Instituto Politécnico Nacional

Escuela Superior de Física y Matemáticas

TESIS

sobre la indemostrabilidad del teorema de Goodstein

que para obtener el grado de

Licenciado en Física y Matemáticas

Presenta

Gabriel Martínez González

Dirigido por

Doctor David José Fernández Bretón

2026

Agradecimientos

XXX
XXX
XXX

Resumen

Desde que Kurt Gödel desmostró sus famosos teoremas de incompletitud en 1931, los matemáticos se han encontrado con una gran cantidad de enunciados que, aunque pueden ser escritos en una cierta teoría, no pueden ser demostrados. En este trabajo se aborda como eje central el *teorema de Goodstein*, un teorema que habla de unas ciertas sucesiones de números naturales y su extraño y completamente antiintuitivo comportamiento. Además, estudiamos de forma paralela unas extrañas estructuras llamadas *hidras* las cuáles tienen un comportamiento parecido a las sucesiones de Goodstein. Para esto nos hemos valido de la teoria de conjuntos, en especial de la teoría de ordinales; así como de herramientas de la teoria de modelos. Todo esto con el objetivo de demostrar el teorema de Goodstein en teoría de conjuntos y dar una prueba sólida, y lo mejor explicada posible, sobre la imposibilidad de demostrar dicho teorema bajo los axiomas que Giuseppe Peano publicó en 1889 (o un conjunto equivalente de axiomas). Así mismo, desarrollaremos las herramientas necesarias para encontrar las conexiones entre las sucesiones de Goodstein y las hidras, y también demostraremos que el hecho de que las hidras puedan ser derrotadas bajo cualquier estrategía es algo indemostrable bajo los mismos axiomas de Peano. Ambas pruebas de indemostrabilidad se darán por medio de teoremas distintos, aunque valge la pena aclarar que, dadas las conexiones, ambos resultados se podrían resolver de la misma forma.

En el primer capítulo, nos encargamos de dar todo resultado que se podría abordar en un curso de licenciatura en matemáticas o equivalente, en el segundo capítulo presentamos nuestros objetos de estudio: las sucesiones de Goodstein y las hidras, en el tercer capítulo desarrollamos nuestra teoría de la aritmética, es decir, aquellas consecuencias de los axiomas de Peano, y también veremos la herramienta más importante de todo este trabajo: los conjuntos $\alpha-$grandes, en el cuarto capítulo veremos las últimas herramientas necesarias para probar la indemostrabilidad de los teoremas mencionador, y finalmente en el quinto capítulo mencionaremos una equivalencia útil en muchas áreas de las matemáticas, y daremos una prueba de que las sucesiones de Goodstein son funciones computables.

Índice general

Capítulo 1

Preliminares

En este capítulo abordaremos las herramientas básicas para abordar los problemas que son el objetivo de este trabajo. Así mismo, este capítulo se compone de temas que se podrían dar en algún curso de licenciatura, o que de hecho se dan, enfocandolos sobre todo a lo necesario para este escrito.

1.1. Propiedades de los ordinales

A continuación se presenta la teoria de ordinales, su tratamiento en la teoría de conjuntos y sus relaciones con elementos importantes de la matemática, como los segmentos iniciales o los buenos ordenes.[1]

1.1 Definición. Un conjunto α es llamado un ordinal si α es transitivo y estrictamente bien ordenado por $\in$.

La definición anterior se puede escribir de la siguiente forma: α es ordinal si $(\forall a, b, c \in \alpha)$,

$$(a \in b \wedge b \in c) \Longrightarrow a \in c,$$

y todo subconjunto de α tiene primer elemento.

1.2 Teorema. *α es un ordinal si, y sólo si, α es transitivo y se cumple la tricotomía bajo $\in$.*

Demostración. Definimos $\prec$ como la relación tal que, para cualesquiera β y γ, elementos de α,

$$\beta \prec \gamma \Longleftrightarrow (\beta \in \gamma \vee \beta = \gamma)$$

Es decir, $\prec$ es el orden parcial inducido por la relación $\in$ en α. Luego, consideremos el subconjunto de α $\{\beta, \gamma\}$. Como $\prec$ es un buen orden, tenemos que $\beta \prec \gamma \vee \gamma \prec \beta$. Así, tenemos que:

$$\beta \in \gamma \vee \beta = \gamma \vee \gamma \in \beta$$

□

Considerando $\langle X, \prec \rangle$ un buen orden estricto. Entonces, $\prec$ es una relación bien fundada estricta sobre X. Luego, existe exactamente un conjunto transitivo α, llamado *el colapso de Mostowki* de $\langle X, \prec \rangle$, y una única biyección $F : X \longrightarrow \alpha$, llamada *la función colapsante* tal que

$$(\forall x, x' \in X)(x \prec x' \Longleftrightarrow F(x) \in F(x')) \qquad \text{(M)}$$

1.3 Teorema. *Sea α un conjunto. Entonces, α es un ordinal si, y sólo si, α es el colapso de Mostowski de un buen orden estricto $\langle X, \prec \rangle$.*

Demostración. Si α es un ordinal, entonces α es el colapso de Mostowski de $\langle \alpha, \in \rangle$, con la función colapsante dada por la identidad. Por otro lado, se muestra que si α es el colapso de Mostowski de un buen orden estricto $\langle X, \prec \rangle$, entonces α es un ordinal y la función colapsante es un isomorfismo de orden entre $\langle X, \prec \rangle$ y $\langle \alpha, \in \rangle$. □

