TEOREMA DE GOODSTEIN: UN PROBLEMA DE TEORÍA DE NÚMEROS RESUELTO CON TEORÍA DE CONJUNTOS

MÓNICA ANDREA CELIS CERÓN

Universidad del Cauca

Facultad de Ciencias Naturales, Exactas y de la Educación

Departamento de Matemáticas

Popayán

2010

Nota de Aceptación

_____

_____

_____

_____

Prof. Fredy William Bustos
Director

_____

Lic. Luz Victoria de la Pava
Comité de seguimiento

_____

Prof. Wilson Martínez
Comité de seguimiento

Fecha de sustentación: Popayán, 01 de octubre de 2010.

TABLA DE CONTENIDO

PREFACIO

Este trabajo se desarrolla en la modalidad de Seminario de Grado. Es una monografía producto del estudio de ciertos artículos además de lo desarrollado en los cursos electivos y en el seminario de Teoría de Conjuntos.

El trabajo de divide en dos capítulos. En el primer capítulo se presenta algunos aspectos de la Tería de Ordinales como lo son: la aritmética ordinal, propiedades de los números ordinales, algunos teoremas importantes que nos ayudaran a definir operaciones entre ordinales y la forma normal. El segundo capítulo corresponde al cuerpo del trabajo; en este capítulo ya se podrá apreciar el Teorema de Goodstein y su demostración para la cual se hará uso de propiedades de los números ordinales y se introducirá una notación especial que nos ayudará a tener un mejor manejo en el momento de realizar la demostración.

INTRODUCCIÓN

En 1931 el matemático Kurt Gödel presentó el teorema de incompletitud, el cual establece:

En todo sistema axiomático el cual sea lo bastante fuerte para definir el concepto de números naturales, se puede construir una afirmación que ni se puede demostrar ni se puede refutar dentro de ese sistema.

Para demostrar este teorema, Gödel construye un sistema axiomático en el cual todo enunciado se puede expresar en términos de ciertos números, e introduce una proposición del metalenguaje de la forma "esta proposición no se puede demostrar", la cual se demuestra que es indecidible, es decir que no se puede demostrar ni ella ni su negación dentro del sistema.

A algunos matemáticos les parece tan artificial la demostración de Gödel que empiezan a preguntarse si existen proposiciones matemáticas "normales" tales que ni la proposición ni su negación sean demostrables en Aritmética de Peano.[1]

La respuesta a esta pregunta se da en 1977 cuando Jeff Paris (University of Manchester) y Leo Harrington (University of California, Berkeley) publicaron el artículo: *A mathematical incompleteness in Peano Arithmetic*, en el que demostraban que una variación del teorema de Ramsey finito era verdadera pero indemostrable en Aritmética de Peano.

[1]La Aritmética de Peano es la aritmética usual de los números naturales, la cual (como alternativa a la presentación que se esboza en los preliminares) se puede desarrollar axiomáticamente a partir de un sistema de axiomas establecidos por Giuseppe Peano.

Este problema de naturaleza combinatoria fue el primer indecidible que se presentó como una proposición matemática "menos artificial" y despertó el interés de algunos investigadores. Se dió origen entonces a una serie de artículos con nuevos descubrimientos matemáticos cada vez más asequibles (mas "normales") que son también indecidibles en Aritmetica de Peano.

En 1944 el matemático inglés Reuben Louis Goodstein presenta las sucesiones y el teorema que hoy en día se conoce con su nombre, y realiza una demostración usando la teoría de ordinales de Cantor.

Las sucesiones de Goodstein utilizan en su construcción el hecho de que todo entero se puede representar en cualquier base $n \geq 2$. Estas sucesiones tienen la propiedad de que inicialmente crecen muy rápido pero a partir de algún momento decrecen hasta alcanzar el valor 0. Esto último es lo que constituye la esencia del Teorema de Goodstein.

En 1982, en el auge de la búsqueda de proposiciones indecidibles, los matemáticos Laurence Kirby (Baruch College of the City University of New York) y Jeff Paris (University of Manchester) demostraron la indecibilidad del Teorema de Goodstein en la Aritmética de Peano.

El objetivo del presente trabajo es mostrar cómo la tería de conjuntos, concretamente la teoría de números ordinales que surge en la axiomática de Zermelo-Fraenklel, permite demostrar el Teorema de Goodstein el cual es una proposición que se enuncia en el lenguaje de la teoría de números. Para tal propósito presentamos algunos aspectos de la teoría de ordinales, presentamos las sucesiones de Goodstein y el Teorema de Goodstein y finalmente realizamos una demostración del teorema usando propiedades de los números ordinales.

PRELIMINARES

I. Axiomas de Zermelo-Fraenkel

1. **Axioma de Existencia.** Existe un conjunto que no tiene elementos.
2. **Axioma de Extensionalidad.** Si todo elemento de X es un elemento de Y y todo elemento de Y es elemento de X, entonces $X = Y$.
3. **Axioma de Pares.** Para cualquier A y B, existe un conjunto C tal que $x \in C$ si y sólo si $x = A$ o $x = B$.
4. **Axioma de Unión.** Para cualquier S, existe un conjunto U tal que $x \in U$ si y sólo si $x \in A$ para algún $A \in S$. Denotamos $\bigcup S = U$.
5. **Axioma Esquema de Comprensión.** Sea $P(x)$ una propiedad de x. Para cualquier A, existe un B tal que $x \in B$ si y sólo si $x \in A$ y $P(x)$ se cumple.
6. **Axioma de Conjunto Potencia.** Para cualquier S, existe P tal que $X \in P$ si y sólo si $X \subseteq S$. Denotamos $P(S) = P$.
7. **Axioma de Infinito.** Existe un conjunto inductivo.
8. **Axioma Esquema de Reemplazo.** Sea $P(x, y)$ una propiedad tal que para todo x existe un único y para el cual $P(x, y)$ se cumple. Para cualquier A existe B tal que para todo $x \in A$ existe $y \in B$ para el cual $P(x, y)$ se cumple.

El Axioma esquema de reemplazo se presentara con más detalle en este trabajo en el momento que se hace necesario para el desarrollo de la teoría de ordinales.

II. Números Naturales

El número natural 0 es el conjunto vacío ($0 = \emptyset$) representando a los conjuntos que no tienen elementos de los cuales hay sólo uno. Ahora procedemos con los conjuntos que tienen un sólo elemento: $\{\emptyset\}, \{\{\emptyset\}\}, \{\{\emptyset, \{\emptyset\}\}\}$; en general $\{x\}$. Dado que ya tenemos definido el número 0 una escogencia natural para un representante de los conjuntos unitarios sería $\{0\}$. Entonces definimos:

$$1 = \{0\} = \{\emptyset\}$$

Ahora consideremos los conjuntos con dos elementos: $\{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, $\{\{\emptyset\}, \{\{\emptyset\}\}\}$, etc. Como ya definimos 0 y 1 y $0 \neq 1$, tomemos en particular el conjunto cuyos elementos son los definidos anteriormente para definir:

$$2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$$

Continuando el proceso:

$$\begin{aligned}
3 &= \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
4 &= \{0, 1, 2, 3\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} \\
&\vdots \\
n &= \{0, 1, \ldots, n-1\} \\
&\vdots \\
\mathbb{N} &= \{0, 1, 2, 3, \ldots\}
\end{aligned}$$

De lo anterior podemos observar que cada número natural n es el conjunto de los números naturales menores que él, es decir:

$$n = \{m \in \mathbb{N} : m < n\}.$$

Además podemos observar que cuando definimos $1 = \{0\}$ obtenemos 2 adicionándole un segundo elemento a 1, el 1:

$$2 = 1 \cup \{1\} = \{0\} \cup \{1\}$$

Similarmente

$$3 = 2 \cup \{2\} = \{0, 1\} \cup \{2\}$$
$$4 = 3 \cup \{3\} = \{0, 1, 2\} \cup \{3\}$$
$$5 = 4 \cup \{4\} = \{0, 1, 2, 3\} \cup \{4\}\,, etc$$

Así, dado un número natural n, obtenemos el siguiente adicionando un elemento más a n, que sería el mismo n.

Lo anterior se formaliza con las siguientes definiciones:

Definición:

El sucesor de $n \in \mathbb{N}$ es el conjunto $S(n) = n \cup \{n\} = \{0, 1, 2, \ldots n\}$. A $S(n)$ lo denotaremos como $n + 1$.

Definición:

Un conjunto I es inductivo si $0 \in I$ y siempre que $n \in I$ entonces $n + 1 \in I$.

Dado que el axioma de infinito garantiza la existencia de un conjunto inductivo se define el conjunto de los números naturales como:

$$\mathbb{N} = \{x \mid x \in I \text{ para todo conjunto inductivo } I\}\,.$$

A continuación destacaremos algunas características de los números naturales:

Principio de Inducción Matemática:

Sea $P(x)$ una propiedad. Asumamos que:

a. $P(0)$ se cumple.

b. Para todo $n \in \mathbb{N}$, $P(n)$ implica $P(n + 1)$.

Entonces P se cumple para todo número natural n.

Segunda Versión del Principio de Inducción Matemática:

Sea $P(x)$ una propiedad. Asumamos que, para todo $n \in \mathbb{N}$,

$$\text{Si } P(k) \text{ se cumple para todo } k < n, \text{entonces } P(n).$$

Entonces P se cumple para todo número natural n.

Ahora definamos un orden sobre $\mathbb{N}$:

Definición:

Si $n, m \in \mathbb{N}$, entonces decimos que $n < m$ si y sólo si $n \in m$.

El conjunto de los números naturales es bien ordenado bajo la relación definida anteriormente. Es decir, $(\mathbb{N}, <)$ es un conjunto bien ordenado.

Además con el Principio de Inducción Matemática se puede demostrar la propiedad ya enunciada: $n = \{m \in \mathbb{N} : m < n\}$.

Teorema de Recursión:

Para cualquier conjunto A, cualquier $a \in A$ y cualquier función $g : A \times \mathbb{N} \longrightarrow A$, existe una única sucesión infinita $f : \mathbb{N} \longrightarrow A$ tal que:

a. $f_0 = a$.

b. $f_{n+1} = g(f_n, n)$ para todo $n \in \mathbb{N}$.

El Teorema de Recursión permite introducir las operaciones suma, producto y exponenciación, tenemos entonces:

Adición de números naturales:

Existe una única función $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ tal que:

a. $+(m, 0) = m$ para todo m $\in \mathbb{N}$.

b. $+(m, n+1) = +(m, n) + 1$ para todo $m, n \in \mathbb{N}$.

Si escribimos $m + n$ en lugar de $+(m, n)$ entonces obtenemos:

a. $m + 0 = m$.

b. $m + (n + 1) = (m + n) + 1$.

Multiplicación de números naturales:

Existe una única función $\times : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ tal que:

a. $\times (m, 0) = 0$ para todo m $\in \mathbb{N}$.

b. $\times (m, n + 1) = \times (m, n) + m$ para todo $m, n \in \mathbb{N}$.

Si escribimos $m \cdot n$ en lugar de $\times (m, n)$ entonces obtenemos:

a. $m \cdot 0 = 0$.

b. $m \cdot (n + 1) = (m \cdot n) + m$.

Exponenciación de números naturales:

Existe una única función $exp : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ tal que:

a. $exp\ (m, 0) = 1$ para todo m $\in \mathbb{N}$.

b. $exp\ (m, n + 1) = exp\ (m, n) \cdot m$ para todo $m, n \in \mathbb{N}$.

Si escribimos m^n en lugar de $exp\ (m, n)$ entonces obtenemos:

a. $m^0 = 1$.

b. $m^{(n+1)} = m^n \cdot m$.

CAPÍTULO 1

NÚMEROS ORDINALES

1.1. Ordinales

Los números ordinales son básicamente una extensión de los números naturales. Los números naturales empiezan en cero y se obtiene el siguiente aumentando el número previo en una unidad. Es deseable poder continuar el proceso de contar más alla de los números naturales. La idea es que podamos imaginar un número ω que venga "después" de todos todos los números naturales, el cual sería el primer ordinal infinito.

Pero una vez ω es permitido, entonces adicionando uno, podemos obtener $\omega+1$, $\omega+2$, $\omega+3$ y así sucesivamente podemos hablar de $\omega+n$ para cualquier natural n, podemos hablar del límite de $\omega, \omega+1, \omega+2, ...$ el cual sería $\omega+\omega$, que se denota como $\omega \cdot 2$ y así podemos obtener $\omega \cdot 2+1$, $\omega \cdot 2+2$,... y el límite de esta sucesión de ordinales sería: $\omega \cdot 3$. De forma similar, podemos obtener otros ordinales como $\omega \cdot 4$, $\omega \cdot 5$, ...

En esta sección se presentan algunos resultados de la teoría de ordinales con el objetivo de formalizar lo anterior.

Definición 1.1.1 *Un conjunto W es bien ordenado bajo la relación $\prec$ si:*

i. (W,$\prec$) es linealmente ordenado.

ii. Si A$\subseteq$ W, con A$\neq \emptyset$, entonces A tiene elemento mínimo.

Definición 1.1.2

Sea $(L, <)$ un conjunto linealmente ordenado. Un conjunto $S \subseteq L$ se llama un segmento inicial de L, si S es un subconjunto propio de L $(S \neq L)$ y si para todo $a \in S$, todo $x < a$ es también elemento de S.

Observación 1.1 *Notemos que para que podamos hablar de segmento inicial, una de las condiciones es que el conjunto sea linealmente ordenado. Por ejemplo el conjunto de los reales no positivos y el conjunto de los reales negativos son segmentos iniciales del conjunto de los números reales. Ahora, cuando el conjunto nos brinda la condición de ser bien ordenado, tenemos que el segmento inicial tiene una forma especial, veámoslo en el siguiente lema.*

Lema 1.1.1

Si $(W, <)$ es un conjunto bien ordenado y si S es un segmento inicial de $(W, <)$, entonces existe un $a \in W$ tal que $S = \{x \in W \mid x < a\}$

Demostración.

Sea $X = W - S$ el complemento de S. Como S es un subconjunto propio de W, X es no vacío, y entonces tiene elemento mínimo con el buen orden $<$. Sea a el elemento mínimo de X. Si $x < a$, entonces x no puede pertenecer a X, pues a es el elemento mínimo , entonces x pertenece a S. Si $x \geq a$, entonces x no puede pertenecer a S porque en tal caso a pertenecería tambien a S, pues S es segmento inicial. Por lo tanto $S = \{x \in W \mid x < a\}$. ∎

Si a es un elemento de un conjunto bien ordenado $(W, <)$, llamamos al conjunto

$$W[a] = \{x \in W \mid x < a\}$$

el segmento inicial de W dado por a.

Podemos notar que si a es el elemento mínimo de W, el conjunto $W[a]$ es vacío. Además tenemos por el lema 1.1.1 que todo segmento inicial de un conjunto bien ordenado es de la forma $W[a]$ para algún $a \in W$. También $W[a]$ es bien ordenado por $<$.

Consideremos ahora el conjunto $A = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$, observemos que:
$\emptyset \in A$ pero además el conjunto vacío esta contenido en A. También $\{\emptyset\}$ y $\{\{\emptyset\}\}$ son elementos del conjunto A y son subconjuntos de él.

Los conjuntos que cumplen con esta característica son llamados *conjuntos transitivos.*

Definición 1.1.3

Un conjunto T es transitivo si todo elemento de T es un subconjunto de T.

En otras palabras, un conjunto transitivo tiene la propiedad de que si $u \in v \in T$ entonces $u \in T$.

Con las definiciones anteriores tenemos ahora los elementos necesarios para introducir la definición de número ordinal.

