 0$: $\{0\}(z) = \{0\}(y) = 0$ y, claramente, $0 \Rightarrow_x 0$.
   - Sea λ sucesor: $\{\lambda\}(z) = \{\lambda\}(y) = \lambda - 1$.

- Sea λ límite: Supongamos que $\{\beta\}(z) \Rightarrow_x \{\beta\}(y)\ \forall \beta < \lambda$. Sea $\lambda = \beta + \omega^{\lambda_m}$.

  Supongamos en primer lugar que λ_m es límite. Entonces, $\{\lambda\}(z) = \beta + \omega^{\{\lambda_m\}(z)}$. Por hipótesis de inducción, $\{\lambda_m\}(z) \Rightarrow_x \{\lambda_m\}(y)$ para una sucesión finita $\{\lambda_m\}(z) = \alpha_0, \alpha_1, \ldots, \alpha_n = \{\lambda_m\}(y)$.

  Vamos a probar que $\beta + \omega^{\alpha_i} \Rightarrow_x \beta + \omega^{\alpha_{i+1}}$:

  Si α_i es límite: $\{\beta + \omega^{\alpha_i}\}(x) = \beta + \omega^{\{\alpha_i\}(x)} = \beta + \omega^{\alpha_{i+1}}$.

  Si α_i es sucesor:

  $$\{\beta + \omega^{\alpha_i}\}(x) = \beta + \omega^{\alpha_i - 1}x = \beta + \omega^{\{\alpha_i\}(x)}x =$$
  $$= \beta + \omega^{\alpha_{i+1}}x = \beta + \omega^{\alpha_{i+1}} + \omega^{\alpha_{i+1}}(x-1) \Rightarrow_x \beta + \omega^{\alpha_{i+1}},$$

  ya que $\omega^{\alpha_{i+1}}(x-1) \Rightarrow_x 0$.

  Por tanto, tenemos que:

  $$\{\lambda\}(z) = \beta + \omega^{\alpha_0} \Rightarrow_x \beta + \omega^{\alpha_1} \Rightarrow_x \cdots \Rightarrow_x \beta + \omega^{\alpha_n} = \beta + \omega^{\{\lambda_m\}(y)} = \{\lambda\}(y).$$

  Supongamos ahora que λ_m es sucesor:

  $$\{\lambda\}(z) = \beta + \omega^{\lambda_m - 1}z = \beta + \omega^{\lambda_m - 1}y + \omega^{\lambda_m - 1}(z-y) \Rightarrow_x \beta + \omega^{\lambda_m - 1}y = \{\lambda\}(y),$$

  ya que $\beta + \omega^{\lambda_m - 1}(z-y) \Rightarrow_x 0$. ⊠

Proposición 5.3.5 *Sea $\alpha < \varepsilon_0$. Entonces, las funciones H_α y G_α son crecientes para argumentos positivos.*

Demostración: Tenemos las siguientes propiedades:

1. Sean $x \in \mathrm{N}$ con $x > 0$ y $\alpha > \beta$ tales que $\alpha \Rightarrow_x \beta$. Entonces,

   $$H_\alpha(x+1) > H_\beta(x+1).$$

2. H_α es creciente para argumentos positivos.

Vamos a probar ambas simultáneamente por inducción en α.

- $\alpha = 0$: Como no existe $\beta < 0$ damos por cierta la primera propiedad. En cuanto a la segunda, $H_0(x) = x < H_0(x+1) = x+1$.

- Suponemos que se cumplen 1 y 2 para un α cualquiera y sea $\alpha + 1 \Rightarrow_x \beta$ para $x > 0$.

  $$H_{\alpha+1}(x+1) = H_\alpha(x+2) > H_\alpha(x+1) = H_{\alpha+1}(x) > H_\beta(x+1)$$

  Con esto quedan probadas 1 y 2 para $\alpha + 1$. Se han usado ambas hipótesis de inducción. Para la de 1 téngase en cuenta que $\{\alpha+1\}(x) = \alpha$ y, por tanto, $\alpha \Rightarrow_x \beta$.

- α límite : Suponemos que se cumplen 1 y 2 para todo $\gamma < \alpha$ y sea $\alpha \Rightarrow_x \beta$ para $x > 0$ y $\alpha > \beta$.

  Por un lado tenemos:

  $$H_\alpha(x+1) = H_{\{\alpha\}(x+1)}(x+1) > H_{\{\alpha\}(x)}(x+1) > H_{\{\alpha\}(x)}(x) = H_\alpha(x).$$

  Téngase en cuenta que $\{\alpha\}(x+1) \Rightarrow_x \{\alpha\}(x)$ según la Proposición 5.3.4.

  Por otro lado se tiene que:

  $$H_\alpha(x+1) = H_{\{\alpha\}(x+1)}(x+1) > H_{\{\alpha\}(x)}(x+1) > H_\beta(x+1).$$

  Aquí téngase en cuenta que como $\alpha \Rightarrow_x \beta$ y $\alpha > \beta$, entonces $\{\alpha\}(x) \Rightarrow_x \beta$.

A continuación, vamos a considerar propiedades similares a 1 y 2 pero para las funciones G_α :

1. Sean $x \in \mathrm{N}$ con $x > 0$ y $\alpha > \beta$ tales que $\alpha \Rightarrow_x \beta$. Entonces,

   $$G_\alpha(x+1) > G_\beta(x+1).$$

2. G_α es creciente para argumentos positivos.

En este caso, demostraremos ambas por separado por inducción sobre α:

1. - $\alpha = 0$: Como no existe $\beta < 0$ lo damos por cierto.
   - Suponemos que se cumple para α. Sea β tal que $\alpha+1 > \beta$ con $\alpha+1 \Rightarrow_x \beta$ para $x > 0$. Entonces:
     $G_{\alpha+1}(x+1) = G_\alpha(x+1) + 1 > G_\alpha(x+1) > G_\gamma(x+1)\ \forall \gamma < \alpha$ con $\alpha \Rightarrow_x \gamma$.
     Por tanto, si $\beta = \alpha$, se cumple. Si, en otro caso, $\beta < \alpha$, también se cumple, ya que $\{\alpha+1\}(x) = \alpha$.
   - α límite: Supongo que se cumple 1 para todo $\gamma < \alpha$ y sea $\beta < \alpha$ con $\alpha \Rightarrow_x \beta$ y $x > 0$. Entonces:

     $$G_\alpha(x+1) = G_{\{\alpha\}(x+1)}(x+1) > G_{\{\alpha\}(x)}(x+1) > G_\beta(x+1).$$

2. Sea $x > 0$.

   - $\alpha = 0$: $G_0(x) = G_0(x+1) = 0$.
   - Suponemos cierto para α:
     $G_{\alpha+1}(x+1) = G_\alpha(x+1) + 1 \geq G_\alpha(x) + 1 = G_{\alpha+1}(x)$.
   - α límite: Supongamos que se cumple 2 $\forall \beta < \alpha$.
     $G_\alpha(x+1) = G_{\{\alpha\}(x+1)}(x+1) \geq G_{\{\alpha\}(x+1)}(x) > G_{\{\alpha\}(x)}(x) = G_\alpha(x)$.
     Para la última desigualdad hemos utilizado la propiedad 1.

Nótese que a diferencia de H_α, G_α no es estrictamente creciente.

$\boxtimes$

Proposición 5.3.6 *Sean $\alpha < \beta < \varepsilon_0$, entonces $H_\alpha <_* H_\beta$ y $G_\alpha <_* G_\beta$. Con $f <_* g$ para dos funciones cualesquiera f y g, indicamos que $f(x) < g(x)$ para casi todo x, es decir, para todo x excepto un conjunto finito de ellas.*

Demostración: Empecemos con la función H. Fijamos α y aplicamos inducción para $\beta > \alpha$.