Definición 1.1.4 *Un conjunto α es un número ordinal si:*

i. *α es transitivo.*

ii. *α es bien ordenado por $\in_\alpha$.*

Consideremos los conjuntos $B = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$ y $C = \{\emptyset, \{\emptyset, \{\{\emptyset\}\}\}\}$, observemos que el conjunto B es transitivo pero no linealmente ordenado por $\in_B$ y el conjunto C es linealmente ordenado pero no es transitivo. De aquí que, ni el conjunto B ni el conjunto C son ordinales.

Teorema 1.1.1

Todo número natural es un ordinal.

Demostración.

Sea $m \in \mathbb{N}$ y $k \in l \in m$ $(k < l < m)$ entonces $k \in m$. Así que m es transitivo. Además todo número natural es bien ordenado por la relación de $\in$ pues para todo $n \in \mathbb{N}$, n es un subconjunto de $\mathbb{N}$ y $\mathbb{N}$ es bien ordenado por $\in$. ∎

Todo elemento de $\mathbb{N}$ es subconjunto de él ($\mathbb{N}$), así el conjunto $\mathbb{N}$ es transitivo y $\mathbb{N}$ es bien ordenado por $\in$. Por lo tanto $\mathbb{N}$ es también un ordinal. Es importante resaltar que $\mathbb{N}$ es el primer ordinal infinito que tenemos hasta el momento. Como sabemos que $\mathbb{N}$ es un ordinal, como ordinal lo denotaremos por ω. Precisemos esto en la siguiente definición.

Definición 1.1.5 $\omega = \mathbb{N}$.

Cuando se presentan los números naturales se introduce el concepto de sucesor de la forma $S(n) = n \cup \{n\}$ pero esto mismo tiene sentido para cualquier conjunto. Así establecemos la siguiente definición.

Definición 1.1.6

El sucesor de un conjunto x es el conjunto $S(x)= x \cup \{x\}$.

Con esta definición ya podemos conocer otros ordinales diferentes a los números naturales y a $\mathbb{N}$.

Lema 1.1.2

Si α es un número ordinal, entonces $S(\alpha)$ es un número ordinal. A $S(\alpha)$ lo denotamos $\alpha + 1$.

Demostración.

i. Verifiquemos que $S(\alpha)$ es transitivo
$S(\alpha)= \alpha \cup \{\alpha\}$. Sea $a \in S(\alpha)$ entonces $a \in \alpha$ o $a \in \{\alpha\}$

- Si $a \in \alpha$ entonces dado que α es un ordinal, tenemos que $a \subset \alpha \subset S(\alpha)$, por lo tanto $a \subset S(\alpha)$.
- Si $a \in \{\alpha\}$ entonces $a = \alpha \subset S(\alpha)$

Por lo tanto, $S(\alpha)$ es transitivo

ii. Veamos que $S(\alpha)$ es bien ordenado
Como α es bien ordenado por $\in_\alpha$ y $\alpha \in S(\alpha)$ entonces $S(\alpha)$ es bien ordenado por $\in$ siendo α es el elemento máximo. Así que $S(\alpha)$ es un ordinal.

■

Por lo anterior si tenemos un ordinal, tendremos uno más (su sucesor), pero 0 y ω no son ordinales sucesores. Tenemos entonces:

Definición 1.1.7

Un número ordinal α es un ordinal sucesor si existe un ordinal β tal que $\alpha = \beta + 1$. Un ordinal es un ordinal límite si no es sucesor.

Buscaremos ahora extender el ordenamiento de los números naturales. Entonces para ordinales cualquiera α y β definimos:

$$\alpha < \beta \text{ si y sólo si } \alpha \in \beta.$$

La axiomática de Zermelo-Fraenkel considerada para el desarrollo de la teoría de ordinales que aquí presentamos, no excluye la posibilidad de que algún conjunto sea elemento de sí mismo. Esto hace especialmente importante el siguiente Lema. Este Lema junto con los tres siguientes nos permitirán precisar características de $<$ en un teorema. De hecho veremos que $<$ se comporta como un ordenamiento lineal.

Lema 1.1.3

Si α es un ordinal entonces $\alpha \notin \alpha$.

Demostración.

Supongamos que $\alpha \in \alpha$, entonces el conjunto $(\alpha, \in_\alpha)$ linealmente ordenado tiene un elemento $x = \alpha$ tal que $x \in x$ esto contradice la propiedad de asimetría de $\in_\alpha$ y por lo tanto $\alpha \notin \alpha$. ■

Lema 1.1.4

Todo elemento de un número ordinal es un número ordinal.

Demostración.

Sea α un ordinal y $x \in \alpha$, probemos que x es ordinal.

i. Sea u y v tales que $u \in v \in x$. Como $x \in \alpha$ y α es transitivo y además tenemos que $v \in x \in \alpha$ entonces $v \in \alpha$. Así que $u \in v \in \alpha$ y también $u \in \alpha$. De aquí que u, v y x son elementos de α y α es bien ordenado por $\in$, entonces $u \in x$. Es decir, x es transitivo.

ii. Por la transitividad de α tenemos que $x \subseteq \alpha$ y la relación $\in_x$ es la restricción de la relación $\in_\alpha$. Así, x es bien ordenado por $\in_x$.

Por lo tanto, de (i) y (ii) tenemos que x es un ordinal. ■

Lema 1.1.5

Si α y β son ordinales tales que $\alpha \subset \beta$, entonces $\alpha \in \beta$.

Demostración.

Sea $\alpha \subset \beta$ entonces $\beta - \alpha \neq \emptyset$ y $\beta - \alpha \subseteq \beta$, además el conjunto $\beta - \alpha$ tiene elemento mínimo en el orden $\in_\beta$, llamémoslo $\gamma \in \beta$.

Veamos que $\gamma = \alpha$

- Tenemos que $\gamma \subseteq \alpha$, de lo contrario existiría un $\delta \in \gamma - \alpha \subseteq \beta - \alpha$ tal que $\delta < \gamma$, y esto es una contradicción ya que γ es el mínimo de $\beta - \alpha$.
- Probemos que si $\delta \in \alpha$ entonces $\delta \in \gamma$. De lo contrario, si $\delta \notin \gamma$ se tendrá que $\gamma \in \delta$ o $\gamma = \delta$ ya que γ, δ están en β y β es bien ordenado por $\in_\beta$.
  En ambos casos $\gamma \in \alpha$ pues α es transitivo, esto contradice el hecho que $\gamma \in \beta - \alpha$.
  Por lo tanto $\gamma = \alpha \in \beta$.

■

Lema 1.1.6

Sea X un conjunto de ordinales entonces $\bigcup X$ es transitivo.

Demostración.

Sea $\mu \in \gamma \in \bigcup X$. Probemos que $\mu \in \bigcup X$. Si $\gamma \in \bigcup X$ entonces existe un $\beta \in X$ tal que $\gamma \in \beta$. Como β es un ordinal entonces $\gamma \subseteq \beta$. Luego $\mu \in \beta$, lo que implica que $\mu \in \bigcup X$. Así que $\bigcup X$ es transitivo. ■

Teorema 1.1.2 *Sean α, β y γ números ordinales.*

a. *Si $\alpha < \beta$ y $\beta < \gamma$ entonces $\alpha < \gamma$.*

b. *No se tienen simultáneamente $\alpha < \beta$ y $\beta < \alpha$.*

c. *Se da una de las siguientes $\alpha < \beta$ o $\alpha = \beta$ o $\beta < \alpha$.*

d. *Cada conjunto no vacío de números ordinales tiene elemento mínimo. En consecuencia, cada conjunto de números ordinales es bien ordenado por $<$.*

e. *Para cada conjunto de números ordinales X existe un número ordinal $\alpha \notin X$, es decir, no existe un conjunto de todos los números ordinales.*

Demostración.

a. Por hipótesis $\alpha \in \beta$ y $\beta \in \gamma$, es decir $\alpha \in \beta \in \gamma$ y como γ es transitivo entonces $\alpha \in \gamma$. Luego $\alpha < \gamma$.

b. Si tenemos que $\alpha \in \beta$ y $\beta \in \alpha$ obtendríamos que $\alpha \in \alpha$ lo que contradice el lema 1.1.3.

c. Si α y β son ordinales entonces $\alpha \cap \beta$ es un ordinal. Además, $\alpha \cap \beta \subseteq \alpha$ y $\alpha \cap \beta \subseteq \beta$.
Si $\alpha \cap \beta = \alpha$, entonces $\alpha \subseteq \beta$ y esto implica que $\alpha \in \beta$ o $\alpha = \beta$ por lema 1.1.5.
Similarmente, si $\alpha \cap \beta = \beta$ entonces $\beta \in \alpha$ o $\beta = \alpha$.
Ahora, si $\alpha \cap \beta \subset \alpha$ y $\alpha \cap \beta \subset \beta$ entonces $\alpha \cap \beta \in \alpha$ y $\alpha \cap \beta \in \beta$, de aquí que $\alpha \cap \beta \in \alpha \cap \beta$ y esto contradice el lema 1.1.3. Luego sólo existen las posibilidades $\alpha \cap \beta = \alpha$ o $\alpha \cap \beta = \alpha$ y esto implica que $\alpha < \beta$ o $\alpha = \beta$ o $\beta < \alpha$.

d. Sea A un conjunto no vacío de ordinales. Tomemos un $\alpha \in A$, consideremos el conjunto $A \cap \alpha$.
Si $A \cap \alpha = \emptyset$, α es el elemento mínimo de A. Si α no es el elemento mínimo de A entonces existe un $\lambda \in A$ tal que $\lambda < \alpha$ ($\lambda \in \alpha$), así $\lambda \in A \cap \alpha$ y esto es una contradicción con el hecho de que $A \cap \alpha = \emptyset$.
Si $A \cap \alpha \neq \emptyset$, entonces $A \cap \alpha \subseteq \alpha$; como α es bien ordenado por $\in_\alpha$ entonces $A \cap \alpha$ tiene elemento mínimo, llamémoslo β. Así, β es el elemento mínimo de A con el orden $<$. Si β no es el mínimo de A entonces existe $\gamma < \beta$ y $\gamma \in A$ luego $\gamma \in \beta \cap A$ pero $\beta \in \alpha$ asi $\gamma \in \alpha \cap A$. Pero esto contradice que β es el mínimo de $\alpha \cap A$.

e. Sea X un conjunto de números ordinales. Así, como todo elemento de X es un conjunto transitivo, $\bigcup X$ es también un conjunto transitivo por lema 1.1.6. De la parte (d) de este teorema se sigue que $\bigcup X$ es bien ordenado por $\in$. Por lo tanto $\bigcup X$ es un número ordinal. Ahora sea $\alpha = S(\bigcup X)$; α es un número ordinal y $\alpha \notin \bigcup X$, pues si $\alpha \in \bigcup X$ entonces $\alpha \subseteq \bigcup X$ y por lema 1.1.5 tendríamos que $\alpha = \bigcup X$ o $\alpha \in \bigcup X$, en cualquiera de los dos casos, $\alpha \in S(\bigcup X) = \alpha$ y esto contradiría el lema 1.1.3.
Por lo tanto no existe el "conjunto de todos los números ordinales".

■

El número ordinal $\bigcup X$ usado en la prueba del literal (e) se llama el supremo de X y lo denotamos por $supX$. En efecto, $\bigcup X$ es el menor ordinal mayor o igual a todos los elementos de X:

a. Si $\alpha \in X$, entonces $\alpha \subseteq \bigcup X$ de aquí que $\alpha \leq \bigcup X$.

b. Si $\alpha \leq \gamma$ para todo $\alpha \in X$, entonces $\alpha \subseteq \gamma$ para todo $\alpha \in X$ y así $\bigcup X \subseteq \gamma$, de aquí que $\bigcup X \leq \gamma$.

Una consecuencia de los anterior es que, análogamente a como ocurre en los números naturales, si α es un número ordinal entonces: $\alpha = \{\beta \mid \beta < \alpha\}$.

El siguiente teorema enfatiza el hecho de que los ordinales son una generalización de los números naturales.

Teorema 1.1.3

Los números naturales son exactamente los números ordinales finitos.

Demostración.

Por el teorema 1.1.1 tenemos que los números naturales son ordinales y además para cada $n \in \mathbb{N}$, n es finito. Falta entonces mostrar que cada ordinal que no es natural es un conjunto infinito.
Si α es ordinal y α no es un número natural por teorema 1.1.2 parte (b) se dará el caso $\alpha \geq \omega$ (porque $\alpha \not< \omega$), así $\alpha \supseteq \omega$ porque α es transitivo. Luego α tiene un subconjunto infinito y por lo tanto α es infinito.

■

Consideremos ahora los siguientes ejemplos:

1. Para la construcción de la sucesión

$$\langle \emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \cdots \rangle$$

Podríamos definir el esquema recursivo

$$a_0 = \emptyset$$
$$a_{n+1} = \{a_n\}, \text{ para todo } n \in \mathbb{N}$$

La dificultad aquí está en que para aplicar el teorema de recursión necesitamos un conjunto A dado de antemano, tal que $g(n, x) : \mathbb{N} \times A \to A$ definida por $g(n, x) = \{x\}$ pueda ser usada para calcular el término $(n + 1)$ de la sucesión a partir de su n-ésimo término.

Pero no es obvio como probar de nuestros axiomas que exista algún conjunto A tal que:

$$\emptyset \in A, \{\emptyset\} \in A, \{\{\emptyset\}\} \in A, \{\{\{\emptyset\}\}\} \in A, ...$$

Parece como si la definición de A requiriera recursión.

2. La existencia de ω se puede garantizar por el axioma de infinito y por como se define $\mathbb{N}$. Los conjuntos $\omega+1, \omega+2, \omega+3, \ldots$ pueden obtenerse usando el axioma de unión y el axioma de pares. Cuando pensamos en definir $\omega+\omega$ lo "definimos" como la unión de ω y de todos los $\omega+n$ para todo $n \in \omega$, pero la existencia de $\omega+\omega$ no la podemos garantizar con los axiomas que tenemos hasta el momento.

La introducción de un nuevo axioma apunta a resolver la dificultad planteada por los ejemplos anteriores y permitirá demostrar un importante teorema que dará la entrada de nuevos ordinales en la teoría.

Axioma 1.1.1 (Axioma Esquema de Reemplazo)

Sea $P(x,y)$ una propiedad tal que para todo x existe un único y tal que $P(x,y)$ se cumple.
Para todo conjunto A, existe un conjunto B tal que, para todo $x \in A$, existe un $y \in B$ el cual permite que $P(x,y)$ se cumpla.

Ahondemos un poco en el significado del axioma:
Sea F la operación definida por la propiedad P, esto es, $F(x)$ denota el único y para el cual se tiene $P(x,y)$. El Axioma de Reemplazo puede enunciarse de la siguiente manera:

Para todo conjunto A hay un conjunto B tal que para todo $x \in A$, $F(x) \in B$.

Consideremos nuevamente la operación F definida por P. El Axioma de Reemplazo implica entonces que la operación F sobre elementos de un conjunto dado A puede ser "reemplazada" por una función, esto es, por un conjunto de parejas ordenadas. De manera más precisa tenemos:

Para todo conjunto A, existe una función f tal que $dom\ f = A$ y $f(x) = F(x)$ para todo $x \in A$.

De lo anterior, $f = \{(x,y) \in A \times B \mid P\,(x,y)\}$, donde B es el conjunto que nos proporciona el Axioma de Reemplazo. Usaremos la notación $F \restriction A$ para denotar la función f. Podemos notar que $ran\ \ (F \restriction A) = F\,[A]\,.$

Los conjuntos bien ordenados pueden ser representados por números ordinales. De manera precisa tenemos el siguiente teorema:

Teorema 1.1.4

Todo conjunto bien ordenado es isomorfo a un único número ordinal.

Demostración.

Sea $(W, <)$ un conjunto bien ordenado. Sea A el conjunto de todos los $a \in W$ para los cuales $W\,[a]$ es isomorfo a algún ordinal.

Como dos ordinales distintos no pueden ser isomorfos, pues uno es segmento inicial del otro, este ordinal es único, y lo denotamos por α_a.

Sea S tal que $S = \{\alpha_a \mid a \in A\}$; la existencia del conjunto S la garantiza el Axioma Esquema de Reemplazo. El conjunto S es bien ordenado por $\in$, por ser un conjunto de ordinales. Este también es transitivo, porque si $\gamma \in \alpha_a \in S$, sea φ un isomorfismo entre $W\,[a]$ y α_a y sea $c = \varphi^{-1}(\gamma)$, entonces $\varphi \restriction W[c]$ es un isomorfismo entre $W\,[c]$ y γ y así $\gamma \in S$. Por lo tanto S es un número ordinal, $S = \alpha$.

Un argumento similar muestra que $a \in A$, $b < a$ implica que $b \in A$: sea φ un isomorfismo de $W\,[a]$ y α_a. Entonces $\varphi \restriction W\,[b]$ es un isomorfismo de $W\,[b]$ y un segmento inicial I de α_a. Por lema 1.1.1 existe un $\beta < \alpha_a$ tal que $I = \{\gamma \in \alpha_a \mid \gamma < \beta\} = \beta$, esto es $\beta = \alpha_b$. Esto muestra que $b \in A$ y $\alpha_b < \alpha_a$.

Podemos concluir o bien que $A = W$ o $A = W\,[c]$ para algún $c \in W$. (Lema 1.1.1).

Ahora definamos la función $f : A \to S$ por $f(a) = \alpha_a$. Por la definición de S y del hecho que $b < a$ implica que $\alpha_b < \alpha_a$ es obvio que f es un isomorfismo de $(A, <)$ en α. Si $A = W\,[c]$ tendríamos que $c \in A$, una contradicción.

Por lo tanto, $A = \omega$, y f es un isomorfismo de $(W, <)$ y el ordinal α.

■

Haciendo uso del teorema anterior tenemos:

Definición 1.1.8

Si W es un conjunto bien ordenado, entonces el tipo de orden de W es el único número ordinal isomorfo a W.

Como extensión de los números naturales que son los ordinales tendremos también un Principio de Inducción Matemática que en este caso va a ser transfinito.

Teorema 1.1.5 (Principio de Inducción Transfinita.)
Sea $P(x)$ una propiedad. Asumamos que para todo número ordinal α:

$$\textit{Si } P(\beta) \textit{ se tiene para todo } \beta < \alpha, \textit{ entonces } P(\alpha). \tag{1.1}$$

Entonces $P(\alpha)$ se cumple para todo ordinal α.

Demostración.

Supongamos que para algún ordinal γ no se tiene la propiedad P, y sea S el conjunto de todos los ordinales $\beta \leq \gamma$ que no tienen la propiedad P.
El conjunto S tiene elemento mínimo α. Por lo tanto, todo $\delta < \alpha$ tiene la propiedad P, por hipótesis tendríamos que $P(\alpha)$ se cumple, esto es una contradicción.
Así que no existe un ordinal γ para el cual no se cumpla P. ∎

Así como en los números naturales manejamos al menos dos Principios de Inducción, se considera conveniente manejar dos versiones para los ordinales.

Teorema 1.1.6 (Segunda Versión del Principio de Inducción Transfinita)
Sea $P(x)$ una propiedad tal que:

a. *$P(0)$ se cumple.*

b. *$P(\alpha)$ implica $P(\alpha+1)$ para todo ordinal α.*

c. *Para todo ordinal límite $\alpha \neq 0$, si $P(\beta)$ se cumple para todo $\beta < \alpha$ entonces $P(\alpha)$ se cumple.*

Entonces $P(\alpha)$ se cumple para todo ordinal α.

Demostración.

Es suficiente mostrar que los literales $(a), (b)$ y (c) implican la propiedad (1.1). Sea α un ordinal tal que $P(\beta)$ se cumple para todo $\beta < \alpha$. Si $\alpha = 0$, entonces $P(\alpha)$ se tiene por el literal (a). Si α es un ordinal sucesor, es decir que existe $\beta < \alpha$ tal que $\alpha = \beta + 1$, como $P(\beta)$ se tiene por hipótesis inductiva entonces por el literal (b) $P(\alpha)$ se cumple. Si α es un ordinal límite, tenemos que por hipótesis inductiva y el literal (c), se cumple $P(\alpha)$. ∎

También tenemos en los ordinales un Teorema de Recursión. Para comprender el significado y la demostración de este teorema introducimos la definición de cómputo y sucesión transfinita.

Definición 1.1.9

Una sucesión transfinita de longitud α es una función cuyo dominio es un ordinal α.

Un cómputo t de longitud α basado en una operación G es una función con $\operatorname{dom} t = \alpha + 1$ en el cual para todo $\beta \leq \alpha$, $t(\beta) = G(t \restriction \beta)$.Si G tiene un parámetro z tendríamos $t(\beta) = G(z, t \restriction \beta)$

Presentamos ahora una versión del Teorema de Recursión Transfinita en el cual se hace distinción entre ordinales sucesores y ordinales límites y además se tiene en cuenta un posible parámetro. La intención es acercarnos a la utilización del Teorema de Recursión en la definición de las operaciones entre ordinales.

Teorema 1.1.7 (Teorema de Recursión Transfinita. Versión Paramétrica)

Sea G_1, G_2 y G_3 operaciones y sea G una operación definida por $G(z,x) = y$ si y sólo si se da una de las siguientes situaciones:

$$\begin{cases} a.\ x = \emptyset \text{ y } y = G_1(z, \emptyset). \\ b.\ x \text{ es una función, } dom\ x = \alpha + 1 \text{ para un ordinal } \alpha \text{ y } y = G_2(z, x(\alpha)) \\ c.\ x \text{ es una función, } dom\ x = \alpha \text{ para un ordinal límite } \alpha \neq \emptyset \text{ y } y = G_3(z, x) \\ d.\ y = \emptyset \text{ en otro caso.} \end{cases}$$

Entonces la propiedad $P(x,y)$ dada por:

$$\begin{cases} x \text{ es un número ordinal y } y = t(x) \text{ para algún cómputo } t \text{ de longitud } x \text{ basado en G} \\ y = \emptyset \text{ en otro caso.} \end{cases}$$

define una operación F tal que para todo z:

$$F(z,0) = F_z(0) = G_1(z, \emptyset).$$

$$F(z, \alpha+1) = G_2(z, F(z,\alpha)) = G_2(z, F_z(\alpha)) \text{ para todo } \alpha.$$

$$F(z,\alpha) = G_3(z, F_z \restriction \alpha) \text{ para todo límite } \alpha \neq 0.^1$$

Demostración.

Verifiquemos que P define una operación, es decir, que para todo ordinal x existe un único y tal que $P(x,y)$. Demostremos por inducción que para todo ordinal α existe único cómputo de longitud α:
Por hipótesis inductiva asumamos que para todo $\beta < \alpha$ hay un único cómputo de longitud β y comprobemos la existencia y unicidad de un cómputo de longitud α.

i. Existencia.

Aplicando el Axioma de Reemplazo en la propiedad *" y es un cómputo de longitud x"* y el conjunto α. Entonces existe el conjunto:

[1] $F_z \restriction \alpha = \{((z,\gamma), F(z,\gamma)) \mid \gamma < \alpha\}$

$$T = \{t \mid t \text{ es un cómputo de longitud } \beta \text{ para algún } \beta < \alpha\}$$

Por hipótesis inductiva tenemos que para todo $\beta < \alpha$ existe un único cómputo de longitud β es decir un único $t \in T$. T es un sistema de funciones.
Sea $\bar{t} = \bigcup T$. Ahora, sea $\tau = \bar{t} \cup \{(\alpha, G(z, \bar{t}))\}$. Probemos que τ es un cómputo de longitud α:

a. τ es una función y $dom\ \tau = \alpha + 1$

Sabemos que $dom\ \bar{t} = \bigcup_{t \in T} dom\ t = \bigcup_{\beta \in \alpha} (\beta + 1) = \alpha$, así que $dom\ \tau = dom\ \bar{t} \cup \{\alpha\} = \alpha + 1$

Ahora, ya que $\alpha \notin dom\ \bar{t}$, es suficiente mostrar que $\bar{t}$ es una función. Pero esto último se debe al hecho de que T es un sistema compatible de funciones. En efecto, sean t_1 y $t_2 \in T$ arbitrarios, y sean $dom\ t_1 = \beta_1$, $dom\ t_2 = \beta_2$.
Sin pérdida de generalidad asumamos que $\beta_1 < \beta_2$, entonces $\beta_1 \subseteq \beta_2$, y es suficiente mostrar que $t_1(\gamma) = t_2(\gamma)$ para todo $\gamma < \beta_1$. Realicemos esto por inducción transfinita, esto es, asumamos que $\gamma < \beta_1$ y $t_1(\delta) = t_2(\delta)$ para todo $\delta < \gamma$ entonces $t_1 \restriction \gamma = t_2 \restriction \gamma$ y tenemos que $t_1(\gamma) = G(z, t_1 \restriction \gamma) = G(z, t_2 \restriction \gamma) = t_2(\gamma)$. Por lo tanto, $t_1(\gamma) = t_2(\gamma)$ para todo $\gamma < \beta_1$.

b. $\tau(\beta) = G(z, \tau \restriction \beta)$, para todo $\beta \leq \alpha$.

Si $\beta = \alpha$ entonces $\tau(\alpha) = G(z, \bar{t}) = G(z, \tau \restriction \alpha)$. Si $\beta < \alpha$, escojamos un $t \in T$ tal que $\beta \in dom\ t$; tenemos $\tau(\beta) = t(\beta) = G(z, t \restriction \beta) = G(z, \tau \restriction \beta)$ porque t es un cómputo y $t \subseteq \tau$.

ii. Unicidad.

Sea σ otro cómputo de longitud α, veamos que $\tau = \sigma$. Como τ y σ son funciones y $dom\ \tau = \alpha + 1 = dom\ \sigma$ es suficiente comprobar por inducción transfinita que $\tau(\gamma) = \sigma(\gamma)$, para todo $\gamma \leq \alpha$:

Asumamos que $\tau(\delta) = \sigma(\delta)$ para todo $\delta < \gamma$. Entonces $\tau(\gamma) = G(z, \tau \restriction \gamma) = G(z, \sigma \restriction \gamma) = \sigma(\gamma)$.

Esto concluye la demostración de que la propiedad P define una operación F.

Notemos que para cualquier cómputo t, $F_z \restriction dom\ t = t$; esto se tiene porque para cualquier $\beta \in dom\ t$, $t_\beta = t \restriction (\beta + 1)$ es obviamente un cómputo de longitud β, y entonces, por la definición de F, $F_z(\beta) = t_\beta(\beta) = t(\beta)$.

Para mostrar que $F_z(\alpha) = G(z, F \restriction \alpha)$ para todo α y todo z, sea t el único cómputo de longitud α, entonces $F_z(\alpha) = t(\alpha) = G(z, t \restriction \alpha) = G(z, F \restriction \alpha)$.

Luego por como se define G tenemos:

$$F(z,0) = G(z, F \restriction 0) = G(z,\emptyset) = G_1(z,\emptyset).$$

$$F(z,\alpha+1) = G(z, F_z \restriction (\alpha+1)) = G_2(z, F_z(\alpha)) \text{ para todo } \alpha.$$

$$F(z,\alpha) = G(z, F_z \restriction \alpha) = G_3(z, F_z \restriction \alpha) \text{ para todo límite } \alpha \neq 0.$$ ■

Corolario 1.1.1

Sea G una operación. Para todo conjunto A existe una única sucesión infinita $\langle a_n \mid n \in \mathbb{N}\rangle$ tal que:

(a) $a_0 = a$.

(b) $a_{n+1} = G(a_n, n)$ *para todo* $n \in \mathbb{N}$.

Con el Corolario 1.1.1 podemos retomar los ejemplos que se plantearon para introducir el Axioma Esquema de Reemplazo y mostrar la existencia de $\langle \emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \cdots \rangle$ y de $\omega + \omega$. Veamos:
Sea $G(x,y) = \{x\}$ entonces por el Corolario 1.1.1 existe una sucesión infinita $\langle a_n \mid n \in \mathbb{N}\rangle$ tal que: $a_0 = \emptyset$ y $a_{n+1} = G(a_n, n) = \{a_n\}$ para todo $n \in \mathbb{N}$ y si definimos $G(x,y) = x+1$ entonces por el Corolario 1.1.1 existe una sucesión infinita $\langle \xi_n \mid n \in \mathbb{N}\rangle$ tal que: $\xi_0 = \omega$ y $\xi_{n+1} = G(\xi_n, n) = \{\xi_n\}$ para todo $n \in \mathbb{N}$. Así que por lo anterior garantizamos la existencia del conjunto $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \cdots\}$ y de $\omega + \omega$.

1.2. Aritmética Ordinal

Ahora, haciendo uso del Teorema de Recursión Transfinita, definimos la adición, multiplicación y exponenciación de números ordinales. Enfatizamos que en lo que respecta a los números naturales como ordinales que son, estas operaciones son las mismas que mostrabamos en los preliminares.

Definición 1.2.1 (Adición de Números Ordinales.) *Para todo ordinal β*

a. $\beta + 0 = \beta$

b. $\beta + (\alpha+1) = (\beta+\alpha) + 1$ para todo α

c. $\beta + \alpha = \ sup\ \{\beta + \gamma \mid \gamma < \alpha\}$ para todo límite $\alpha \neq 0$

Veamos como la definición 1.2.1 se ajusta a la versión formal del Teorema de Recursión Transfinita.

Consideremos las operaciones G_1, G_2 y G_3 donde:

$G_1(z,x) = z$, $G_2(z,x) = x+1$ y $G_3(z,x) = sup(ran\ x)$ si x es función (y $G_3(z,x) = 0$ en otro caso).

El teorema 1.1.7 proporciona una operación F tal que para todo z:

$$(1.2)\quad \begin{cases} F(z,0) = G_1(z,0) = z \\ F(z,\alpha+1) = G_2(z, F_z(\alpha)) = F(z,\alpha) + 1 \\ F(z,\alpha) = G_3(z, F_z \restriction \alpha) = sup(ran(F_z \restriction \alpha)) = sup(\{F(z,\gamma) \mid \gamma < \alpha)\}), \\ \text{para el ordinal límite } \alpha \neq 0. \end{cases}$$

Si β *y* α son ordinales, entonces escribimos $\beta + \alpha$ en lugar de $F(\beta,\alpha)$ y así observamos que las condiciones de (1.2) son exactamente los literales (a),(b) y (c) de la definición 1.2.1.

Si $\alpha = 0$ en la parte (b) de la definición 1.2.1 tenemos la igualdad $\beta + 1 = \beta + 1$; el lado izquierdo denota la suma de números ordinales β y 1 mientras que el lado derecho es el sucesor de β.