- $\beta = \alpha+1$: Para $x > 0$, $\alpha+1 \Rightarrow_x \alpha$. Por la Proposición 5.3.5, $H_{\alpha+1}(x+1) > H_\alpha(x+1)$ para todo $x > 0$. Es decir, $H_\beta(x) > H_\alpha(x)$ $\forall x > 1$ y, por tanto, para casi todo x.
- Supongamos que se cumple la propiedad para un $\beta \geq \alpha + 1$ cualquiera. Veamos que se cumple para $\beta + 1$:

  $H_{\beta+1}(x) = H_\beta(x+1) > H_\beta(x)$ para $x > 0$ por la Proposición 5.3.5. Además, por hipótesis de inducción, $H_\alpha <_* H_\beta$.
- β límite: Sea $\beta > \alpha$ y supongamos que se cumple el resultado para todo $\gamma < \beta$.

  Vamos a escoger $x_0 > 0$ tal que $\{\beta\}(x_0) > \alpha$. Entonces, $H_\alpha <_* H_{\{\beta\}(x_0)}$ por hipótesis de inducción.

  Por otro lado, $\forall x \geq x_0$, $\beta \Rightarrow_x \{\beta\}(x) \Rightarrow_x \{\beta\}(x_0)$ según la Proposición 5.3.4.

  Por tanto, por la Proposición 5.3.5, para todo $x \geq x_0$:

$$H_\alpha(x+1) <_* H_{\{\beta\}(x_0)}(x+1) < H_\beta(x+1).$$

A continuación, lo probaremos para G también por inducción en β con α fijo.

- $\beta = \alpha+1$: Por la Proposición 5.3.5, $G_\beta(x+1) = G_{\alpha+1}(x+1) > G_\alpha(x+1)$ para todo $x > 0$.
- Supongamos que se cumple la propiedad para un $\beta \geq \alpha + 1$ cualquiera. Veamos que se cumple para $\beta + 1$:

  $G_\alpha(x) <_* G_\beta(x) + 1 = G_{\beta+1}(x)$ por hipótesis de inducción.
- β límite: Sea $\beta > \alpha$ y supongamos que se cumple el resultado para todo $\gamma < \beta$.

  Vamos a escoger $x_0 > 0$ tal que $\{\beta\}(x_0) > \alpha$. Entonces, $G_\alpha <_* G_{\{\beta\}(x_0)}$ por hipótesis de inducción.

  Así, para todo $x \geq x_0$: $G_\alpha(x+1) <_* G_{\{\beta\}(x_0)}(x+1) < G_{\{\beta\}(x+1)}(x+1) = G_\beta(x+1)$.

$\boxtimes$

Proposición 5.3.7 *Vamos a definir $G_{\varepsilon_0}(x)$ como $G_{\omega_x}(x)$. Entonces, $(G_{\varepsilon_0})^3 \leq_* H_{\omega^3}$.*

Demostración: $G_{\varepsilon_0}(x) = G_{\omega_x}(x) = f_{\omega_x,\omega}(x) = x^{x^{\cdot^{\cdot^{\cdot^{x}}}}}$ con x niveles.

Primero, debemos probar que $H_{\omega^3}(x) \geq 2^{2^{\cdot^{\cdot^{\cdot^{2^x}}}}}$ (con $x \geq 1$ niveles).

Sea $h_0(x) = x$ y $h_n(x) = 2^{2^{\cdot^{\cdot^{\cdot^{2^x}}}}}$ con n niveles si $n \geq 1$. Tenemos entonces que $h_{n+1}(x) = 2^{h_n(x)}$.

Vamos a probar por inducción en n que para todo $x \geq 1$, $H_{\omega^2 n}(x) \geq h_n(x)$.

- $H_{\omega^2 0}(x) = H_0(x) = x = h_0(x)$.
- $H_{\omega^2}(x) = 2^x x \geq 2^x = h_1(x)$
- Supongamos cierto para un $n \geq 1$:

$$H_{\omega^2(n+1)}(x) = H_{\omega^2 n+\omega^2}(x) = H_{\omega^2 n}(H_{\omega^2}(x)) \geq h_n(H_{\omega^2}(x)) = h_n(2^x x) \geq h_{n+1}(x).$$

Por tanto, $H_{\omega^3}(x) = H_{\{\omega^3\}(x)}(x) = H_{\omega^2 x}(x) \geq h_x(x) = 2^{2^{\cdot^{\cdot^{\cdot^{2^x}}}}}$ para $x \geq 1$.

Ahora, sea $g_0(x) = 1$ y $g_n(x) = x^{x^{\cdot^{\cdot^{\cdot^{x}}}}}$ con n niveles para $n \geq 1$. Se tiene que $g_{n+1}(x) = x^{g_n(x)}$. Además, $G_{\varepsilon_0}(x) = g_x(x)$ para $x \geq 1$.

Probaremos por inducción en n que $h_n(x) \geq x(g_n(x))^3$ $\forall x \geq 16$:

- $h_0(x) = x = x(g_0(x))^3$.
- $h_1(x) = 2^x \geq x(g_1(x))^3 = x^4$ para $x \geq 16$.
- Supongamos cierto para $n \geq 1$:

$$h_{n+1}(x) = 2^{h_n(x)} \geq 2^{x(g_n(x))^3} = (2^x)^{(g_n(x))^3} \geq (x^2)^{(g_n(x))^3} \geq x \cdot x^{(g_n(x))^3} \geq x \cdot x^{3g_n(x)} =$$
$$= x \cdot (x^{g_n(x)})^3 = x \cdot (g_{n+1}(x))^3.$$

Puede comprobarse fácilmente que para $n \geq 1$ y $x \geq 16$:

$$2^x \geq x^2 \text{ y } (g_n(x))^3 \geq 3g_n(x).$$

Por tanto, para $x \geq 16$:

$$H_{\omega^3}(x) \geq h_x(x) \geq x \cdot (g_x(x))^3 \geq (g_x(x))^3 = (G_{\varepsilon_0}(x))^3.$$

$\boxtimes$

Teorema 5.3.8 (Independencia del Teorema de Goodstein de PA.) *El Teorema de Goodstein no puede probarse en* PA.

Demostración: Lo haremos por reducción al absurdo. Supongamos que el Teorema de Goodstein tiene prueba en PA. Vamos a extender la ya conocida función $h(g,p)$ y añadimos a su dominio los pares $(g,0)$ y $(g,1)$ para cualquier $g \in N$ haciendo $h(g,0) = h(g,1) = 0$. De esta manera, $h(g,p)$ es demostrablemente total en PA (por hipótesis).

A continuación, consideremos la función h' definida como sigue:

$$h'(x) = h(K(x), L(x)) + L(x) + 1$$

Como K y L son demostrablemente totales (J es biyectiva), tendrá sentido entonces si ponemos:

$$h'(J(g,p)) = h(K(J(g,p)), L(J(g,p))) + L(J(g,p)) + 1 = h(g,p) + p + 1.$$

Por ser K y L demostrablemente totales y ser h demostrablemente total por hipótesis, entonces h' también lo es. De esta manera, estamos en condiciones de aplicar el Teorema de Wainer a la función h': $\exists \beta < \varepsilon_0$ tal que $h' \leq_* H_\beta$. Como $\beta < \varepsilon_0$, habrá algún k tal que $\beta < \omega_k$. Como podemos escoger dicho k tan grande como queramos, podemos suponer que ω_k es de la forma ω^γ con $\gamma \geq 3$. Como por la Proposición 5.3.6 $H_\beta <_* H_{\omega_k}$, podemos escoger β directamente de la forma ω^γ con $\gamma \geq 3$.

Si $h' \leq_* H_\beta$, entonces existe x_0 tal que $h'(x) \leq H_\beta(x)$ para todo $x \geq x_0$. Fijamos ahora un $\alpha < \varepsilon_0$ tal que $\alpha \geq \omega^\gamma + \omega^3 = \beta + \omega^3$. Vamos a probar que para infinitos p:

$$h'(J(G_\alpha(p)), p)) \leq H_{\omega^\gamma + \omega^3}(p).$$

Tenemos que $J(G_\alpha(p), p) \leq (G_\alpha(p))^3$ para $p \geq 3$.

En efecto, para $m \geq n \geq 3$ con $m, n \in$ N cualesquiera, se tiene:

$$J(m,n) = \frac{(m+n)(m+n+1)}{2} + m \leq \frac{2m(2m+1)}{2} + m = m(2m+1) + m = 2m(m+1) \leq m^3$$

La última desigualdad la probaremos por inducción para $m \geq 3$:

Si $m = 3 : 24 < 27$.