Ejemplo 1.2.1

1. $\beta + 2 = (\beta) + (1+1) = (\beta+1) + 1$ *, para todo ordinal* β*.*
2. $\beta + 3 = (\beta + 2) + 1$*, para todo ordinal* β*.*
3. $0 + \beta = \beta$*. Veamos que esto se verifica utilizando el Principio de Inducción Transfinita.*
   Si $\beta = 0$ *entonces tendríamos* $0 + 0 = 0$ *por definición 1.2.1, ahora si* $0 + \gamma = \gamma$ *Y* $\beta = \gamma + 1$*, entonces* $0 + \beta = 0 + (\gamma + 1) = (0 + \gamma) + 1 = \gamma + 1 = \beta$*, finalmente verifiquemos que* $0 + \beta = \beta$ *cuando* β *es un ordinal límite y* $0 + \gamma = \gamma$ *para* $\gamma < \beta$*:* $0 + \beta = sup\ \{0 + \gamma \mid \gamma < \beta\} = sup\ \{\gamma \mid \gamma < \beta\} = \beta$*.*
4. $\omega + \omega = sup\{\omega + n \mid n < \omega\}$.
5. $(\omega + \omega) + \omega = sup\{(\omega + \omega) + n \mid n < \omega\}$
6. $m + \omega = sup\{m + n \mid n < \omega\} = \omega$

Observación 1.2 *Del ejemplo* (6) *vemos que* $m+\omega$ *no tiene máximo.*

Ahora $\omega+m$ *es mayor que* ω *y además tiene como máximo* $\omega+n$ *donde* m *es el sucesor de* $n \in \omega$. *Así que* $m+\omega \neq \omega+m$. *Por lo tanto, la adición de números ordinales no es conmutativa.*

También podemos notar que, si bien $1 \neq 2$, *tenemos que* $1+\omega = 2+\omega$. *Por lo tanto la cancelación a derecha en igualdades o desigualdades no se tiene.*

Como existe la posibilidad de sumar conjuntos bien ordenados es importante mostrar que la suma de ordinales definida en 1.2.1 es compatible con la suma de conjuntos bien ordenados. Tenemos entonces el siguiente teorema:

Teorema 1.2.1

Sea $(W_1, <_1)$ *y* $(W_2, <_2)$ *conjuntos bien ordenados, isomorfos a los ordinales* α_1 *y* α_2 *respectivamente, y sea* $(W, <)$ *la suma de* $(W_1, <_1)$ *y* $(W_2, <_2)$. *Entonces,* $(W, <)$ *es isomorfo al ordinal* $\alpha_1 + \alpha_2$.

Demostración.

Asumamos que W_1 y W_2 son disjuntos, que $W = W_1 \cup W_2$ y que cada elemento en W_1 precede en $<$ a cada elemento en W_2, mientras que $<$ coincide con $<_1$ y $<_2$ en W_1 y W_2 respectivamente. Demostremos el teorema por inducción sobre α_2:

Si $\alpha_2 = 0$ entonces $W_2 = \emptyset$, asi $W = W_1$ y $\alpha_1 + \alpha_2 = \alpha_1$.

Si $\alpha_2 = \beta + 1$ entonces W_2 tiene elemento máximo a, y $W\,[a]$ es isomorfo a $\alpha_1 + \beta$; el isomorfismo se puede extender a un isomorfismo entre W y $\alpha_1 + \alpha_2 = (\alpha_1 + \beta) + 1$.

Si α_2 es un ordinal límite, para cada $\beta < \alpha_2$ existe un isomorfismo f_β de $\alpha_1 + \beta$ sobre $W\,[a_\beta]$ donde $a_\beta \in W_2$; más áun, f_β es único, a_β es el $\beta-$ésimo elemento de W_2, y si $\beta < \gamma$ entonces $f_\beta \subset f_\gamma$. Sea $f = \bigcup_{\beta<\alpha_2} f_\beta$. Como $\alpha_1 + \alpha_2 = \bigcup_{\beta<\alpha_2} (\alpha_1 + \beta)$, de aquí se sigue que f es un isomorfismo de $\alpha_1 + \alpha_2$ sobre W. ∎

Si bien en la suma de ordinales no tenemos la conmutatividad ni la cancelación a la derecha si tenemos la cancelación a izquierda tanto en igualdades como en desigualdades y la asociatividad.

Lema 1.2.1

a. *Si* α_1, α_2 *y* β *son ordinales, entonces* $\alpha_1 < \alpha_2$ *si y sólo si* $\beta + \alpha_1 < \beta + \alpha_2$.

b. *Para todo ordinal* α_1, α_2 *y* β, $\beta + \alpha_1 = \beta + \alpha_2$ *si y sólo si* $\alpha_1 = \alpha_2$.

c. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ para todo ordinal α, β y γ.

d. Sea α, β y γ ordinales y sea $\alpha < \beta$ entonces $\alpha + \gamma \leq \beta + \gamma$.

Demostración.

a. Haciendo inducción transfinita sobre α_2 mostremos que $\alpha_1 < \alpha_2$ implica que $\beta+\alpha_1 < \beta+\alpha_2$. Supongamos que $\alpha_1 < \alpha_2$ y que $\alpha_1 < \delta$ implica que $\beta+\alpha_1 < \beta+\delta$ para todo $\delta < \alpha_2$.
Si α_2 es un ordinal sucesor entonces $\alpha_2 = \delta + 1$ donde $\delta \geq \alpha_1$. En el caso que $\delta = \alpha_1$ entonces $\beta + \alpha_1 \leq \beta + \delta < (\beta + \delta) + 1 = \beta + (\delta + 1) = \beta + \alpha_2$ y si $\alpha_1 < \delta$, $\beta + \alpha_1 < \beta + \delta < (\beta + \delta) + 1 = \beta + (\delta + 1) = \beta + \alpha_2$.
Si α_2 es un ordinal límite entonces $\alpha_1 < \alpha_2$ y así tenemos que $\beta+\alpha_1 < (\beta + \alpha_1)+1$ $= \beta + (\alpha_1 + 1) \leq sup\{\beta + \delta \mid \delta < \alpha_2\} = \beta + \alpha_2$.

Para demostrar la otra implicación asumamos que $\beta + \alpha_1 < \beta + \alpha_2$.
Si $\alpha_2 < \alpha_1$, por la anterior implicación tendríamos que $\beta + \alpha_2 < \beta + \alpha_1$, y esto contradice la hipótesis. Si $\alpha_2 = \alpha_1$, entonces $\beta + \alpha_2 = \beta + \alpha_1$, lo que nos lleva una contradicción. Luego, por la linealidad de $<$ tenemos que $\alpha_1 < \alpha_2$.

b. Si $\alpha_1 \neq \alpha_2$, entonces se tiene $\alpha_1 < \alpha_2$ o $\alpha_1 > \alpha_2$ y por el literal (a) tendríamos que $\beta + \alpha_1 < \beta + \alpha_2$ o $\beta + \alpha_2 < \beta + \alpha_1$ pero esto contradice la hipótesis. Luego $\alpha_1 = \alpha_2$. Si $\alpha_1 = \alpha_2$ entonces $\beta + \alpha_1 = \beta + \alpha_2$ se tiene trivialmente.

c. Hagamos inducción transfinita sobre γ.
Si $\gamma = 0$, entonces $(\alpha + \beta) + 0 = \alpha + \beta = \alpha + (\beta + 0)$
Asumamos que la igualdad se tiene para γ y probemola para $\gamma + 1$
$(\alpha + \beta) + (\gamma + 1) = [(\alpha + \beta) + \gamma] + 1 = [\alpha + (\beta + \gamma)] + 1 = \alpha + [(\beta + \gamma) + 1] =$ $\alpha + [\beta + (\gamma + 1)]$.

Ahora, sea γ un ordinal límite, $\gamma \neq 0$.Entonces:

$$(\alpha + \beta) + \gamma = \{(\alpha + \beta) + \delta \mid \delta < \gamma\} = sup\ \{\alpha + (\beta + \delta)\ \mid \delta < \gamma\}.$$

Observemos que:

$$sup\ \{\beta + \delta \mid \delta < \gamma\} = \beta + \gamma.$$

y además $\beta + \gamma$ es límite, en efecto, si $\xi < \beta + \gamma$ entonces $\xi \leq \beta + \delta$ para algún $\delta < \gamma$ y entonces $\xi + 1 \leq (\beta + \gamma) + 1 = \beta + (\delta + 1) < \beta + \gamma$.

Notemos:

$(\alpha + \beta)+\gamma = sup\ \{\alpha + (\beta + \delta)\ \mid \delta < \gamma\} = sup\{\alpha + \xi \mid \xi < \beta + \gamma\} = \alpha+(\beta + \gamma)$.

Así que, $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

■

El siguiente lema nos muestra que es posible definir la sustracción de números ordinales.

Lema 1.2.2

Si $\alpha \leq \beta$ entonces existe un único número ordinal ξ tal que $\alpha + \xi = \beta$.

Demostración.

Como α es segmento inicial del conjunto bien ordenado β *o* $\alpha = \beta$, el teorema 2.2.2 implica que $\beta = \alpha + \xi$ donde ξ es el tipo de orden del conjunto $\beta - \alpha = \{\nu \mid \alpha \leq \nu < \beta\}$. El lema 1.2.1 parte (b) nos garantiza que el ordinal ξ es único. ■

Definición 1.2.2 (Multiplicación de Números Ordinales.)

Para todo ordinal β,

a. $\beta \cdot 0 = 0$.

b. $\beta \cdot (\alpha + 1) = \beta \cdot \alpha + \beta$ para todo α.

c. $\beta \cdot \alpha = \ sup\ \{\beta \cdot \gamma \mid \gamma < \alpha\}$ para todo límite $\alpha \neq 0$.

Consideremos las operaciones G_1, G_2 y G_3 donde:

$G_1(z, x) = x$, $G_2(z, x) = x + z$ y $G_3(z, x) = sup(ranx)$ si x es función (y $G_3(z, x) = 0$ en otro caso).

El teorema 1.1.7 proporciona una operación F tal que para todo z:

$$(1.3) \quad \begin{cases} F(z, 0) = G_1(z, 0) = 0 \\ F(z, \alpha + 1) = G_2(z, F_z(\alpha)) = F(z, \alpha) + z \\ F(z, \alpha) = G_3(z, F_z \restriction \alpha) = sup(ran(F_z \restriction \alpha)) = sup(\{F(z, \gamma \mid \gamma < \alpha)\}), \\ \text{para el ordinal límite } \alpha \neq 0. \end{cases}$$

Si β *y* α son ordinales, entonces escribimos $\beta \cdot \alpha$ en lugar de $F(\beta, \alpha)$ y así observamos que las condiciones de (1.3) son exactamente los literales (a),(b) y (c) de la definición 1.2.2.

Ejemplo 1.2.2

1. $\beta \cdot 1 = \beta \cdot (0+1) = \beta \cdot 0 + \beta = 0 + \beta = \beta$.
2. $\beta \cdot 2 = \beta \cdot (1+1) = \beta \cdot 1 + \beta = \beta + \beta$. *En particular,* $\omega \cdot 2 = \omega + \omega$.
3. $\beta \cdot 3 = \beta \cdot (2+1) = \beta \cdot 2 + \beta = \beta + \beta + \beta$.
4. $\beta \cdot \omega = sup\{\beta \cdot n \mid n \in \omega\} = \{\beta, \beta+\beta, \beta+\beta+\beta, \ldots\}$.
5. $1 \cdot \alpha = \alpha$, *para todo* α. *Demostremos esto por inducción.*
   Si $\alpha = 0$ *entonces* $1 \cdot 0 = 0$; *si* $1 \cdot \gamma = \gamma$ *y* $\alpha = \gamma + 1$ *entonces* $1 \cdot (\gamma+1) = 1 \cdot \gamma + 1 = \gamma + 1$ *y si para* $\gamma < \alpha$ *se tiene* $1 \cdot \gamma = \gamma$ *y* α *ordinal límite tenemos:* $1 \cdot \alpha = sup\ \{1 \cdot \gamma \mid \gamma < \alpha\} = sup\ \{\gamma \mid \gamma < \alpha\} = \alpha$.
6. $2 \cdot \omega = sup\{2 \cdot n \mid n \in \omega\} = \omega$.

Observación 1.3 *De los ejemplos* (2) *y* (6) *podemos concluir que en general la multiplicación de ordinales no es conmutativa.*

Como también es posible multiplicar conjuntos bien ordenados tenemos en el siguiente teorema la compatibilidad entre este producto y el producto de números ordinales.

Teorema 1.2.2 *Sea* α *y* β *números ordinales. Los órdenes lexicográfico*[2] *y antilexicográfico* [3] *son buenos órdenes. El tipo de orden del orden antilexicográfico de* $\alpha \times \beta$ *es* $\alpha \cdot \beta$, *mientras que el orden lexicográfico de* $\alpha \times \beta$ *tiene el tipo de orden* $\beta \cdot \alpha$

Proposición 1.2.1 (Propiedades del producto de ordinales)

1. *Si* α_1, α_2 *y* β *son ordinales y* $\beta \neq 0$ *entonces* $\alpha_1 < \alpha_2$ *si y sólo si* $\beta \cdot \alpha_1 < \beta \cdot \alpha_2$.
2. *Si* α_1, α_2 *y* $\beta \neq 0$, $\beta \cdot \alpha_1 = \beta \cdot \alpha_2$ *si y sólo si* $\alpha_1 = \alpha_2$.
3. $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$, *para todo ordinal* α, β *y* γ.
4. $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$, *para todo ordinal* α, β *y* γ.
5. *Sea* α, β *y* γ *ordinales y sea* $\alpha < \beta$ *entonces* $\alpha \cdot \gamma \leq \beta \cdot \gamma$, *para todo ordinal* α, β *y* γ.

[2] *Sean* $(A_1, <_1)$ *y* $(A_2, <_2)$ *conjuntos linealmente ordenados definimos el orden lexicográfico* $<$ *sobre* $A_1 \times A_2$ *así:* $(a_1, a_2) < (b_1, b_2)$ *si y sólo si* $a_1 <_1 b_1$ *o* $(a_1 = b_1$ *y* $a_2 <_2 b_2)$.

[3] *Sean* $(A_1, <_1)$ *y* $(A_2, <_2)$ *conjuntos linealmente ordenados definimos el orden antilexicográfico* $\prec$ *sobre* $A_1 \times A_2$ *así:* $(a_1, a_2) \prec (b_1, b_2)$ *si y sólo si* $a_2 <_2 b_2$ *o* $(a_2 = b_2$ *y* $a_1 <_1 b_1)$.

Definición 1.2.3 (Exponenciación de Números Ordinales.)

Para todo ordinal β,

a. $\beta^0 = 1$.

b. $\beta^{\alpha+1} = \beta^\alpha \cdot \beta$ *para todo* α.

c. $\beta^\alpha = \ sup\ \{\beta^\gamma \mid \gamma < \alpha\}$ *para todo límite* $\alpha \neq 0$

Veamos como la definición 1.2.3 se ajusta a la versión formal del Teorema de Recursión Transfinita.

Consideremos las operaciones G_1, G_2 y G_3 donde:

$G_1(z,x) = 1$, $G_2(z,x) = x \cdot z$ y $G_3(z,x) = sup(ran\ x)$ si x es función (y $G_3(z,x) = 0$ en otro caso).

El teorema 1.1.7 proporciona una operación F tal que para todo z:

$$(1.4)\quad \begin{cases} F(z,0) = G_1(z,0) = 1 \\ F(z,\alpha+1) = G_2(z, F_z(\alpha)) = F(z,\alpha) \cdot z \\ F(z,\alpha) = G_3(z, F_z \restriction \alpha) = sup(ran(F_z \restriction \alpha)) = sup(\{F(z,\gamma) \mid \gamma < \alpha)\}), \\ \text{para el ordinal límite } \alpha \neq 0. \end{cases}$$

Si β *y* α son ordinales, entonces escribimos β^α en lugar de $F(\beta,\alpha)$ y así observamos que las condiciones de (1.4) son exactamente los literales (a),(b) y (c) de la definición 1.2.2.

Ejemplo 1.2.3

1. $\beta^1 = \beta$.

2. $\beta^2 = \beta \cdot \beta$.

3. $\beta^3 = \beta^2 \cdot \beta = \beta \cdot \beta \cdot \beta$.