Supongamos que se cumple para $m \geq 3$ cualquiera:

$$2(m+1)(m+2) = 2m(m+1) + 4m + 4 \leq m^3 + 4m + 4 < m^3 + 3m \cdot m + 3m + 1 = (m+1)^3.$$

Por último, como podemos escoger α tan grande como se quiera, podemos asegurar que $G_\alpha(p) \geq p$.

Tomemos ahora p tal que $p \geq 3$ y $J(G_\alpha(p), p) \geq x_0$. Entonces, por la Proposición 5.3.5:

$$h'(J(G_\alpha(p), p)) \leq H_{\omega^\gamma}(J(G_\alpha(p), p)) \leq H_{\omega^\gamma}((G_\alpha(p))^3)$$

Sea x_1 tal que $G_\alpha(x) < G_{\varepsilon_0}(x)$ y $(G_{\varepsilon_0}(x))^3 \leq H_{\omega^3}(x)$ para todo $x \geq x_1$. Téngase en cuenta que existe $m \in \mathrm{N}$ tal que $\alpha < \omega_m$ y $G_\alpha <_* G_{\omega_m}$ por la Proposición 5.3.6. Además, para todo $x > m$, $G_{\omega_m}(x) < G_{\omega_x}(x) = G_{\varepsilon_0}(x)$ por la Proposición 5.3.5, ya que $\omega_x \Rightarrow_{x-1} \omega_m$. Teniendo en cuenta también la Proposición 5.3.7, podemos asegurar que tal x_1 existe. Supongamos además que $p \geq x_1$. Entonces:

$$h'(J(G_\alpha(p), p)) \leq H_{\omega^\gamma}((G_\alpha(p))^3) \leq H_{\omega^\gamma}((G_{\varepsilon_0}(p))^3) \leq H_{\omega^\gamma}(H_{\omega^3}(p)) = H_{\omega^\gamma+\omega^3}$$

por la Proposición 5.3.5 y el Lema 5.2.6.

Hemos demostrado que $h'(J(G_\alpha(p), p)) \leq H_{\beta+\omega^3}(p)$ para casi todo p. Ahora, escogemos p tal que $g = G_\alpha(p)$ y $\alpha = f_{g,p}(\omega)$. Dicho p existe por la Proposición 5.3.2 (deberá ser mayor que los coeficientes de la representación de α en base pura ω). Por lo tanto, tendremos:

$$h'(J(G_\alpha(p), p)) = h'(J(g, p)) = h(g, p) + p + 1 = H_\alpha(p + 1) = H_{\alpha+1}(p)$$

por el Teorema de Cichon. Además, como $\alpha + 1 > \beta + \omega^3$, por la Proposición 5.3.6 se tiene que $H_{\alpha+1}(p) = h'(J(G_\alpha(p), p)) > H_{\beta+\omega^3}(p)$ para casi todo p, con lo que llegamos a una contradicción.

Por consiguiente, el Teorema de Goodstein no puede probarse en PA. ⊠

Capítulo 6

Equivalencia entre PA y una teoría de conjuntos finitos.

A lo largo de este capítulo probaremos que PA es *esencialmente equivalente* a una teoría de conjuntos finitos muy concreta. Con esencialmente equivalente se quiere decir que una es interpretable en la otra y que ambas interpretaciones son inversas mutuamente. Veremos cuál es exactamente esta teoría y concretaremos las nociones de interpretación e inversa, para así entender el sentido exacto de esta *equivalencia*.

6.1. Interpretaciones.

Definición 6.1.1 *Sea $\mathcal{L}$ un lenguaje. Una teoría con lenguaje $\mathcal{L}$ es un conjunto consistente (no se puede deducir una contradicción) de sentencias de $\mathcal{L}$.*

A continuación, definiremos el concepto de *interpretación* entre dos teorías cuando el lenguaje de la primera es relacional. Este tipo de lenguaje sólo cuenta con un conjunto finito de símbolos de predicado o relación y una secuencia ordenada de variables. A diferencia de otros lenguajes de la lógica de primer orden, no cuenta con símbolos de función ni de constantes.

Una interpretación $\mathfrak{i}$ de una teoría T_2 con lenguaje $\mathcal{L}_2$ relacional en una teoría T_1 con lenguaje $\mathcal{L}_1$ viene dada por:

1. Una fórmula $\delta_{\mathfrak{i}}(v_0)$ de T_1 llamada *fórmula de dominio* cuya única variable es v_0.
2. Para cada símbolo de predicado R de $\mathcal{L}_2$ de aridad n, una fórmula asignada $R^{\mathfrak{i}}(v_1, \ldots, v_n)$ de $\mathcal{L}_1$ con las variables libres $v_1, \ldots, v_n$.
3. Se exige además que:
   - $T_1 \vdash \exists v_0 \delta_{\mathfrak{i}}(v_0)$.
   - Si σ es un axioma no lógico de T_2 o un axioma de igualdad (el axioma de identidad o un axioma de sustitución), entonces $T_1 \vdash \sigma^{\mathfrak{i}}$, donde $\sigma^{\mathfrak{i}}$ se define recursivamente con las reglas que siguen.

Sean φ y σ fórmulas de $\mathcal{L}_2$. Entonces:

- $(\neg\sigma)^{\mathfrak{i}} \equiv \neg\sigma^{\mathfrak{i}}$.
- $(\sigma \to \varphi)^{\mathfrak{i}} \equiv \sigma^{\mathfrak{i}} \to \varphi^{\mathfrak{i}}$.
- $(\forall x\sigma)^{\mathfrak{i}} \equiv \forall x(\delta_{\mathfrak{i}}(x) \to \sigma^{\mathfrak{i}})$.
- $(\exists x\sigma)^{\mathfrak{i}} \equiv \exists x(\delta_{\mathfrak{i}}(x) \wedge \sigma^{\mathfrak{i}})$.

Si $\mathfrak{i}$ es una interpretación de T_2 en T_1 escribiremos $\mathfrak{i} : T_2 \lhd T_1$.

Definición 6.1.2 *Diremos que dos interpretaciones* $\mathfrak{i} : T_2 \lhd T_1$ *y* $\mathfrak{j} : T_2 \lhd T_1$ *son iguales si:*

- $T_1 \vdash \delta_{\mathfrak{i}} \leftrightarrow \delta_{\mathfrak{j}}$.
- $T_1 \vdash (\delta_{\mathfrak{i}}(v_0) \wedge \cdots \wedge \delta_{\mathfrak{i}}(v_{n-1})) \to (R^{\mathfrak{i}}(v_0, \ldots, v_{n-1}) \leftrightarrow R^{\mathfrak{j}}(v_0, \ldots, v_{n-1}))$ *para todo predicado* R *de* $\mathcal{L}_2$ *de aridad* n.

Definición 6.1.3 *Dada una teoría* T*, la interpretación identidad* $\mathfrak{I}_T : T \lhd T$ *es la interpretación que cumple que* $R^{\mathfrak{i}}(v_0, \ldots, v_{n-1}) = R(v_0, \ldots, v_{n-1})$ *para todo predicado* R *de aridad* n.

Definición 6.1.4 *La composición* $\mathfrak{ji} : T_3 \lhd T_1$ *de dos interpretaciones* $\mathfrak{i} : T_3 \lhd T_2$ *y* $\mathfrak{j} : T_2 \lhd T_1$ *es la interpretación que cumple que:* $R^{\mathfrak{ji}}(v_0, \ldots, v_{n-1}) = (R^{\mathfrak{i}})^{\mathfrak{j}}(v_0, \ldots, v_{n-1})$ *para todo predicado* R *de* $\mathcal{L}_3$ *de aridad* n.

Definición 6.1.5 *Dos interpretaciones* $\mathfrak{i} : T \lhd S$ *y* $\mathfrak{j} : S \lhd T$ *son inversas mutuamente si* $\mathfrak{ij} = \mathfrak{I}_S$ *y* $\mathfrak{ji} = \mathfrak{I}_T$.

Proposición 6.1.6 *Sea* $\mathfrak{i} : T_2 \lhd T_1$ *una interpretación y supongamos que* $T_2 \vdash \sigma$ *para una fórmula* σ *de* $\mathcal{L}_2$*. Entonces,* $T_1 \vdash \sigma^{\mathfrak{i}}$.

Demostración: Si $T_2 \vdash \sigma$, entonces existe una demostración de σ en T_2. Es decir, existe una sucesión de fórmulas $\theta_1, \ldots, \theta_m$ tales que $\theta_m = \sigma$ y para cada $i = 1, \ldots, m$ se tiene una de las siguientes posibilidades:

1. θ_i es un axioma lógico.
2. θ_i es un axioma de T_2 o de igualdad.
3. Existen $j, k < i$ tales que θ_j es $\theta_k \to \theta_i$.
4. Existe $j < i$ tal que θ_i es $\forall x\theta_j(x)$.

Por tanto, para cada $i = 1, \ldots, m$ tendremos que:

1. Si θ_i es un axioma lógico, entonces, es fácil comprobar por la definición de interpretación que θ_i^{i} es equivalente a un axioma lógico de T_1. Por tanto, $T_1 \vdash \theta_i^{\mathsf{i}}$.

2. Si θ_i es un axioma de T_2 o de igualdad, entonces $T_1 \vdash \theta_i^{\mathsf{i}}$ por definición.

3. Si existen $j, k < i$ tales que θ_j es $\theta_k \to \theta_i$, entonces θ_j^{i} es $\theta_k^{\mathsf{i}} \to \theta_i^{\mathsf{i}}$.

4. Si existe $j < i$ tal que θ_i es $\forall x \theta_j(x)$, entonces θ_i^{i} es $\forall x \theta_j^{\mathsf{i}}(x)$.

Por consiguiente, es claro que a partir de la secuencia $\theta_1^{\mathsf{i}}, \ldots, \theta_m^{\mathsf{i}}$ es posible construir una demostración de σ^{i} en T_1. Por tanto, $T_1 \vdash \sigma^{\mathsf{i}}$. ⊠

Proposición 6.1.7 *Sean* $\mathsf{i} : T_2 \lhd T_1$ *y* $\mathsf{j} : T_2 \lhd T_1$ *dos interpretaciones iguales. Entonces, para cada fórmula* σ *de* $\mathcal{L}_2$ *tenemos* $T_1 \vdash \sigma^{\mathsf{i}} \leftrightarrow \sigma^{\mathsf{j}}$.

Demostración: Por inducción estructural sobre σ. ⊠

6.2. La interpretación de Ackermann.

En 1937, Ackermann observó que $\mathbb{N}$ con la siguiente relación de pertenencia:

$$n \in m \leftrightarrow \text{ el } n\text{-ésimo dígito de la representación binaria de } m \text{ es 1.}$$

satisface $\mathsf{ZF}_{\mathsf{fin}}$.

Si trabajamos en PA, se puede definir la interpretación estableciendo $\delta_{\mathfrak{a}}(x)$ como '$x = x$', $(x = y)^{\mathfrak{a}}$ como $'x = y'$ y $(x \in y)^{\mathfrak{a}}$ como:

$$\exists w < y \exists p \leq y \exists r < p(p = 2^x \wedge y = (2w + 1)p + r),$$

donde $p = 2^x$ debe ser reemplazado por la fórmula $Exp(2, x, p)$ que definimos en el Capítulo 4.

Por simplicidad en la notación, escribimos 0 y 1 en lugar de $\mathbf{0}$ y $\mathbf{1}$ y n en lugar de Λ_n.

En un principio, esta interpretación puede resultar poco intuitiva. Por ello, vamos a interpretar algunas fórmulas como ejemplo para ver qué conjuntos se corresponden con los primeros numerales.

$$(y = \varnothing)^{\mathfrak{a}} \leftrightarrow (\neg \exists x (x \in y))^{\mathfrak{a}} \leftrightarrow \neg \exists x [x = x \wedge (x \in y)^{\mathfrak{a}}] \leftrightarrow \neg \exists x (x \in y)^{\mathfrak{a}} \leftrightarrow y = 0$$

La última equivalencia asume que si y no tiene ningún dígito que sea 1 en su representación binaria es porque $y = 0$. Esta equivalencia puede ser probada fácilmente en PA por reducción al absurdo para ambas implicaciones.

$$(y = \{\varnothing\})^{\mathfrak{a}} \leftrightarrow [\forall x(x \in y \leftrightarrow x = \varnothing)]^{\mathfrak{a}} \leftrightarrow \forall x[(x \in y)^{\mathfrak{a}} \leftrightarrow x = 0] \leftrightarrow y = 1$$

De nuevo, la última equivalencia puede probarse en PA sin mucha dificultad. Observamos que el 0 y el 1 coinciden con los conjuntos que definimos como números naturales en $\mathsf{ZF_{fin}}$. Sin embargo, a partir del 2 esto va a cambiar, ya que según esta interpretación, los elementos de un conjunto y en $\mathsf{ZF_{fin}}$ son "los conjuntos que corresponden a los coeficientes que son 1 en su representación binaria". En cambio, los números naturales en $\mathsf{ZF_{fin}}$ tienen como elementos a todos los números naturales menores que él mismo.

$$(y = \{\{\varnothing\}\})^{\mathfrak{a}} \leftrightarrow [\forall x(x \in y \leftrightarrow x = \{\varnothing\})]^{\mathfrak{a}} \leftrightarrow \forall x[(x \in y)^{\mathfrak{a}} \leftrightarrow x = 1] \leftrightarrow y = 2$$

Procediendo de esta manera, obtendríamos que $(y = \{\varnothing, \{\varnothing\}\})^{\mathfrak{a}} \leftrightarrow y = 3$, $(y = \{\{\{\varnothing\}\}\})^{\mathfrak{a}} \leftrightarrow y = 4, \ldots$

Es directo, aunque muy laborioso, probar el siguiente resultado:

Teorema 6.2.1 $\mathfrak{a} : \mathsf{ZF_{fin}} \lhd \mathsf{PA}$ *($\mathfrak{a}$ es una interpretación de $\mathsf{ZF_{fin}}$ en PA).*

Para definir la inversa de la interpretación de Ackermann necesitamos considerar el principio de ϵ-inducción el cual definimos a continuación.

Definición 6.2.2 *Sea $\varphi(x, y_1, \ldots, y_k)$ una fórmula de $\mathcal{L}_\epsilon$. $I_\epsilon\varphi$ es la sentencia:*

$$\forall y_1, \ldots, y_k[\forall x(\forall w \in x\varphi(w, y_1, \ldots, y_k) \to \varphi(x, y_1, \ldots, y_k)) \to \forall x\varphi(x, y_1, \ldots, y_k)].$$

ϵ-Ind denota el esquema $\{I_\epsilon\psi : \psi(x, y_1, \ldots, y_k)$ es una $\mathcal{L}_\epsilon$-fórmula$\}$.

Resulta que no todos los modelos de $\mathsf{ZF_{fin}}$ admiten ϵ-Ind. Vamos a ver la noción de cierre transitivo, que está estrechamente relacionada con ésta.

Definición 6.2.3 *Decimos que y es el cierre transitivo de x ($y = TC(x)$) si:*

$$x \subseteq y \wedge Trans(y) \wedge \forall y'(x \subseteq y' \wedge Trans(y') \to y \subseteq y').$$

Definición 6.2.4 *Designamos como **TC** al 'Axioma del Cierre Transitivo', que se expresa con la siguiente fórmula:*

$$\forall x \exists u(x \subseteq u \wedge Trans(u)).$$

Lema 6.2.5 $\mathsf{EST} \vdash \forall x[\exists y(x \subseteq y \wedge Trans(y)) \leftrightarrow \exists y(TC(x) = y)]$.

Demostración: La implicación de derecha a izquierda es inmediata. Vayamos con la contraria. Sea x cualquiera tal que existe y con $x \subseteq y$ y $Trans(y)$.