4. $\beta^\omega = \ sup\ \{\beta^n \mid n \in \omega\}$

5. *El ordinal ϵ definido como $\epsilon = \sup\left\{\omega, \omega^{\omega}, \omega^{\omega^{\omega}}, \omega^{\omega^{\omega^{\omega}}}, \ldots\right\}$ tiene la propiedad $\omega^{\epsilon} = \epsilon$. Veamos:*
   Por el Corolario 1.1.1 tenemos si $\xi_0 = 1$, $\xi_{n+1} = \omega^{\xi_n}$ y si $\xi = \sup\{\xi_n \mid n \in \omega\}$, entonces $\xi_0 = 1, \xi_1 = \omega, \xi_2 = \omega^{\omega}, \xi_3 = \omega^{\omega^{\omega}}, \ldots, \xi_n = \omega^{\omega^{\omega}}$.
   Luego, $\xi = \sup\left\{1, \omega, \omega^{\omega}, \omega^{\omega^{\omega}}, \ldots\right\}$, por lo tanto

$$\omega^{\xi} = \sup\left\{\omega, \omega^{\omega}, \omega^{\omega^{\omega}}, \omega^{\omega^{\omega^{\omega}}}, \ldots\right\} = \epsilon.$$

Proposición 1.2.2 (Propiedades de la exponenciación de ordinales)
Para todo ordinal α, β y γ tenemos:

1. *Si $\alpha \leq \beta$ entonces $\alpha^{\gamma} \leq \beta^{\gamma}$.*
2. *Si $\alpha > 1$ y si $\beta < \gamma$ entonces $\alpha^{\beta} < \alpha^{\gamma}$.*
3. $\alpha^{\beta+\gamma} = \alpha^{\beta} \cdot \alpha^{\gamma}$.
4. $\left(\alpha^{\beta}\right)^{\gamma} = \alpha^{\beta \cdot \gamma \cdot}$

1.3. La Forma Normal

Usando exponenciación, podemos representar los números ordinales en una forma similar a la expansión decimal de enteros.

Anotemos que las funciones ordinales : $\alpha + \beta$, $\alpha \cdot \beta$ y α^{β} tienen un comportamiento continuo en la segunda variable, esto es si β es un ordinal límite entonces $\alpha + \beta$, $\alpha \cdot \beta$ y α^{β} son límites.

Lema 1.3.1

a. *Si $0 < \alpha \leq \gamma$ entonces existe un ordinal máximo β tal que $\alpha \cdot \beta \leq \gamma$.*

b. *Si $1 < \alpha \leq \gamma$ entonces existe un ordinal máximo β tal que $\alpha^{\beta} \leq \gamma$.*

Demostración.

a. Como $\alpha \cdot (\gamma + 1) \geq \gamma + 1 > \gamma$ entonces existe un δ tal que $\alpha \cdot \delta > \gamma$. El menor ordinal δ tal que $\alpha \cdot \delta > \gamma$ debe ser un ordinal sucesor, ya que si δ es límite, $\alpha \cdot \delta$

es límite y existiría un $\alpha \cdot \delta_\upsilon$ tal que $\gamma < \alpha \cdot \delta_\upsilon < \alpha \cdot \delta$ y esto contradice el hecho de que $\alpha \cdot \delta = \sup_{\upsilon<\gamma} (\alpha \cdot \delta_\upsilon)$. Así que $\delta = \beta + 1$. Entonces β es el mayor ordinal tal que $\alpha \cdot \beta \leq \gamma$.

b. Como $\alpha^{\gamma+1} \geq \gamma + 1 > \gamma$, entonces existe un δ tal que $\alpha^\delta > \gamma$. El menor ordinal δ tal que $\alpha^\delta > \gamma$ debe ser un ordinal sucesor, ya que si δ es un ordinal límite, α^δ es límite y así existiría un α^{δ_υ} tal que $\gamma < \alpha^{\delta_\upsilon} < \alpha^\delta$ pero esto contradice el hecho de que α^δ es el supremo. Luego, $\delta = \beta + 1$. Así, β es el máximo ordinal tal que $\alpha^\beta \leq \gamma$.

■

El siguiente lema es análogo al algoritmo de división para enteros.

Lema 1.3.2

Si γ es un ordinal arbitrario y si $\alpha \neq 0$, entonces existe un único ordinal β y un único $\rho < \alpha$ tal que $\gamma = \alpha \cdot \beta + \rho$.

Demostración.

Sea β el mayor ordinal tal que $\alpha \cdot \beta \leq \gamma$ (*si* $\alpha > \gamma$ *entonces* $\beta = 0$) y sea ρ el único ordinal (Lema 2.1.2) tal que $\alpha \cdot \beta + \rho = \gamma$. El ordinal ρ es menor que α, ya que si $\rho \geq \alpha$ tendríamos

$$\alpha + (\beta + 1) = \alpha\beta + \alpha \leq \alpha\beta + \rho = \gamma$$

y esto contradice el hecho que β es el mayor ordinal tal que $\alpha\beta \leq \gamma$.

Comprobemos la unicidad. Sea $\gamma = \alpha \cdot \beta_1 + \rho_1 = \alpha \cdot \beta_2 + \rho_2$ con $\rho_1, \rho_2 < \alpha$.
Asumamos que $\beta_1 < \beta_2$, entonces $\beta_1 + 1 \leq \beta_2$ y tenemos $\alpha \cdot \beta_1 + (\alpha + \rho_2) = \alpha\,(\beta_1 + 1) + \rho_2 \leq \alpha \cdot \beta_2 + \rho_2 = \alpha \cdot \beta_1 + \rho_1$ y por lema 1.2.1 (a) $\rho_1 \geq \alpha + \rho_2 \geq \alpha$, esto es una contradicción pues $\rho_1 < \alpha$. Análogamente, si $\beta_2 < \beta_1$ entonces $\beta_2 + 1 \leq \beta_1$ y así tenemos $\alpha \cdot \beta_2 + (\alpha \cdot \rho_1) = \alpha\,(\beta_2 + 1) + \rho_1 \leq \alpha \cdot \beta_1 + \rho_1 = \alpha \cdot \beta_2 + \rho_2$ y por lema 1.2.1 (a) $\rho_2 \geq \alpha + \rho_1 > \alpha$, y esto es una contradicción ya que $\rho_2 < \alpha$. Por lo tanto, $\beta_1 = \beta_2$.

Ahora, veamos que $\rho_1 = \rho_2$.
Supongamos que $\rho_1 < \rho_2$. Como $\beta_1 = \beta_2$ entonces $\alpha \cdot \beta_1 = \alpha \cdot \beta_2$, y como $\rho_1 < \rho_2$ entonces $\alpha \cdot \beta_1 + \rho_1 < \alpha \cdot \beta_2 + \rho_2$ y esto es una contradicción pues $\alpha \cdot \beta_1 + \rho_1 = \alpha \cdot \beta_2 + \rho_2$.
También obtenemos contradicción si suponemos que $\rho_1 > \rho_2$. Por lo tanto, $\rho_1 = \rho_2$. ■

Lema 1.3.3

Si $\beta < \gamma$ entonces $\omega^\beta \cdot k < \omega^\gamma$, para todo k finito.

Demostración.

$\omega^\beta \cdot k < \omega^\beta \cdot \omega = \omega^{\beta+1} \leq \omega^\gamma$ *entonces* $\omega^\beta \cdot k < \omega^\gamma$. ∎

Del lema anterior tenemos que si $\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \cdots + \omega^{\beta_n}$ con $\beta_1 > \beta_2 > \cdots > \beta_n$ y los k_i con $i = 1, \ldots n$ finitos positivos y $\gamma > \beta_1$ tendremos que $\alpha < \omega^\gamma$. En efecto, $\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \cdots + \omega^{\beta_n} \cdot k_n \leq \omega^{\beta_1} (k_1 + \cdots k_n) < \omega^\gamma$.

La forma normal para ordinales es el análogo a la expansión decimal para enteros, considerando como base el ordinal ω.

Teorema 1.3.1

Todo ordinal $\alpha > 0$ puede ser expresado de manera única como

$$\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \cdots + \omega^{\beta_n} \cdot k_n,$$

donde $k_1 > 0, k_2 > 0, \ldots, k_n > 0$ son finitos y $\beta_1 > \beta_2 > \cdots > \beta_n$.

Demostración.

Garanticemos la existencia de la forma normal por inducción sobre α.
Si $\alpha = 1$, entonces 1 se puede expresar como $1 = \omega^0 \cdot 1$.
Ahora sea $\alpha > 0$ arbitrario. Supongamos que lo afirmado es cierto siempre que el ordinal a representar sea menor que α. Por el lema 1.3.1 (b) existe un máximo β tal que $\omega^\beta \leq \alpha$ (si $\alpha < \omega$ *entonces* $\beta = 0$). Por el lema 1.3.2 existen δ y ρ únicos tales que $\rho < \omega^\beta$ y $\alpha = \omega^\beta \cdot \delta + \rho$. Como $\omega^\beta \leq \alpha$, tenemos que $\delta > 0$ y $\rho < \alpha$.
Si δ fuese infinito, entonces $\alpha \geq \omega^\beta \cdot \delta \geq \omega^\beta \cdot \omega = \omega^{\beta+1}$, y esto contradice la maximalidad de β. Luego δ es finito.

Hacemos entonces $\beta_1 = \beta$ y $\delta = k_1$. Si $\rho = 0$ entonces $\alpha = \omega^{\beta_1} \cdot k_1$ está en la forma normal. En otro caso $0 < \rho < \alpha$ y por la hipótesis de inducción

$$\rho = \omega^{\beta_2} \cdot k_2 + \cdots + \omega^{\beta_n} \cdot k_n, \text{ para algunos } \quad k_2, \ldots, k_n \text{ finitos } y\ \beta_2 > \cdots > \beta_n.$$

Como $\rho < \omega^{\beta_1}$, tenemos $\omega^{\beta_2} \leq \rho < \omega^{\beta_1}$ en consecuencia $\beta_1 > \beta_2$. De aquí que $\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \cdots + \omega^{\beta_n} \cdot k_n$ está expresado en forma normal.

Comprobemos la unicidad. Mediante inducción sobre α.
Para $\alpha = 1$, la expresión $1 = \omega^0$ es claramente única. Supongamos válida la unicidad para todo ordinal positivo menor que α y consideremos

$$\alpha = \omega^{\beta_1} \cdot k_1 + \cdots + \omega^{\beta_n} \cdot k_n = \omega^{\gamma_1} \cdot l_1 + \cdots + \omega^{\gamma_m} \cdot l_m$$

Si $\beta_1 \neq \gamma_1$ por el lema 1.3.3 conduciría a una contradicción. Luego $\beta_1 = \gamma_1$.

Llamemos $\delta = \omega^{\beta_1} = \omega^{\gamma_1}$, $\rho = \omega^{\beta_2} \cdot k_2 + \cdots + \omega^{\beta_n} \cdot k_n$ y $\sigma = \omega^{\gamma_2} \cdot l_2 + \cdots + \omega^{\gamma_m} \cdot l_m$, entonces tenemos $\alpha = \delta \cdot k_1 + \rho = \delta \cdot k_1 + \sigma$ y como $\rho < \delta$ y $\sigma < \delta$, por lema 1.3.2 se tiene que $k_1 = l_1$, $\rho = \sigma$.
Por hipótesis de inducción, la unicidad de la forma normal es válida para ρ. Luego, $m = n$, $\beta_2 = \gamma_2, \ldots, \beta_n = \gamma_n$, $k_2 = l_2, \ldots, k_n = l_n$. Por lo tanto, la forma normal es única. ■

CAPÍTULO 2

TEOREMA DE GOODSTEIN

2.1. Sucesiones de Goodstein

En este capítulo desarrollaremos el objetivo principal del trabajo presentando el Teorema de Goodstein y su demostración. Iniciamos con la introducción de una notación que nos permitirá un manejo cómodo de los enunciados relacionados con las sucesiones de Goodstein.

Definición 2.1.1

Dados dos números naturales $m > 0$ y $n \geq 2$, denotaremos por $\boldsymbol{m_{(n}}$ la expresión del número m en base n, es decir,

$$m_{(n} = \sum_{1 \leq i \leq k} a_i \cdot n^{e_1} = a_1 \cdot n^{e_1} + \cdots + a_k \cdot n^{e_k},$$

donde $k > 0$, $e_1, \cdots, e_k \geq 0$, $n > a_1, \cdots, a_{k-1} > 0$.

Ejemplo 2.1.1

1. $15_{(2} = 2^3 + 2^2 + 2^1 + 1$.
2. $21_{(2} = 2^4 + 2^2 + 1$.
3. $328_{(3} = 3^5 + 3^4 + 3^1 + 1$.

4. $279_{(4} = 4^4 + 4^2 + 4^1 + 3$.

5. $17200_{(7} = 7^5 + 7^3 + 7^2 + 1$.

Definición 2.1.2

Dados dos números naturales $m > 0$ y $n \geq 2$, la expresión del número m en ***base pura*** *n se define como sigue:*

Consideremos la expresión de m en base n:

$$m_{(n} = \sum_{1 \leq i \leq k} a_i \cdot n^{e_1} = a_1 \cdot n^{e_1} + \cdots + a_k \cdot n^{e_k},$$

con las condiciones de la definición 2.1.1. Entonces la expresión de m en base pura es:

$$\begin{cases} m_{[n} = m & \text{si } m \leq n \\ m_{[n} = \sum_{1 \leq i \leq k} a_i \cdot n^{e_{i_{[n}} & \text{en otro caso} \end{cases}$$

Es decir, expresamos el número m en base n, cuidando después de expresar a su vez los exponentes, los exponentes de los exponentes , etc, también en base n, hasta que no haya en los exponentes números mayores que n.

Ejemplo 2.1.2

1. $21_{[2} = 2^{4_{[2}} + 2^{2_{[2}} + 1 = 2^{2^2} + 2^2 + 1$.

2. $261_{[2} = 2^{8_{[2}} + 2^{2_{[2}} + 1 = 2^{2^{3_{[2}}} + 2^2 + 1 = 2^{2^{2+1}} + 2^2 + 1$.

3. $19847_{[3} = 3^{9_{[3}} + 2 \cdot 3^{4_{[3}} + 2 = 3^{3^2} + 2 \cdot 3^{3+1} + 2$.

4. $4294967559_{[4} = 4^{16_{[4}} + 4^{4_{[4}} + 4^{4_{[4}} + 3 = 4^{4^2} + 4^4 + 4^4 + 3$

A la representación de un número natural en base pura se le conoce como *la forma normal de Cantor.*

Definición 2.1.3

Sea $m > 0$, $n \geq 2$ y $x \geq n$ o $x = \omega$. Definimos el resultado de sustituir en la expresión de m en base n (o en base pura n) la base n por x, operaciones que denotamos por $m^x_{(n}$ y $m^x_{[n}$ respectivamente, del siguiente modo:

Calculamos el mayor exponente e de n tal que n^e no supera a m

$$e = máx\left\{k : n^k \leq m\right\}$$

y, una vez calculado e, calculamos el mayor coeficiente a tal que $a \cdot n^e$ no supere a m:

$$a = máx\left\{k : k \cdot n^e \leq m\right\}$$

Una vez tenemos e y a definimos

$$m^x_{(n} = \begin{cases} m & si\ m \leq n \\ a \cdot x^e + (m - a \cdot n^e)^x_{(n} & en\ otro\ caso \end{cases}$$

$$m^x_{[n} = \begin{cases} m & si\ m \leq n \\ a \cdot x^{e^x_{[n}} + (m - a \cdot n^e)^x_{[n} & en\ otro\ caso \end{cases}$$

Nota 2.1 *Las expresiones $m^x_{(n}$ (y $m^x_{[n}$) las leemos m cambiado de la base n (base pura n) a la base x.*

Ejemplo 2.1.3

1. *Hallemos* $21^3_{(2}$.

   $21 = 2^4 + 2^2 + 1$.
   $e = máx\left\{k : n^k \leq m\right\} = 4$, $e = 4$.
   $a = máx\left\{k : k \cdot n^e \leq m\right\} = 1$, $a = 1$.
   Luego, $21^3_{(2} = 1 \cdot 3^4 + (21 - 1 \cdot 2^4)^3_{(2} = 3^4 + 5^3_{(2} = 3^4 + 3^2 + 1^3_{(2} = 3^4 + 3^2 + 1$.
   Así, $21^3_{(2} = 3^4 + 3^2 + 1$.