Sea $A = \{a \in y : \forall z[(x \subseteq z \wedge Trans(z)) \to a \in z]\}$. Tal A existe por **Sep**. Claramente, $A = TC(x)$. ⊠

Proposición 6.2.6 $\mathsf{EST} + \boldsymbol{Reg} \vdash \epsilon\text{-}Ind \leftrightarrow \boldsymbol{TC}$.

Demostración: Para la implicación de izquierda a derecha. Supongamos que se tiene $\mathsf{EST}+$ ϵ-Ind (**Reg** no será necesario). Hay que probar que se cumple **TC**. Lo hacemos por ϵ-inducción en $x \in V$, siendo x tal que todos sus elementos tienen cierre transitivo (tengamos en cuenta la equivalencia del Lema 6.2.5).

Consideremos el conjunto $A = \bigcup\{z : \exists x' \in x(z = TC(x'))\} \bigcup x$, que existe por **Unión**. Veamos que A es transitivo: sea $a \in b$ y $b \in A$. Si $b \in x$, entonces $TC(b) \subseteq A$. Por tanto, $a \in A$. Si $b \in TC(x')$ para algún $x' \in x$, entonces $a \in TC(x')$ por transitividad y, por tanto, $a \in A$.

Ya hemos encontrado pues un conjunto transitivo que contiene a x. Así, por ϵ-inducción, esto se cumple para todo $x \in V$ y $\mathsf{EST} \vDash \epsilon\text{-}Ind \rightarrow \mathbf{TC}$.

Para la implicación de derecha a izquierda. Supongamos que se tiene $\mathsf{EST}+\mathbf{Reg}+\mathbf{TC}$. Hay que probar que se cumple $\epsilon\text{-}Ind$.

Sean $y_1, \ldots, y_k, \varphi$ cualesquiera. Supongamos que

$$\forall x[(\forall w \in x\varphi(w, y_1, \ldots, y_k)) \rightarrow \varphi(x, y_1, \ldots, y_k)].$$

Por reducción al absurdo, supongamos que existe z tal que $\neg\varphi(z, y_1, \ldots, y_k)$.

Sea $M = \{m \in TC(z) : \neg\varphi(m, y_1, \ldots, y_k)\} \neq \varnothing$, que existe por **Sep**. Por **Reg**, existe $m^* \in M$ tal que para todo $m \in M, m \notin m^*$. Tenemos entonces $\neg\varphi(m^*, y_1, \ldots, y_k)$ y $\varphi(p, y_1, \ldots, y_k)$ para todo $p \in m^*$. Así, por hipótesis, tendría que darse $\varphi(m^*, y_1, \ldots, y_k)$ y llegamos a una contradicción. Por tanto, $\forall x\varphi(x, y_1, \ldots, y_k)$ y $\mathsf{EST} + \mathbf{Reg} \vdash \mathbf{TC} \rightarrow \epsilon\text{-}Ind$. ⊠

El siguiente resultado implica que **TC** no se puede demostrar en $\mathsf{ZF_{fin}}$.

Teorema 6.2.7 $\mathsf{ZF_{fin}} \cup \{\neg \boldsymbol{TC}\}$ *es consistente.*

⊠

Por tanto, necesitamos añadir la hipótesis extra **TC** para que la ϵ-inducción funcione.

La siguiente proposición, que no probaremos, demuestra que cualquier inversa de la interpretación de Ackermann usa **TC** en alguna forma.

Proposición 6.2.8 *Sea* $\mathfrak{a} : \mathsf{ZF_{fin}} \lhd \mathsf{PA}$ *la interpretación de Ackermann. Entonces,* $\mathsf{PA} \vdash \boldsymbol{TC}^{\mathfrak{a}}$.

⊠

De este modo, si $\mathfrak{b} : \mathsf{PA} \lhd \mathsf{ZF_{fin}}$ es inversa de $\mathfrak{a}$, entonces tendríamos $\mathsf{ZF_{fin}} \vdash (TC^{\mathfrak{a}})^{\mathfrak{b}}$. Y por la Proposición 6.1.7 y la definición de inversa $\mathsf{ZF_{fin}} \vdash \mathbf{TC}$, lo cual es imposible por el Teorema 6.2.7.

Por consiguiente, si se quiere definir la inversa de la interpretación de Ackermann sin incurrir en la contradicción anterior, debemos considerar la teoría $\mathsf{ZF_{fin}}^* = \mathsf{ZF_{fin}} + \mathbf{TC}$.

6.3. La interpretación Ordinal.

Recordemos la definición y propiedades que vimos de los números ordinales en ZF. A continuación, trabajaremos con ellos en $\mathsf{ZF_{fin}}$. Por tanto, muchas de sus propiedades seguirán intactas y podremos utilizar todas aquellas en las que no intervenga **Inf**. Otras, sin embargo, cambiarán, ya que nos estamos limitando únicamente a los ordinales finitos, es decir, a los números naturales.

En la sección 6.1 vimos lo que era una interpretación de una teoría con lenguaje relacional en otra. A continuación, vamos a definir una *interpretación* de una teoría en otra donde el lenguaje de la primera no tiene por qué ser relacional (será el lógico de primer orden, que incluye símbolos de constante y de función).

Definición 6.3.1 *Sea $\mathcal{L}$ un lenguaje. Llamamos fórmulas atómicas sin anidación de $\mathcal{L}$ a las fórmulas de la forma:*

- $x = y$ para dos variables x e y.
- $R(x_1, \ldots, x_n)$ para un símbolo de predicado R de aridad n y variables $x_1, \ldots, x_n$.
- $c = x$ para una constante c y una variable x.
- $f(x_1, \ldots, x_n) = y$ para un símbolo de función f y variables $x_1, \ldots, x_n, y$.

Lema 6.3.2 *Para toda fórmula atómica $\theta(x_1, \ldots, x_n)$ existe una fórmula $\alpha(x_1, \ldots, x_n, z_1, \ldots, z_m)$ que es una conjunción de fórmulas atómicas sin anidación y que verifica que*

$$\theta(x_1, \ldots, x_n) \leftrightarrow \exists z_1 \ldots \exists z_m \alpha(x_1, \ldots, x_n, z_1, \ldots, z_m).$$

Denotaremos esta fórmula por $\theta_\exists(x_1, \ldots, x_n)$.

Demostración: Se prueba por inducción estructural sobre fórmulas atómicas. ⊠

Una interpretación $\mathfrak{i}$ de una teoría T_2 con lenguaje $\mathcal{L}_2$ en una teoría T_1 con lenguaje $\mathcal{L}_1$ viene dada por:

1. Una fórmula $\delta_\mathfrak{i}(v_0)$ de T_1 llamada *fórmula de dominio* cuya única variable es v_0.
2. Para cada símbolo de predicado R de $\mathcal{L}_2$ de aridad n, una fórmula asignada $R^\mathfrak{i}(v_1, \ldots, v_n)$ de $\mathcal{L}_1$ con las variables libres $v_1, \ldots, v_n$.
3. Para cada símbolo de función f de $\mathcal{L}_2$ de aridad n, una fórmula asignada $(f(v_1, \ldots, v_n) = v_{n+1})^\mathfrak{i}$ de $\mathcal{L}_1$ con las variables libres $v_1, \ldots, v_n, v_{n+1}$.
4. Para cada símbolo de constante c de $\mathcal{L}_2$, una fórmula asignada $(c = v_1)^\mathfrak{i}$ de $\mathcal{L}_1$ con la variable libre v_1.
5. Se exige además que:

- $T_1 \vdash \exists v_0 \delta_{\mathfrak{i}}(v_0)$.
- Para cada símbolo de constante c, $T_1 \vdash \exists! x(c = x)^{\mathfrak{i}}$.
- Para cada símbolo de función f de aridad n,

$$T_1 \vdash \forall x_1 \ldots \forall x_n \exists! y(f(x_1, \ldots, x_n) = y)^{\mathfrak{i}}.$$

- Si σ es un axioma no lógico de T_2 o un axioma de igualdad (el axioma de identidad o un axioma de sustitución), entonces $T_1 \vdash \sigma^{\mathfrak{i}}$, donde $\sigma^{\mathfrak{i}}$ se define como en el caso relacional salvo que cada fórmula atómica $\theta(x_1, \ldots, x_n)$ se sustituye previamente por $\theta_\exists(x_1, \ldots, x_n)$, que es la que se interpreta.