2. *Hallemos* $40^4_{(3}$.

   $40 = 3^3 + 3^2 + 3 + 1$.
   $e = máx\left\{k : n^k \leq m\right\} = 3$, $e = 3$.
   $a = máx\left\{k : k \cdot n^e \leq m\right\} = 1$, $a = 1$.
   Luego, $40^4_{(3} = 1 \cdot 4^3 + (40 - 1 \cdot 3^3)^4_{(3} = 4^3 + 13^4_{(3} = 4^3 + 4^2 + 4 + 1$.
   Así, $40^4_{(3} = 4^3 + 4^2 + 4 + 1$.

3. *Hallemos* $25^\omega_{(2}$.

   $25 = 2^4 + 2^3 + 1$.
   $e = máx\left\{k : n^k \leq m\right\} = 4$, $e = 4$.
   $a = máx\left\{k : k \cdot n^e \leq m\right\} = 1$, $a = 1$.
   Luego, $25^\omega_{(2} = \omega^4 + (25 - 2^4)^\omega_2 = \omega^4 + (9)^\omega_2 = \omega^4 + \omega^3 + 1$.
   Por lo tanto, $25^\omega_{(2} = \omega^4 + \omega^3 + 1$.

4. *Hallemos* $21^3_{[2}$.

   $e = máx\left\{k : n^k \leq m\right\} = 4$, $e = 4$.
   $a = máx\left\{k : k \cdot n^e \leq m\right\} = 1$, $a = 1$.
   Luego, $21^3_{[2} = 3^{4^3_{[2}} + (21 - 2^4)^3_{[2} = 3^{3^3} + 5^3_{[2} = 3^{3^3} + 3^3 + 1$.

5. *Hallemos* $34^\omega_{[2}$.

   $34 = 2^5 + 2 = 2^{2^2+1}$
   $e = máx\left\{k : n^k \leq m\right\} = 5$, $e = 5$.
   $a = máx\left\{k : k \cdot n^e \leq m\right\} = 1$, $a = 1$.
   $34^\omega_{[2} = \omega^{5^\omega_{[2}} + (34 - 2^5)^\omega_{[2} = \omega^{\omega^\omega+1} + \omega$.

Observación 2.1 *Si* α *es un ordinal tal que* $\alpha = \omega^{a_r} \cdot k_r + \ldots + \omega^{a_2} \cdot k_2 + \omega^{a_1} \cdot k_1$ *(con* $a_r > a_{r-1} > \cdots > a_2 > a_1$ *y* $k_1, \cdots, k_r$ *todos naturales), entonces* $\alpha < \omega^{a_r+1} < \omega^\omega$ *(Lema 1.3.3). Recordemos también que* $\epsilon = \sup\left\{\omega^\omega, \omega^{\omega^\omega}, \ldots\right\}$.

Definición 2.1.4

Para cada $k \geq 2$, *definimos dos funciones* $\underline{o}_k : \omega \longrightarrow \omega^\omega$ *y* $\bar{O}_k : \omega \longrightarrow \epsilon$ *del siguiente modo:*

$$\underline{o}_k(n) := n^\omega_{(k}$$
$$\bar{O}_k(n) := n^\omega_{[k}$$

Con la notación introducida presentamos ahora las sucesiones de Goodstein. En primer lugar una versión débil de las mismas que fue dado a conocer por Beckmann y McAloon.

Definición 2.1.5 (Sucesiones Débiles de Goodstein)

Sea m *un número natural, hagamos* $m_0 = m$ *y construyamos* m_1 *del siguiente modo: sustituimos la base 2 por 3 en la expresión en base 2 de* m_0 *y restamos* 1 *al resultado, es decir, en nuestra notación,*

$$m_1 = (m_0)^3_{(2} - 1$$

Los siguientes elementos m_i *de la sucesión se construyen aplicando el mismo procedimiento. En general,*

$$m_{i+1} = (m_i)^{i+3}_{(i+2} - 1$$

La sucesión de números así obtenida se denomina ***Sucesión Débil de Goodstein*** *comenzando por* m *en la base 2.*

La definición se generaliza sin dificultad al caso en que comencemos por una base $n \geq 2$ cualquiera, en ese caso, la expresión general sería:

$$m_{i+1} = (m_i)^{i+n+1}_{(i+n} - 1$$

y llamaríamos a la sucesión: Sucesión Débil de Goodstein comenzando por m en la base n.

Ejemplo 2.1.4

1. $m = 7$, $n = 3$
   $m_0 = m_{(3} = 2 \cdot 3 + 1 = 7$
   $m_1 = (m_0)^4_{(3} - 1 = 2 \cdot 4 + 1 - 1 = 2 \cdot 4 = 8.$
   $m_2 = 2 \cdot 5 - 1 = 5 + 4 = 9$
   $m_3 = 6 + 4 - 1 = 6 + 3 = 9$
   $m_4 = 7 + 3 - 1 = 7 + 2 = 9$
   $m_5 = 8 + 2 - 1 = 8 + 1 = 9$
   $m_6 = 9 + 1 - 1 = 9$
   $m_7 = 10 - 1 = 9$
   $m_8 = 9 - 1 = 8$
   $m_9 = 8 - 1 = 7$
   $\vdots$
   $m_{16} = 1$
   $m_{17} = 0$

2. $m = 15$,$n = 2$
   $m_0 = m_{(2} = 2^3 + 2^2 + 2 + 1$
   $m_1 = (m_0)^3_{(2} - 1 = 3^3 + 3^2 + 3 = 39$
   $m_2 = 4^3 + 4^2 + 3 = 83$
   $m_3 = 5^3 + 5^2 + 2 = 152$
   $m_4 = 6^3 + 6^2 + 1 = 253$
   $m_5 = 7^3 + 7^2 = 392$
   $m_6 = 8^3 + 8^2 - 1 = 8^3 + 7 \cdot 8 + 7 = 575$
   $\vdots$
   $m_{13} = 15^3 + 15 \cdot 7 = 3480$
   $\vdots$
   $m_{100} = 102^3 + 4 \cdot (102) + 25 = 1061641$
   $\vdots$

3. $m = 21,\ n = 2$

$m_0 = m_{(2} = 2^4 + 2^2 + 1 = 21$

$m_1 = 3^4 + 3^2 = 90$

$m_2 = 4^4 + 4^2 - 1 = 4^4 + 4 \cdot 3 + 3 = 271$

$\vdots$

$m_5 = 7^4 + 7 \cdot 3 - 1 = 7^4 + 7 \cdot 2 + 6 = 2421$

$\vdots$

$m_{11} = 13^4 + 13 \cdot 2 - 1 = 13^4 + 13 + 12 = 28586$

$\vdots$

$m_{23} = 25^4 + 25 = 390650$

$m_{24} = 26^4 + 25 = 457001$

$\vdots$

$m_{49} = 51^4 - 1 = 50 \cdot 51^3 + 50 \cdot 51^2 + 50 \cdot 51 + 50 = 6765200$

$\vdots$

La definición de las sucesiones débiles de Goodstein admite una generalización :

Definición 2.1.6

Sean $m \in \omega$ y $n \geq 2$. La ***Sucesión de Goodstein*** *comenzando por m en base n se define recursivamente del siguiente modo:*

$$m_0 = m$$

y para cada $k \geq 0$,

$$m_{k+1} = (m_k)^{k+n+1}_{[k+n} - 1$$

Ejemplo 2.1.5

1. $m = 3, n = 2$

$m_0 = 2 + 1 = 3$

$m_1 = 3 + 1 - 1 = 3$

$m_2 = 2$

$m_3 = 1$

$m_4 = 0$

2. $m = 8, n = 3$

$m_0 = 2 \cdot 3 + 2 = 8$

$m_1 = 2 \cdot 4 + 1 = 9$

$m_2 = 2 \cdot 5 = 10$

$m_3 = 2 \cdot 6 - 1 = 6 + 5 = 11$

$\vdots$

$m_8 = 11$

$m_9 = 12 - 1 = 11$

$\vdots$

$m_{20} = 0$

3. $m = 5, n = 2$

$m_0 = 2^2 + 1 = 5$

$m_1 = 3^3 = 27$

$m_2 = 4^4 - 1 = 3 \cdot 4^3 + 3 \cdot 4^2 + 3 \cdot 4 + 3 = 255$

$m_3 = 3 \cdot 5^3 + 3 \cdot 5^2 + 3 \cdot 5 + 2 = 467$

$m_4 = 3 \cdot 6^3 + 3 \cdot 6^2 + 3 \cdot 6 + 1 = 775$

$m_5 = 3 \cdot 7^3 + 3 \cdot 7^2 + 3 \cdot 7 = 1197$

$m_6 = 3 \cdot 8^3 + 3 \cdot 8^2 + 3 \cdot 8 - 1 = 3 \cdot 8^3 + 3 \cdot 8^2 + 2 \cdot 8 + 7 = 1751$

$\vdots$

$m_{13} = 3 \cdot 15^3 + 3 \cdot 15^2 + 2 \cdot 15 = 10830$

$m_{14} = 3 \cdot 16^3 + 3 \cdot 16^2 + 2 \cdot 16 - 1 = 3 \cdot 16^3 + 3 \cdot 16^2 + 16 + 15 = 13087$

$\vdots$

$m_{29} = 3 \cdot 31^3 + 3 \cdot 31^2 + 31 = 92287$

$m_{30} = 3 \cdot 32^3 + 3 \cdot 32^2 + 32 - 1 = 3 \cdot 32^3 + 3 \cdot 32^2 + 31 = 101407$

$\vdots$

$m_{61} = 3 \cdot 63^3 + 3 \cdot 63^2 = 762048$

$m_{62} = 3 \cdot 64^3 + 3 \cdot 64^2 - 1 = 3 \cdot 64^3 + 2 \cdot 64^2 + 63 \cdot 64 + 63 = 798719$

$\vdots$

$m_{125} = 3 \cdot (127)^3 + 2 \cdot (127)^2 + 63 \cdot 127 = 6185408$

$m_{126} = 3 \cdot (128)^3 + 2 \cdot (128)^2 + 63 \cdot 128 - 1 = 3 \cdot (128)^3 + 2 \cdot (128)^2 + 62 \cdot 128 + 127 = 6332287$

$\vdots$

4. $m = 7, n = 2$

$m_0 = 2^2 + 2 + 1$

$m_1 = 3^3 + 3 = 30$

$m_2 = 4^4 + 4 - 1 = 4^4 + 3 = 259$

$\vdots$

$m_5 = 7^7 = 823543$

$m_6 = 8^8 - 1 = 7 \cdot 8^7 + 7 \cdot 8^6 + 7 \cdot 8^5 + 7 \cdot 8^4 + 7 \cdot 8^3 + 7 \cdot 8^2 + 7 \cdot 8 + 7 = 16777215$

$\vdots$

$m_{13} = 7 \cdot 15^7 + 7 \cdot 15^6 + 7 \cdot 15^5 + 7 \cdot 15^4 + 7 \cdot 15^3 + 7 \cdot 15^2 + 7 \cdot 15 = 1281445305$

$m_{14} = 7 \cdot 16^7 + 7 \cdot 16^6 + 7 \cdot 16^5 + 7 \cdot 16^4 + 7 \cdot 16^3 + 7 \cdot 16^2 + 7 \cdot 16 - 1 =$
$7 \cdot 16^7 + 7 \cdot 16^6 + 7 \cdot 16^5 + 7 \cdot 16^4 + 7 \cdot 16^3 + 7 \cdot 16^2 + 6 \cdot 16 + 15 = 2004318063$

$\vdots$

$m_{29} = 7 \cdot 31^7 + 7 \cdot 31^6 + 7 \cdot 31^5 + 7 \cdot 31^4 + 7 \cdot 31^3 + 7 \cdot 31^2 + 6 \cdot 31 = 199007908698$

$m_{30} = 7 \cdot 32^7 + 7 \cdot 32^6 + 7 \cdot 32^5 + 7 \cdot 32^4 + 7 \cdot 32^3 + 7 \cdot 32^2 + 6 \cdot 32 - 1 =$
$7 \cdot 32^7 + 7 \cdot 32^6 + 7 \cdot 32^5 + 7 \cdot 32^4 + 7 \cdot 32^3 + 7 \cdot 32^2 + 5 \cdot 32 + 31 = 248276819135$

$\vdots$

5. $m = 266, n = 2$

$m_0 = 2^8 + 2^3 + 2 = 2^{2^{2+1}} + 2^{2+1} + 2$

$m_1 = 3^{3^{3+1}} + 3^{3+1} + 3 - 1 = 3^{3^{3+1}} + 3^{3+1} + 2 \approx 4{,}4 * 10^{38}$

$m_2 = 4^{4^{4+1}} + 4^{4+1} + 1 \approx 3{,}2 * 10^{617}$

$m_3 = 5^{5^{5+1}} + 5^{5+1} \approx 2{,}5 * 10^{10922}$

$m_4 = 6^{6^{6+1}} + 6^{6+1} - 1 = 6^{6^{6+1}} + 5 \cdot 6^6 + 5 \cdot 6^5 + 5 \cdot 6^4 + 5 \cdot 6^3 + 5 \cdot 6^2 + 5 \cdot 6 + 5$

$m_5 = 7^{7^{7+1}} + 5 \cdot 7^7 + 5 \cdot 7^5 + 5 \cdot 7^4 + 5 \cdot 7^3 + 5 \cdot 7^2 + 5 \cdot 7 + 4$

$\vdots$

El siguiente lema nos presenta una interesante propiedad de las funciones definidas en 2.1.4. Concretamente, el cambio de la base n a la base ω la podemos realizar en dos pasos sin que se afecte el resultado.