Definamos ahora la interpretación ordinal, $\mathfrak{o}$, de PA en los naturales en $\mathsf{ZF_{fin}}$.

Definición 6.3.3 *Establecemos* $\delta_{\mathfrak{o}}(x)$ *como* $'x \in \mathbf{On}'$; $(x = y)^{\mathfrak{o}}$ *como* $'x = y'$; $(x < y)^{\mathfrak{o}}$ *como* $'x \in y'$; $(x + y = z)^{\mathfrak{o}}$ *como* $'x + y = z'$ *(suma ordinal);* $(x \cdot y = z)^{\mathfrak{o}}$ *como* $'x \cdot y = z'$ *(multiplicación ordinal);* $(x = 0)^{\mathfrak{o}}$ *como* $'\neg\exists y(y \in x)'$ *y* $(x = 1)^{\mathfrak{o}}$ *como* $'\forall y(y \in x \leftrightarrow \neg\exists z(z \in y)'$.

La interpretación ordinal es mucho más natural e intuitiva que la interpretación de Ackermann. En este caso, el orden $<$ de PA se interpreta como la relación de pertenencia entre ordinales, que coincide precisamente con el buen orden de los números naturales. Por tanto, cada numeral n de PA sí corresponderá con el ordinal n de $\mathsf{ZF_{fin}}$.

Teorema 6.3.4 $\mathfrak{o} : \mathsf{PA} \lhd \mathsf{ZF_{fin}}$.

Demostración: Bastará con comprobar que $\mathsf{ZF_{fin}} \vdash \sigma^{\mathfrak{o}}$ para todo axioma σ de PA. Recordemos cómo se presentaban los axiomas de PA en el Capítulo 3. Seguiremos ese mismo orden:

1. Comencemos por la asociatividad. Debemos probar que:

$$\mathsf{ZF_{fin}} \vdash (\forall x \forall y \forall z(x + (y + z) = (x + y) + z))^{\mathfrak{o}}.$$

   Por la definición recursiva de interpretación esta fórmula es equivalente a:

$$\forall x \forall y \forall z(x, y, z \in \mathbf{On} \to (x + (y + z) = (x + y) + z))^{\mathfrak{o}}).$$

   A continuación, para interpretar la fórmula que nos queda, debemos expresarla como una conjunción de fórmulas atómicas sin anidación precedida de los cuantificadores existenciales:

$$(x+(y+z) = (x+y)+z))^{\mathfrak{o}} \leftrightarrow (\exists u \exists v \exists w(y+z = u \wedge x+y = v \wedge v+z = w \wedge x+u = w))^{\mathfrak{o}}.$$

Por equivalencia lógica, las interpretaciones respetan la conjunción y por la definición recursiva de interpretación y la definición de $\mathfrak{o}$ respecto de la suma, la última fórmula es equivalente a:

$$\exists u \exists v \exists w (u, v, w \in \mathbf{On} \wedge y + z = u \wedge x + y = v \wedge v + z = w \wedge x + u = w),$$

que es a su vez equivalente a:

$$x + (y + z) = (x + y) + z.$$

Esto, claramente, se satisface en $\mathsf{ZF}_{\mathsf{fin}}$ para cualesquiera ordinales x, y, z por la propiedad asociativa de la suma ordinal.

Una vez que hemos visto cómo funciona $\mathfrak{o}$, no es necesario que escribamos la interpretación para las fórmulas de la asociatividad del producto y la distributividad del producto respecto de la suma, ya que se procede de manera análoga.

Con la interpretación de los axiomas de la conmutatividad también se procede de este modo. Obtendríamos que en $\mathsf{ZF}_{\mathsf{fin}}$, las fórmulas

$$(\forall x \forall y (x + y = y + x))^{\mathfrak{o}} \text{ y } (\forall x \forall y (x \cdot y = y \cdot x))^{\mathfrak{o}}$$

son equivalentes a las fórmulas

$$\forall x \forall y (x, y \in \mathbf{On} \to (x + y = y + x)) \text{ y } \forall x \forall y (x, y \in \mathbf{On} \to (x \cdot y = y \cdot x))$$

respectivamente.

Sin embargo, recordemos que la suma y la multiplicación ordinal no son conmutativas. Por tanto, debemos probar que estas fórmulas se satisfacen para los ordinales finitos. Para ello, vamos a utilizar el principio de inducción de los números naturales que vimos en el Teorema 2.2.8.

Como es natural, la adición ordinal en $\mathsf{ZF}_{\mathsf{fin}}$ se define como en ZF quitando el caso de ordinal límite. Es decir, $m + 0 = m$ y $m + n^+ = (m + n)^+$ para cualesquiera ordinales m, n. Antes de probar su conmutatividad vamos a ver primero un par de resultados.

Lema 1: $0 + n = n \ \forall n \in \mathbf{On}$ (en $\mathsf{ZF}_{\mathsf{fin}}$).

Demostración: Por inducción. $0+0 = 0$. Si $0+n = n$, entonces $0+n^+ = 0+(n+1) = (0 + n) + 1 = n^+$. Así, se cumple para todo n.

Lema 2: $m^+ + n = (m + n)^+ \ \forall m, n \in \mathbf{On}$ (en $\mathsf{ZF}_{\mathsf{fin}}$).

Demostración: Por inducción sobre n: $m^+ + 0 = m^+ = (m+0)^+$. Supongamos ahora que se cumple para cierto n. Entonces, $m^+ + n^+ = (m^+ + n)^+ = ((m + n)^+)^+ = (m + n^+)^+$.

Equipados con estos resultados, probemos por inducción en n que $m + n = n + m$ con m cualquiera: $m + 0 = m = 0 + m$. Supongamos ahora que se cumple para n. Entonces, $m + n^+ = (m + n)^+ = (n + m)^+ = n^+ + m$. Con esto, queda probada la conmutatividad para la adición ordinal en $\mathsf{ZF}_{\mathsf{fin}}$.

Al igual que con la adición, la multiplicación ordinal en $\mathsf{ZF}_{\mathsf{fin}}$ se define como $m \cdot 0 = 0$ y $m \cdot n^+ = m \cdot n + m$ para cualesquiera $m, n \in \mathbf{On}$. Veamos primero un resultado técnico.

Lema 3: $0 \cdot n = 0\ \forall n \in \mathbf{On}$ (en $\mathsf{ZF}_{\mathsf{fin}}$).

Demostración: Por inducción sobre n. $0 \cdot 0 = 0$. Supongamos que se cumple para un n cualquiera. Entonces, $0 \cdot n^+ = 0 \cdot n + 0 = 0 + 0 = 0$.

Veamos ahora por inducción en n que $m \cdot n = n \cdot m$ para m fijo cualquiera. $m \cdot 0 = 0 = 0 \cdot m$. Supongamos que se cumple para n cualquiera. Se tiene que $m \cdot n^+ = m \cdot n + m = n \cdot m + m = (n + 1) \cdot m = n^+ \cdot m$. Con esto, queda probada la conmutatividad de la multiplicación de los ordinales en $\mathsf{ZF}_{\mathsf{fin}}$.

Por último, quedan los axiomas de los elementos neutros de la suma y el producto.

En primer lugar, hay que probar que $\mathsf{ZF}_{\mathsf{fin}} \vdash (\forall x(x + 0 = x))^{\mathbf{o}}$. Se tiene que:

$$(\forall x(x + 0 = x))^{\mathbf{o}} \leftrightarrow \forall x(x \in \mathbf{On} \rightarrow \exists u(u \in \mathbf{On} \wedge (u = 0)^{\mathbf{o}} \wedge (x + u = x)^{\mathbf{o}})).$$

En realidad, la fórmula $(u = 0)^{\mathbf{o}}$ (equivalente a $\neg\exists y(y \in u)$) la abreviamos como $'u = \varnothing'$ (recordemos que en **Vacío** asignábamos este símbolo al conjunto vacío). Como en los ordinales $\varnothing$ corresponde al ordinal 0, finalmente nos quedaría:

$$\forall x(x \in \mathbf{On} \rightarrow \exists u(u \in \mathbf{On} \wedge u = 0 \wedge (x + u = x))),$$

que se satisface en $\mathsf{ZF}_{\mathsf{fin}}$ por la definición de suma ordinal.

A continuación, nos queda ver que $\mathsf{ZF}_{\mathsf{fin}} \vdash (\forall x(x \cdot 1 = x))^{\mathbf{o}}$. De manera análoga a lo que acabamos de hacer, obtendríamos la siguiente fórmula:

$$\forall x(x \in \mathbf{On} \rightarrow \exists u(u \in \mathbf{On} \wedge (u = 1)^{\mathbf{o}} \wedge x \cdot u = x)).$$

$(u = 1)^{\mathbf{o}} \leftrightarrow u = \{\varnothing\}$. Como en los ordinales $\{\varnothing\}$ corresponde al ordinal 1, ésto último es equivalente a $'u = 1'$. Ya sólo nos queda ver que para todo $x \in \mathbf{On}$, $x \cdot 1 = x$.

Por inducción: $0 \cdot 1 = 0$; supongamos que se cumple para x. Tenemos que

$$(x + 1) \cdot 1 = (x + 1) \cdot 0 + (x + 1) = x + 1.$$

2. Ahora debemos interpretar la ley de la resta. Hay que comprobar que

$$\mathsf{ZF_{fin}} \vdash (\forall x \forall y \forall z (x + z = y + z \to x = y))^{\mathfrak{o}}.$$

Aplicando la definición recursiva de interpretación, se tiene que esta fórmula es equivalente a:

$$\forall x \forall y \forall z (x, y, z \in \mathbf{On} \to ((x + z = y + z)^{\mathfrak{o}} \to x = y)).$$

La fórmula $(x + z = y + z)^{\mathfrak{o}}$ es equivalente a $(\exists u(x + z = u \wedge y + z = u))^{\mathfrak{o}}$. Ya expresada de esta manera procedemos a su interpretación y obtenemos lo siguiente:

$$\exists u(u \in \mathbf{On} \wedge x + z = u \wedge y + z = u).$$

De esta manera, aplicando la conmutatividad de la adición en $\mathsf{ZF_{fin}}$, se tiene que $z + x = z + y$. Por las propiedades de los ordinales , esto último implica que $x = y$. Por tanto, se satisface en $\mathsf{ZF_{fin}}$ la fórmula inicial.

3. A continuación, hay que ver que $\mathsf{ZF_{fin}} \vdash (x \neq 0 \leftrightarrow \exists y(x = y + 1))^{\mathfrak{o}}$, lo cual es equivalente a:

$$x \neq \varnothing \leftrightarrow (\exists y(x = y + 1))^{\mathfrak{o}}$$

por la definición recursiva de interpretación. Además, el lado derecho de la implicación lo reexpresamos como:

$$(\exists y \exists u(u = 1 \wedge y + u = x))^{\mathfrak{o}},$$

lo cual se puede interpretar para obtener algo como lo siguiente:

$$\exists y \exists u(u = 1 \wedge y + u = x).$$

Por tanto, la fórmula inicial se satisface por el Teorema 2.2.6 y teniendo en cuenta que el ordinal $y + 1$ es $y \cup \{y\}$.

4. Vayamos con el axioma de inducción. Sean $F(x)$ y x una fórmula y una variable de PA respectivamente.
$((F(0) \wedge \forall x[F(x) \to F(x + 1)]) \to \forall x F(x))^{\mathfrak{o}} \leftrightarrow$
$(F(0) \wedge \forall x[F(x) \to F(x + 1)])^{\mathfrak{o}} \to (\forall x F(x))^{\mathfrak{o}} \leftrightarrow$
$(F(0))^{\mathfrak{o}} \wedge \forall x(x \in On \to [F(x) \to F(x + 1)]^{\mathfrak{o}}) \to (\forall x F(x))^{\mathfrak{o}}.$

Llegados a este punto, iremos por partes. En primer lugar:

$$(F(0))^{\mathfrak{o}} \leftrightarrow (\exists u[0 = u \wedge F(u)])^{\mathfrak{o}} \leftrightarrow \exists u[u \in On \wedge 0 = u \wedge (F(u))^{\mathfrak{o}}]$$

A la fórmula $(F(u))^{\mathfrak{o}}$ la renombramos como $G(u)$. Por tanto, finalmente obtendríamos que:

$$(F(0))^{\mathfrak{o}} \leftrightarrow G(0).$$

Por otro lado tenemos que:

$$[F(x) \to F(x{+}1)]^{\mathfrak{o}} \leftrightarrow (F(x))^{\mathfrak{o}} \to (F(x{+}1))^{\mathfrak{o}} \leftrightarrow G(x) \to \exists u \exists v(u, v \in \mathbf{On} \wedge 1 = u \wedge x{+}u = v \wedge G(v)).$$

Por tanto, se tiene que:

$$[F(x) \to F(x+1)]^{\mathfrak{o}} \leftrightarrow (G(x) \to G(x+1)).$$

Por último:

$$(\forall x F(x))^{\mathfrak{o}} \leftrightarrow \forall x(x \in \mathbf{On} \to G(x)).$$

En conclusión, si sustituimos cada fórmula por su equivalente ya interpretada en $\mathsf{ZF}_{\mathsf{fin}}$, obtenemos el principio de inducción para los naturales para la fórmula G, que se satisface por el Teorema 2.2.8.

Con esto, queda demostrado que para todo axioma σ de PA se tiene que $\mathsf{ZF}_{\mathsf{fin}} \vdash \sigma$. ⊠

La interpretación ordinal $\mathfrak{o}$ no es inversa de la interpretación de Ackermann, aunque la utilizaremos para definir una interpretación que sí lo es.

6.4. La inversa de la interpretación de Ackermann.

Equipados con la ϵ-inducción obtendremos una interpretación $\mathfrak{b} : \mathsf{PA} \lhd \mathsf{ZF}_{\mathsf{fin}}{}^*$ inversa de $\mathfrak{a}$. Para ello, primero debemos definir una biyección $p : V \to \mathbf{On}$, donde V es el universo de los conjuntos de $\mathsf{ZF}_{\mathsf{fin}}{}^*$. Esta biyección tomará parte en la definición de $\mathfrak{b}$ que daremos más adelante.

Definición 6.4.1 *Sea $\mathcal{P}(\mathbf{On})$ la clase que contiene a todos los conjuntos de ordinales. Es decir,*

$$\mathcal{P}(\mathbf{On}) = \{x : x \subseteq \mathbf{On}\}.$$

Vamos a definir recursivamente la función $\Sigma' : \mathbf{On} \times \mathcal{P}(\mathbf{On}) \to \mathbf{On}$.

$$\Sigma'(0,x) = 0 \qquad \text{para todo } x \in \mathcal{P}(\mathbf{On})$$

$$\Sigma'(c \cup \{c\}, x) = \Sigma'(c,x) \qquad \text{si } c \cup \{c\} \notin x$$

$$\Sigma'(c \cup \{c\}, x) = \Sigma'(c,x) + (c \cup \{c\}) \qquad \text{si } c \cup \{c\} \in x$$

La función $\Sigma'(c,x)$ no hace otra cosa que sumar todos los ordinales de x que sean menores o iguales que el ordinal c.

Definición 6.4.2 *Se define la función* $\Sigma : \mathcal{P}(\mathbf{On}) \to \mathbf{On}$ *como*

$$\Sigma(x) = \Sigma'(\cup x, x).$$

Recordemos que, según el Corolario 2.2.7, si $x \neq \varnothing$ entonces $\cup x$ pertenece a x y es su elemento máximo. Por tanto, $\Sigma(x)$ suma todos los ordinales que pertenecen a x.