Lema 2.1.1 *Para cada* $m > 0$, $n \geq 2$, $k \geq n$

a. $m^{\omega}_{(n} = (m^{k}_{(n})^{\omega}_{(k}$

b. $m^{\omega}_{[n} = (m^{k}_{[n})^{\omega}_{[k}$

Es decir,

a. $\underline{o}_n(m) = \underline{o}_k(m^k_{(n})$

b. $\bar{O}_n(m) = \bar{O}_k(m^k_{[n})$

Demostración.

a. Usamos inducción sobre m.

i. Si $m < n$, claramente $\underline{o}_n(m) = m$ y $m^k_{(n} = m$ entonces $\underline{o}_k(m^k_{(n}) = \underline{o}_k(m) = m^\omega_{(k}$, dado que $k \geq n$ tenemos que $\underline{o}_k(m) = m$. De aquí que $\underline{o}_n(m) = \underline{o}_k(m^k_{(n}).$

ii. Si $m \geq n$,Sean $e = \text{máx}\{r : n^r \leq m\}$ y $a = \text{máx} = \{r : r \cdot n^e \leq m\}$ entonces

$$\underline{o}_n(m) = m^\omega_{(n} = \omega^e \cdot a + (m - a \cdot n^e)^\omega_{(n} \qquad (1)$$

Ahora, $m^k_{(n} = k^e \cdot a + (m - n^e \cdot a)^k_{(n}$

$$\underline{o}_k(m^k_{(n}) = \underline{o}_k\left(k^e \cdot a + (m - n^e \cdot a)^k_{(n}\right) = \underline{o}_k(k^e \cdot a) + \underline{o}_k\left[(m - n^e \cdot a)^k_{(n}\right] \quad (2)$$

Veamos,

- $\underline{o}_k(k^e \cdot a) = (k^e \cdot a)^\omega_{(k} = \omega^e \cdot a.$

- Como $a = \text{máx}\{r : r \cdot n^e \leq m\}$ entonces $n^e \cdot a \leq m$ y $0 < m - n^e \cdot a < m$ entonces por hipótesis inductiva tenemos que:

$$\underline{o}_k\left[(m - \cdot n^e \cdot a)^k_{(n}\right] = \underline{o}_n(m - n^e \cdot a).$$

Entonces en (2) tenemos $\underline{o}_k(m^k_{(n}) = \omega^e \cdot a + (m - a \cdot n^e)^\omega_{(n} \qquad (3).$

Por lo tanto, de (1) y (3) tenemos que $\underline{o}_n(m) = \underline{o}_k(m^k_{(n}).$

Luego por Principio de Inducción Matemática tenemos que $\underline{o}_n(m) = \underline{o}_k(m^k_{(n})$ para todo $m > 0$.

b. Usamos inducción sobre m.

i. Si $m < n$, claramente $\bar{O}_n(m) = m$ y $m^k_{[n} = m$ entonces $\bar{O}_k(m) = m^\omega_{[k}$, como $k \geq n$ tenemos que $\bar{O}_k(m) = m$. Es decir, $\bar{O}_n(m) = \bar{O}_k(m^k_{[n}).$
ii. Si $m \geq n$,

Sean $a = \text{máx}\{r : r \cdot n^e \leq m\}$ y $e = \text{máx}\{r : n^r \leq m\}$ entonces

$$\bar{O}_n(m) = m^{\omega}_{[n} = \omega^{e^{\omega}_{[n}} \cdot a + (m - n^e \cdot a)^{\omega}_{[n} \qquad (1)$$

Ahora, $m^k_{[n} = k^{e^k_{[n}} \cdot a + (m - n^e \cdot a)^k_{[n}$
$\bar{O}_k(m^k_{[n}) = \bar{O}_k\left(k^{e^k_{[n}} \cdot a + (m - n^e \cdot a)^k_{[n}\right) = \bar{O}_k(k^{e^k_{[n}} \cdot a) + \bar{O}_k\left[(m - \cdot n^e \cdot a)^k_{[n}\right] \qquad (2)$

Observemos,

- $\bar{O}_k(k^{e^k_{[n}} \cdot a) = \left(k^{e^k_{[n}} \cdot a\right)^{\omega}_{(k} = \omega^{e^k_{[n}} \cdot a.$
- $\bar{O}_k\left[(m - n^e \cdot a)^k_{[n}\right] = \bar{O}_n(m - n^e \cdot a)$, ya que $(m - n^e \cdot a) < m$ entonces podemos aplicar hipótesis inductiva.

Reemplazando en (2) tenemos , $\bar{O}_k(m^k_{[n}) = \omega^{e^k_{[n}} \cdot a + (m - n^e \cdot a)^{\omega}_{[n} \qquad (3).$

De (1) y (3) tenemos que $\bar{O}_n(m) = \bar{O}_k(m^k_{[n})$.

Así que por Principio de Inducción Matemática tenemos que $\bar{O}_n(m) = \bar{O}_k(m^k_{[n})$ para todo $m > 0$. ∎

Otra importante propiedad de las funciones $\bar{O}$ y $\underline{o}$ es la monotonía. El siguiente lema nos muestra esto.

Lema 2.1.2 *Sean $m_2 > m_1 > 0$ y $k \geq 2$. Entonces:*

a. $\underline{o}_k(m_1) < \underline{o}_k(m_2)$

b. $\bar{O}_k(m_1) < \bar{O}_k(m_2)$

Demostración.

a. Hagamos inducción sobre m_2: supongamos que siempre que $n < m_2$ se tiene que si $0 < t < n$ entonces $\underline{o}_k(t) < \underline{o}_k(n)$.
Si $m_1 < m_2 \leq k$ entonces $\underline{o}_k(m_1) = m_1 < m_2 = \underline{o}_k(m_2)$. Si $m_1 \leq k < m_2$ entonces $\underline{o}_k(m_1) = m < \underline{o}_k(m_2)$ pues $\underline{o}_k(m_2)$ contiene una potencia de ω.
Si $k < m_1 < m_2$ tenemos: $m_1{}^{\omega}_{(k} = \omega^{e_1} \cdot a_1 + (m_1 - a_1 \cdot k^{e_1})^{\omega}_{(k}$ donde
$e_1 = \text{máx}\{r : k^r \leq m_1\}$ y $a_1 = \text{máx}\{r : r \cdot k^{e_1} \leq m_1\}$ y $m_2{}^{\omega}_{(k} = \omega^{e_2} \cdot a_2 + (m_2 - a_2 \cdot k^{e_2})^{\omega}_{(k}$ donde $e_2 = \text{máx}\{r : k^r \leq m_2\}$ y $a_2 = \text{máx}\{r : r \cdot k^{e_2} \leq m_2\}$
Como $m_1 < m_2$ entonces $e_1 \leq e_2$.

Si $e_1 < e_2$ entonces por propiedad de los ordinales se tiene que:

$$\omega^{e_1} \cdot a_1 + (m_1 - a_1 \cdot k^{e_1})^{\omega}_{(k} < \omega^{e_2} \cdot a_2.$$

Luego $\underline{o}_k(m_1) < \underline{o}_k(m_2)$. Si $e_1 = e_2$ consideremos los coeficientes a_1 y a_2. Podemos observar que $a_1 \leq a_2$ por como están definidos.
Si $a_1 < a_2$ entonces $\omega^{e_1} \cdot a_1 < \omega^{e_1} \cdot a_2$. Luego $\underline{o}_k(m_1) < \underline{o}_k(m_2)$.

Ahora, si $a_1 = a_2$ y teniendo que $e_1 = e_2$ entonces con $m_1 < m_2$ tenemos que $(m_1 - k^{e_1} \cdot a_1) < (m_2 - k^{e_1} \cdot a_2)$. Por hipótesis inductiva tenemos:

$$\underline{o}_k(m_1 - k^{e_1} \cdot a_1) < \underline{o}_k(m_2 - k^{e_2} \cdot a_2)$$
$$\omega^{e_1} \cdot a_1 + (m_1 - k^{e_1} \cdot a_1)^{\omega}_{(k} < \omega^{e_2} \cdot a_2 + (m_1 - k^{e_2} \cdot a_2)^{\omega}_{(k}$$
$$\underline{o}_k(m_1) < \underline{o}_k(m_2)$$

Por lo tanto, por Principio de Inducción Matemática tenemos que:

$$\underline{o}_k(m_1) < \underline{o}_k(m_2), \text{donde } 0 < m_1 < m_2.$$

La parte $(b.)$ del teorema se hace de forma similar.

■

Finalmente el lema 2.1.3 nos muestra una relación entre las funciones $\underline{o}$ y $\bar{O}$.

Lema 2.1.3 *Si $n \geq 2$ y $0 < m < n$ entonces, $\underline{o}_n(m) = \bar{O}_n(m) = m$; y si $m \geq n$, entonces $\bar{O}_n(m) \geq \underline{o}_n(m) \geq m$ para cualquier m*

Demostración. Si $m \geq n$ demostremos que $\bar{O}_n(m) \geq \underline{o}_n(m) \geq m$ para cualquier m por inducción.

$\underline{o}_n(m) = \omega^e \cdot a + (m - n^e \cdot a)^{\omega}_{(n}$ y $\bar{O}_n(m) = \omega^{e^{\omega}_{[n}} \cdot a + (m - n^e \cdot a)^{\omega}_{[n}$.
Por hipótesis inductiva tenemos que: $(m - n^e \cdot a)^{\omega}_{[n} \geq (m - n^e \cdot a)^{\omega}_{(n}$.

Ahora si $e = n$ entonces $e^{\omega}_{[n} = n^{\omega}_{[n} = \omega$. Así, $\omega^{e^{\omega}_{[n}} = \omega^{\omega}$. Luego, $\omega^e \leq \omega^{\omega}$. Si $e > n$ entonces $e^{\omega}_{[n} = \omega^{e'} \cdot a' + \left(e - a' \cdot n^{e'}\right)^{\omega}_{[n}$ y además $e < \omega^{e'} \cdot a'$ esto implica $e < \omega^{e'} \cdot a' + \left(e - a' \cdot n^{e'}\right)^{\omega}_{[n}$.

Luego por Lema 1.3.3 tenemos que $\omega^e \cdot a < \omega^{e^{\omega}_{[n}} \cdot a$.
De lo anterior tenemos $\bar{O}_n(m) = \omega^{e^{\omega}_{[n}} \cdot a + (m - n^e \cdot a)^{\omega}_{[n} \geq \underline{o}_n(m) = \omega^e \cdot a + (m - n^e \cdot a)^{\omega}_{(n}$.

■

2.2. Teorema de Goodstein

Teorema 2.2.1 (Teorema de Goodstein.)

Denotemos por m_i la sucesión de Goodstein comenzando por m en base $n \geq 2$; entonces, para cada número natural $m > 0$ y cada base n, existe un k tal que $m_k = 0$.

Demostración.

La sucesión m_i se obtiene del siguiente modo:

$$m_0 = m_{\lfloor n}$$

$$m_1 = (m_0)_{\lfloor n}^{n+1} - 1$$

$$m_2 = (m_1)_{\lfloor n+1}^{n+2} - 1$$

$$\vdots$$

Consideremos una sucesión paralela de ordinales O_i obtenidos mediante

$$O_i = \bar{O}_{n+i}(m_i)$$

es decir,

$$\begin{array}{ll} m_0 = m_{\lfloor n} & O_0 = \bar{O}_n(m_0) = \bar{O}_n(m) \\ m_1 = (m_0)_{\lfloor n}^{n+1} - 1 & O_1 = \bar{O}_{n+1}(m_1) = \bar{O}_{n+1}((m_0)_{\lfloor n}^{n+1}) - 1) \\ m_2 = (m_1)_{\lfloor n+1}^{n+2} - 1 & O_2 = \bar{O}_{n+2}(m_2) = \bar{O}_{n+2}((m_1)_{\lfloor n+1}^{n+2} - 1) \\ \dots & \end{array}$$

es decir, para cada $k > 0$,

$$O_{k+1} = \bar{O}_{n+k+1}(m_{k+1}) = \bar{O}_{n+k+1}((m_k)_{\lfloor n+k}^{n+k+1} - 1)$$

por el lema 2.1.2,

$$\bar{O}_{n+k+1}((m_k)_{\lfloor n+k}^{n+k+1} - 1) < \bar{O}_{n+k+1}((m_k)_{\lfloor n+k}^{n+k+1})$$

y por lema 2.1.1,

$$\bar{O}_{n+k+1}((m_k)_{\lfloor n+k}^{n+k+1}) = \bar{O}_{n+k}(m_k) = O_k$$

es decir, $O_{k+1} < O_k$ para cada k, de modo que los ordinales forman una sucesión estrictamente decreciente

$$O_0 > O_1 > \cdots > O_k > \cdots ;$$

como no hay sucesiones estrictamente decrecientes infinitas de ordinales, forzosamente hay algun i tal que $O_i = 0$. pero si ahora aplicamos el lema 2.1.3 , para cada $k > 0$ es $O_k \geq m_k$, y por lo tanto también $m_i = 0$. ■

Teorema 2.2.2 *Sea m_i la sucesión débil de Goodstein comenzando por m en la base n; entonces, para cada número natural $m > 0$ y cada base $n \geq 2$, existe un k tal que $m_k = 0$.*

Demostración.

Probemos el teorema para las sucesiones débiles de Goodstein.
La sucesión m_i se obtiene del siguiente modo:

$$m_0 = m_{(n}$$

$$m_1 = (m_0)^{n+1}_{(n} - 1$$

$$m_2 = (m_1)^{n+2}_{(n+1} - 1$$

$$\vdots$$

Consideremos una sucesión paralela de ordinales o_i obtenidos mediante

$$o_i = \underline{o}_{n+i}(m_i)$$

es decir,

$$\begin{array}{ll} m_0 = m_{(n} & o_0 = \underline{o}_n(m_0) = \underline{o}_n(m) \\ m_1 = (m_0)^{n+1}_{(n} - 1 & o_1 = \underline{o}_{n+1}(m_1) = \underline{o}_{n+1}((m_0)^{n+1}_{(n}) - 1) \\ m_2 = (m_1)^{n+2}_{(n+1} - 1 & o_2 = \underline{o}_{n+2}(m_2) = \underline{o}_{n+2}((m_1)^{n+2}_{n+1} - 1) \\ \ldots & \end{array}$$

es decir, para cada $k > 0$,

$$o_{k+1} = \underline{o}_{n+k+1}(m_{k+1}) = \underline{o}_{n+k+1}((m_k)^{n+k+1}_{(n+k} - 1)$$

por el lema 2.1.2,

$$\underline{o}_{n+k+1}((m_k)^{n+k+1}_{n+k} - 1) < \underline{o}_{n+k+1}((m_k)^{n+k+1}_{(n+k})$$

y por lema 2.1.1,

$$\underline{o}_{n+k+1}((m_k)_{(n+k)}^{n+k+1}) = \underline{o}_{n+k}(m_k) = o_k$$

es decir, $o_k + 1 = o_k$ para cada k, de modo que los ordinales forman una sucesión estrictamente decreciente

$$o_0 > o_1 > \cdots > o_k > \cdots ;$$

como no hay sucesiones estrictamente decrecientes infinitas de ordinales, forzosamente hay algun i tal que $o_i = 0$. pero si ahora aplicamos el lema 2.1.3 , para cada $k > 0$ es $o_k \geq m_k$, y por lo tanto también $m_i = 0$ ■

APÉNDICE A

EL JUEGO DE LA HIDRA

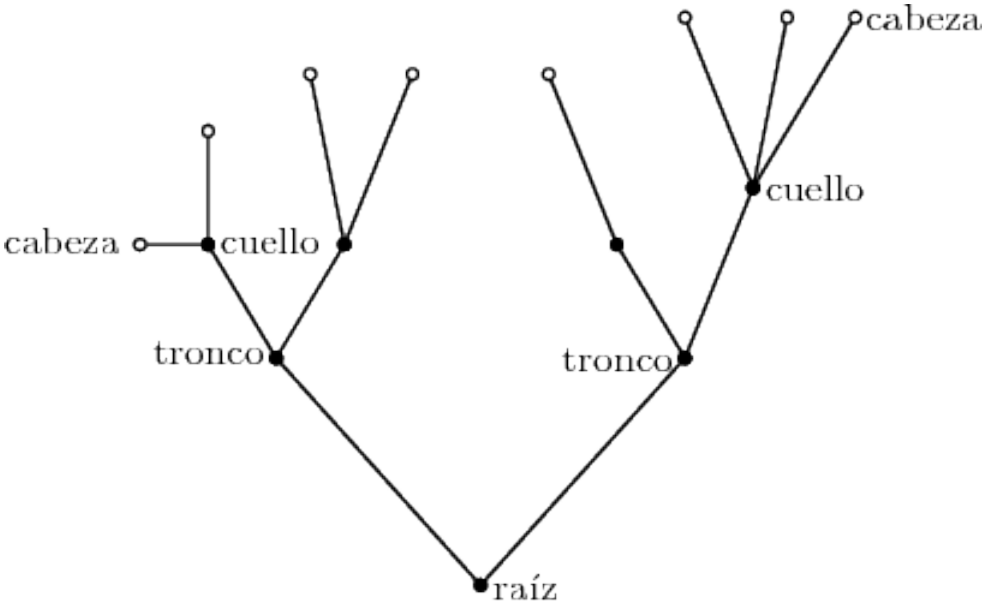
De acuerdo con la mitología griega Hércules como castigo por haber matado a su propia esposa e hijos debió cumplir penitencia y trabajos forzados por sus asesinatos, uno de estos castigos era el de matar a la Hidra quien era un peligroso monstruo de sangre envenenada y muchas cabezas. Hércules enfrento a la Hidra en una batalla, cortándole sus cabezas con una espada. Sin embargo cada vez que Hércules cortaba una cabeza, del cuerpo de la Hidra brotaban muchas mas cabezas en sustitución de la que cortaba. Pero de acuerdo con la historia sabemos que Hércules ganó la batalla.

Los matemáticos Jeff Paris y Leo Harrington quienes demostraron la indecibilidad del Teorema de Goodstein, también crearon un juego, llamado el juego de la Hidra, teniendo como base el comportamiento de las sucesiones de Goodstein.

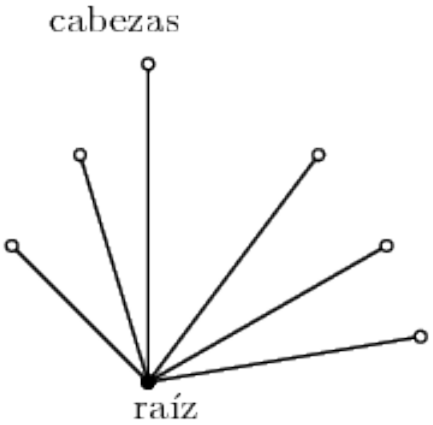
A continuación mostraremos un modelo matemático de las Hidras y de la batalla de Hércules. Representaremos matemáticamente a la Hidra como un árbol y a Hércules como una flecha apuntando a una de las cabezas del árbol.

Definición A.0.1

Una Hidra H es un árbol, esto es, un grafo finito acíclico y conectado, con un nodo fijo llamado raíz y denotado por R_H. Cualquier nodo terminal distinto de la raíz se llama cabeza.



Hidra con 8 cabezas



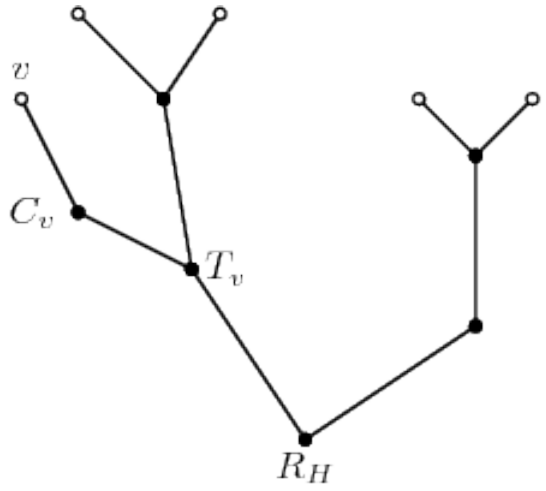
Hidra estrella

Hidra lineal

Hay Hidras que aparte de raíz y cabezas se componen de cuello, tronco y cuerpo. En las siguientes definiciones veremos esto.

Definición A.0.2

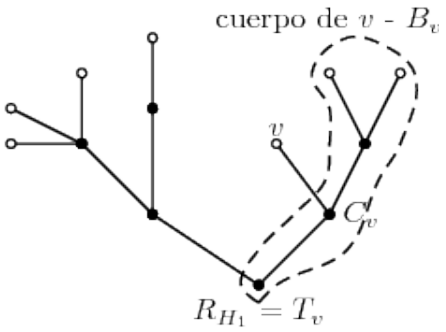
Sea v una cabeza de una Hidra H. El nodo anterior a v se llama cuello y se denota por C_v. Si el cuello C_v tiene a su vez un nodo que lo antecede en la ruta hacia la raíz R_H, entonces a este nodo lo llamamos tronco de v y lo denotamos T_v. En caso de que el cuello $C_v = R_H$, entonces decimos que v no tiene tronco.



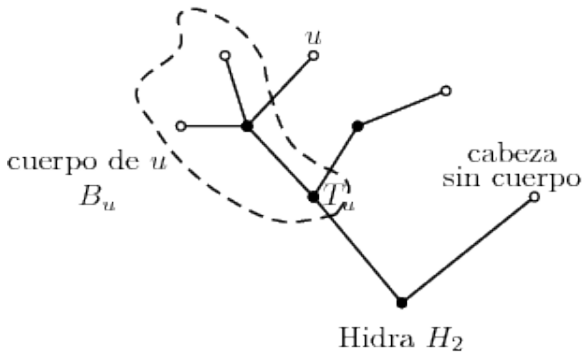
Hidra H

Definición A.0.3

Sea H un Hidra y sea v una cabeza de H. Si v tiene tronco, definimos el cuerpo de v el cual denotamos por B_v como el subárbol que contiene los nodos C_v y todos sus sucesores, eliminando v y luego agragándole el nodo T_v como raíz. En caso de que v no tenga tronco, decimos que v no posee cuerpo.



Hidra H_1

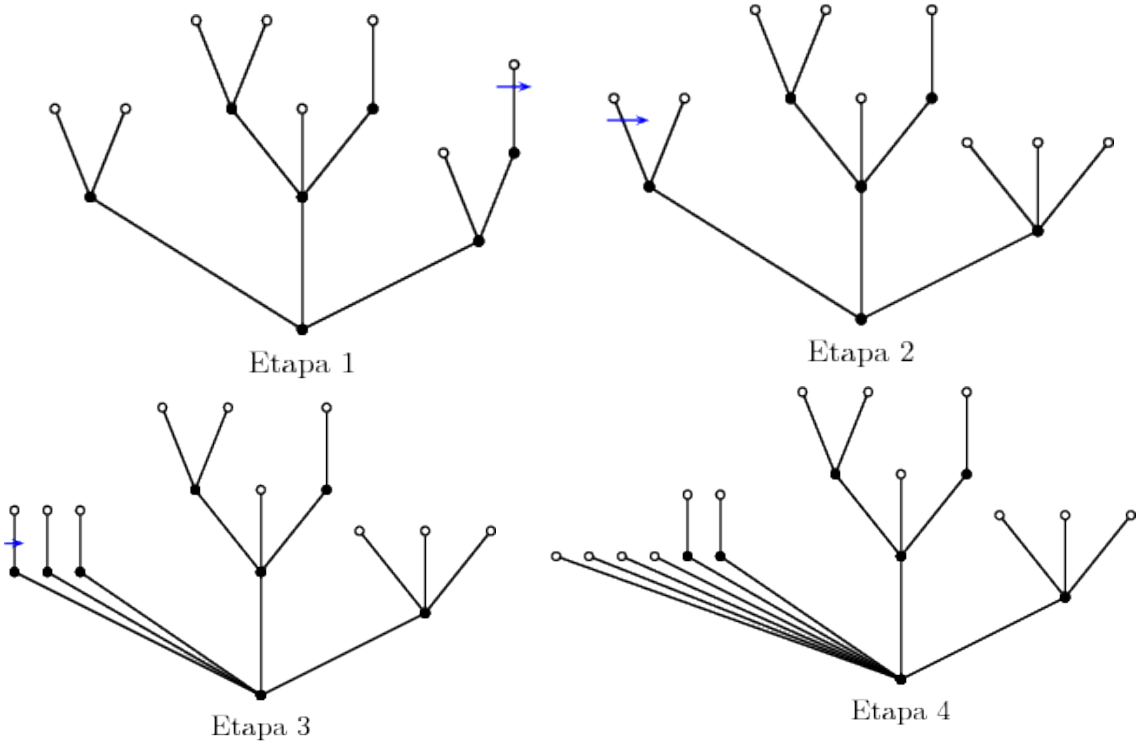


Hidra H_2

El proceso de reproducción de las cabezas de la Hidra luego del corte de una de ellas presentado por Kirby y Paris viene descrito en la siguiente definición.

Definición A.0.4

Sea H una Hidra. Una batalla entre Hércules y la Hidra H es una sucesión de Hidras $H_0 = H, H_1, H_2, \ldots$ donde la Hidra H_n se obtiene de la anterior, H_{n-1}, mediante el siguiente esquema de reproducción: Hércules corta una cabeza cualquiera $v \in H_{n-1}$; en respuesta la Hidra añade n réplicas del cuerpo de v, a partir del tronco T_v, si v tiene cuerpo. En caso de que la cabeza cortada no tenga cuerpo, entonces la Hidra no se reproduce en esta etapa. Hércules gana la batalla si, despues de un número finito de etapas k (el largo de la batalla), la Hidra H_k es justamente la raíz.



Teorema A.0.3 *Contra cualquier Hidra inicial H_0 toda estrategia de Hércules es una estrategia ganadora.*

Existen números ordinales asociados a las Hidras. En la siguiente definición describimos el procedimiento para asociarle a la Hidra H un número ordinal α.

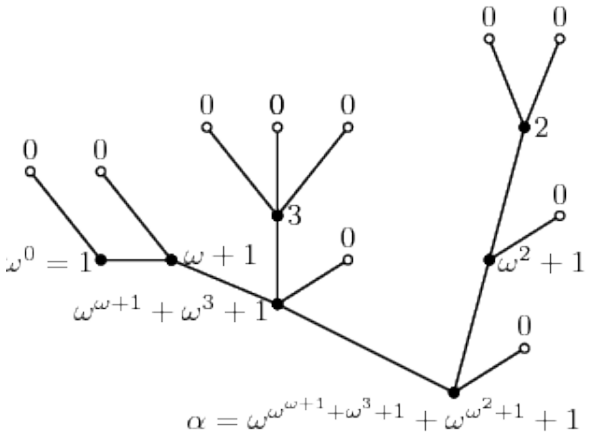
Definición A.0.5

Sea H una Hidra. Podemos asociar a H con un número ordinal $\alpha = \alpha(H)$ de acuerdo con el siguiente procedimiento recursivo: a cada nodo $s \in H$ le asociamos un número ordinal:

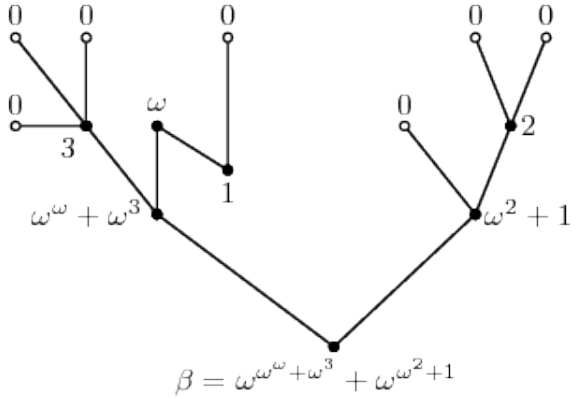
(a) Si s es una cabeza, le asociamos el número ordinal 0.

(b) Si s no es una cabeza, entonces s tiene digamos k nodos sucesores inmediatos. Sean $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_k$ los números ordinales asociados a estos sucesores inmediatos. Entonces asociamos a s el número ordinal $\omega^{\beta_1} + \omega^{\beta_2} + \cdots + \omega^{\beta_k}$.

Finalmente, $\alpha(H)$ será el ordinal asociado al nodo R_H.

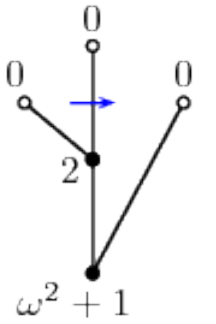


Hidra $H(\alpha)$ correspondiente al ordinal α

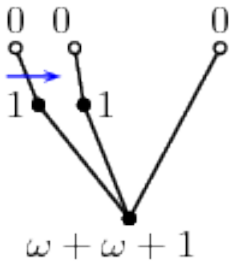


Hidra $H(\beta)$ correspondiente al ordinal β

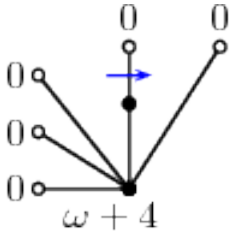
A continuación se mostraran dos ejemplos de como se le asignan los ordinales a las Hidras en una batalla.



Etapa 1



Etapa 2



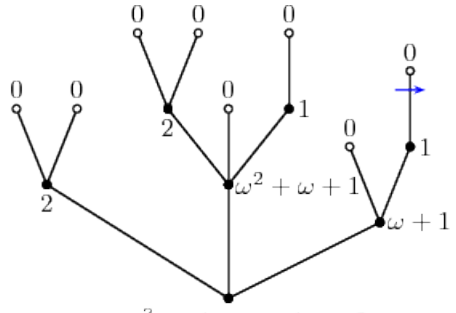
Etapa 3

Etapa 4

⋮

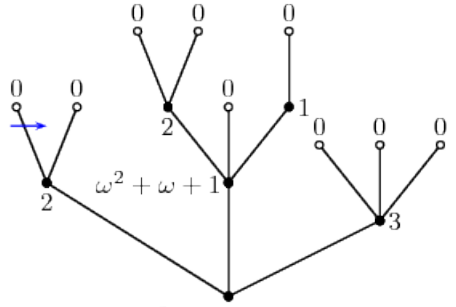
Etapa 11

Etapa 12
Muerte de la Hidra



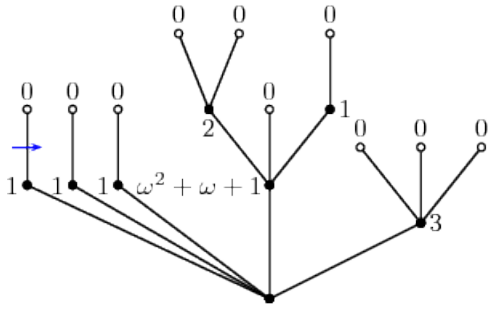
$\alpha_0 = \omega^{\omega^2+\omega+1} + \omega^{\omega+1} + \omega^2$

Etapa 1



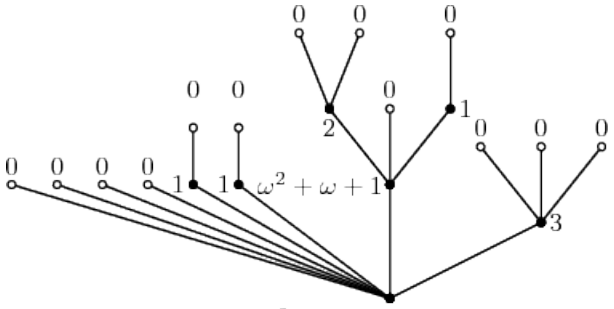
$\alpha_1 = \omega^{\omega^2+\omega+1} + \omega^3 + \omega^2$

Etapa 2



$\alpha_2 = \omega + \omega + \omega + \omega^{\omega^2+\omega+1} + \omega^3$

Etapa 3



$\alpha_3 = \omega^{\omega^2+\omega+1} + \omega^3 + \omega + \omega + 4$

Etapa 4

COMENTARIOS FINALES

1. La teoría de ordinales presentada en este trabajo fue conocida básicamente en desarrollo de la modalidad de cursos electivos del Programa de Matemáticas. En este sentido resaltó la importancia de dicha modalidad pues contribuye a la fortaleza académica de los egresados.

2. Una de las motivaciones para la realización de este trabajo fue el reconocimiento que tiene el Teorema de Goodstein de ser un indecidible en la Aritmética de Peano. Al presentar el Teorema y su demostración con Teoría de Conjuntos queda abierta en la Universidad una puerta para que se motive el interés por otros indecidibles y para que además se empiece a ahondar en demostraciones de indecibilidad.

2. Con la elaboración y presentación de este trabajo espero hacer un aporte significativo de la divulgación de la Teoría de Conjuntos en la Universidad y una invitación a los estudiantes de matemáticas a acercarse al estudio de esta importante área de la Matemática.

BIBLIOGRAFÍA

[1] Blasco, J.M. *Notas sobre el Teorema de Goodstein*. Universidad de Barcelona, 2005.

[2] Caicedo, A.E. *Goodstein's function*.California Institute of Technology, 2007.

[3] K. Hrbacek, T. Jech. *Introduction to set theory*. Third Edition, Marcel Dekker, New York, 1999.

[4] Sladek,Will. *The Termite and the Tower: Goodstein sequences and provability in PA*. 2007.

[5] Piza, Eduardo. *Hércules contra la Hidra y la muerte del Internet*. Revista de Matemática: Teoría y Aplicaciones 2004.