Proposición 6.4.3 *Σ' y Σ son funciones en $\mathsf{ZF}_{\mathsf{fin}}{}^*$.*

Demostración: Por el Teorema de Recursión (2.3.6). ⊠

Definición 6.4.4 *Sea V el universo de $\mathsf{ZF}_{\mathsf{fin}}{}^*$, se define $p : V \to \mathbf{On}$ recursivamente como sigue:*

$$p(x) = \Sigma(\{2^{p(y)} \in \mathbf{On} : y \in x\}).$$

Recordemos que $\mathfrak{a}$ interpreta a cada conjunto x de $\mathsf{ZF}_{\mathsf{fin}}{}^*$ como el número que resulta de desarrollar la interpretación binaria en la que los coeficientes que son 1 son exactamente las interpretaciones de los $y \in x$. Pues bien, pensemos en p como en la función que desarrolla esa interpretación binaria, pero en lugar de devolvernos el número nos devuelve el número natural en forma de ordinal. Por ejemplo:

$$p(\{\{\varnothing\}\}) = \Sigma(\{2^{p(\{\varnothing\})}\}) = 2^{p(\{\varnothing\})} = 2^{\Sigma(\{2^{\varnothing}\})} = 2^{\Sigma(\{1\})} = 2^1 = 2.$$

Efectivamente, recordemos que $\mathsf{PA} \vdash (x = \{\{\varnothing\}\})^{\mathfrak{a}} \leftrightarrow x = 2$.

Proposición 6.4.5 *$\mathsf{ZF}_{\mathsf{fin}}{}^*$ prueba que p es una función biyectiva.*

Demostración: Por ϵ-inducción.

En primer lugar, supongamos que $p(x) = p(x')$ para $x, x' \in V$ tales que p es inyectiva para todo $y \in x \cup x'$. Entonces, $\sum_{y \in x} 2^{p(y)} = \sum_{y' \in x'} 2^{p(y')}$ (sumatorio de ordinales). Por hipótesis de inducción y por el Teorema de la Forma Normal de Cantor (2.4.4), x y x' deben tener los mismos elementos y $x = x'$. Así, p es inyectiva.

Ahora, sea $\alpha \in \mathbf{On}$ y supongamos que para todo $\beta \in \alpha$ existe $x_\beta \in V$ tal que $p(x_\beta) = \beta$. Entonces, por el Teorema de la Forma Normal de Cantor existen ordinales $\beta_0, \ldots, \beta_n$ únicos tales que

$$\alpha = 2^{\beta_0} + \cdots + 2^{\beta_n}.$$

y sabemos que $\beta_i < \alpha$ para todo $i = 0, \ldots, n$. Entonces, por hipótesis de inducción, existen conjuntos x_{β_i} tales que $p(x_{\beta_i}) = \beta_i$ para todo $i = 0, \ldots, n$. De esta manera, se tiene que:

$$\alpha = 2^{p(x_{\beta_0})} + \cdots + 2^{p(x_{\beta_n})} = p(\{x_{\beta_0}, \ldots, x_{\beta_n}\}).$$

Por tanto, se tiene que p es sobreyectiva. ⊠

A continuación, vamos a definir la interpretación $\mathfrak{b}$.

Definición 6.4.6 *Establecemos $\delta_{\mathfrak{b}}(x)$ como $'x = x'$; $(x = y)^{\mathfrak{b}}$ como $'x = y'$; $(x < y)^{\mathfrak{b}}$ como $'p(x) < p(y)'$; $(x+y = z)^{\mathfrak{b}}$ como $'p(x)+p(y) = p(z)'$; $(x \cdot y = z)^{\mathfrak{b}}$ como $'p(x) \times p(y) = p(z)'$; $(x = 0)^{\mathfrak{b}}$ como $'\neg\exists y(y \in x)'$ y $(x = 1)^{\mathfrak{b}}$ como $'\forall y(y \in x \leftrightarrow \neg\exists z(z \in y)'$, donde $<, +$ y $\cdot$ son el orden y las funciones usuales de los ordinales.*

Teorema 6.4.7 $\mathfrak{b} : \mathsf{PA} \lhd \mathsf{ZF_{fin}}^*$.

Demostración: Sigue del Teorema 6.3.4 y de la Proposición 6.4.5. ⊠

Teorema 6.4.8 *Las interpretaciones $\mathfrak{a} : \mathsf{ZF_{fin}}^* \to \mathsf{PA}$ y $\mathfrak{b} : \mathsf{PA} \lhd \mathsf{ZF_{fin}}^*$ son inversas mutuamente.*

Demostración: Hay que probar que $\mathfrak{ba} = \mathfrak{I}_{\mathsf{ZF}^*_{\mathsf{fin}}}$ y $\mathfrak{ab} = \mathfrak{I}_{\mathsf{PA}}$. En realidad, no haremos una demostración completa sino que realizaremos algunas indicaciones. Para la primera igualdad, basta con comprobar que:

$$\mathsf{ZF_{fin}}^* \vdash ((x \in y)^{\mathfrak{a}})^{\mathfrak{b}} \leftrightarrow x \in y.$$

$(x \in y)^{\mathfrak{a}}$ se satisface en PA si y sólo si el x-ésimo dígito de la representación binaria de y es 1. Pero esto, al ser interpretado con $\mathfrak{b}$, es equivalente a que $2^{p(x)}$ aparezca en la Forma Normal de Cantor (única) en base 2 de $p(y)$. Por lo que, por la definición de p y su biyectividad, no queda otra que $x \in y$.

Para probar $\mathfrak{ab} = \mathfrak{I}_{\mathsf{PA}}$, como $\mathcal{L}_{\mathsf{PA}}$ no es un lenguaje relacional, debe probarse la equivalencia para todas las fórmulas atómicas sin anidación que definen la interpretación $\mathfrak{ab}$. Debemos comprobar en primer lugar que:

$$\mathsf{PA} \vdash (x = 0)^{\mathfrak{b}})^{\mathfrak{a}} \leftrightarrow x = 0 \qquad \text{y}$$

$$\mathsf{PA} \vdash (x = 1)^{\mathfrak{b}})^{\mathfrak{a}} \leftrightarrow x = 1.$$

Ya vimos anteriormente que $(x = \varnothing)^{\mathfrak{a}}$ es equivalente a $x = 0$ y $(x = \{\varnothing\})^{\mathfrak{a}}$ es equivalente a $x = 1$. Por tanto, lo anterior es directo. A continuación, hay que ver que:

$$\mathsf{PA} \vdash x + y = z \leftrightarrow ((x + y = z)^{\mathfrak{b}})^{\mathfrak{a}}.$$

Ésto puede probarse por inducción en y. El producto se hace de manera análoga. Además, téngase en cuenta que como el símbolo de relación '$<$' se define en PA a partir de la suma, no hace falta hacer prueba para éste. ⊠

Bibliografía

[1] Zofia Adamowicz y Pawel Zbierski, *"Logic of Mathematics: A Modern Course of Classical Logic"*. John Wiley & Sons, Inc. 1997.

[2] Stefano Baratella y Ruggero Ferro, *"A Theory of Sets with the Negation of the Axiom of Infinity"*. Mathematical Logic Quarterly, volumen 39 , páginas 338-352, 1993.

[3] E. A. Cichon. *A short proof of the recently discovered independence results using recursion theoretic methods*. Proc. Amer. Math. Soc. 87 (1983), 704-706.

[4] Hodges, W. *Model Theory*. Encyclopedia of Mathematics and its Applications. Cambridge: Cambridge University Press, 1993.

[5] Richard Kaye y Tin Lok Wong, *"On Interpretations of Arithmetic and Set Theory"*. Notre Dame Journal of Formal Logic, volumen 48, número 4, 2007.

[6] Gaisi Takeuti y Wilson M. Zaring, *"Introduction to Axiomatic Set Theory"*. Springer-Verlag New York Inc., 1982.

[7] Visser, A. *Categories of theories and interpretations*. En A. Enayat, I. Kalantari, & M. Moniri (Eds.), Logic in Tehran (Lecture Notes in Logic, pp. 284-341). Cambridge: Cambridge University Press, 2006.

[8] S. S. Wainer. *A classification of the ordinal recursive functions*. Arch. Math. Logik Grundlagenforsch. 13 (1970), 136-153.

[9] S. S. Wainer. *Ordinal recursion and a refinement of the Gnegorczyk hierarchy*. J. Symb. Logic 37 (1972), 281-292.