1.4 Proposición. *Si $\langle X, \prec_X \rangle$ y $\langle Y, \prec_Y \rangle$ son isomorfos (bajo su orden parcial estricto), entonces estos tienen el mismo colapso de Mostowski.*

Demostración. Sea α es colapso de Mostowski de $\langle X, \prec_X \rangle$ y $F : X \longrightarrow \alpha$ su función colapsante. Entonces, se satisface (M). Luego, sea $\varphi : X \longrightarrow Y$ el isomorfismo de orden parcial estricto entre Y y X. Tomemos $F' = F \circ \varphi$, una biyección. Observemos que si tenemos $y, y' \in Y$ y $x, x' \in X$ tales que $x = \varphi(y)$ y $x' = \varphi(y')$, entonces:

$$y \prec_Y y' \iff x \prec_X x' \iff F(x) \in F(x') \iff F(\varphi(y)) \in F(\varphi(y')) \iff F'(y) \in F'(y')$$

Así pues, tomando F' como la función colapsante de $\langle Y, \prec_Y \rangle$, tenemos que α es el colapso de Mostowski de $\langle Y, \prec_Y \rangle$. Esto completa la prueba. □

1.5 Definición. Se define el conjunto WOT como el conjunto de las parejas ordenadas $\langle x, y \rangle$ tales que x es un buen orden estricto y y es el colapso de Mostowski de x.

Lo anterior puede escribirse como:

$$\text{WOT} = \{\langle x, y \rangle | x \text{ es buen orden estricto} \wedge y \text{ es colapso de Mostowski de } x\}$$

1.6 Proposición. *WOT es una clase funcional que satisface lo siguiente:*

1. *Si $\langle x, y \rangle \in$ WOT, entonces x y $\langle y, \in \rangle$ son bien ordenado estricto isomorfos.*
2. *El dominio de WOT es la clase de todos los buenos ordenes estrictos.*
3. *Para cualesquiera buenos ordenes estrictos x y y, y para todo ordinal z, si $\langle x, z \rangle \in$ WOT y $x \cong y$, entonces $\langle y, z \rangle \in$ WOT.*

Demostración. Que sea clase funcional viene del hecho de que el colapso de Mostowski es único. Por otro lado:

1. Como $\langle x, y \rangle \in$ WOT, x es buen orden estricto, de la forma $\langle X, \prec \rangle$, y y su colapso de Mostowski. Luego, existe una función biyectiva $F : X \longrightarrow y$ tal que se satisface (M), ecuación la cuál garantiza que F preserva el orden entre $x = \langle X, \prec \rangle$ y $\langle y, \in \rangle$. Más aún, por un teorema anterior, ya sabemos que $\in$ es un orden parcial estricto en y (por ser colapso de Mostowski, luego ordinal), por lo que se satisface la proposición, con F el isomorfismo.

2. Inmediato del hecho de que sólo pedimos que x sea un buen orden estricto para asegurar la existencia de su colapso de Mostowski.

3. Por la proposición anterior, x y y tienen el mismo colapso de Mostowski, el cuál, por hipótesis, es z. Luego, por la proposición anterior, como y es un buen orden estricto y z su colapso de Mostowski, $\langle y, z \rangle \in$ WOT.

□

1.7 Definición. Sean X un conjunto:

- Sea $\langle X, \prec \rangle$ un buen orden estricto. Se define el tipo de orden de $\langle X, \prec \rangle$, escrito como $\text{ot}(\langle X, \prec \rangle)$, como el único ordinal α tal que

$$\langle X, \prec \rangle \cong \langle \alpha, \in \rangle.$$

- Sea $\langle X, \preceq \rangle$ un buen orden, y sea

$$\prec = \{(x, y) \in X \times X | x \preceq \wedge x \neq y\},$$

el buen orden estricto correspondiente a $\preceq$. Se define el tipo de orden $\text{ot}(\langle X, \preceq \rangle)$ como sigue:

$$\text{ot}(\langle X, \preceq \rangle) = \text{ot}(\langle X, \prec \rangle).$$

1.8 Proposición.

$$\text{ot}(\langle X, \preceq \rangle) = \alpha \Longleftrightarrow \langle \langle X, \prec \rangle, \alpha \rangle \in WOT.$$

Demostración. Notemos que

$$\text{ot}(\langle X, \preceq \rangle) = \alpha \Longleftrightarrow \text{ot}(\langle X, \prec \rangle) = \alpha.$$

Si $\text{ot}(\langle X, \prec \rangle) = \alpha$, por ser $\langle X, \prec \rangle$ buen orden estricto, existe un β, ordinal, tal que β es el colapso de Mostowski de $\langle X, \prec \rangle$. Luego $\langle \langle X, \prec \rangle, \beta \rangle \in \text{WOT}$, y por la proposición anterior, $\langle X, \prec \rangle \cong \langle \beta, \in \rangle$. Por como se define el tipo de orden, $\alpha = \beta$ y $\langle \langle X, \prec \rangle, \alpha \rangle \in \text{WOT}$.
Por otro lado, si suponemos $\langle \langle X, \prec \rangle, \alpha \rangle \in \text{WOT}$, de inmediato tenemos (por la proposición anterior)

$$\langle X, \prec \rangle \cong \langle \alpha, \in \rangle,$$

luego $\text{ot}(\langle X, \preceq \rangle) = \alpha$. □

1.9 Definición. La clase de todos los ordinales se denota ON.

1.10 Lema.

$$(\forall \alpha \in ON)(\alpha \subseteq ON).$$

Demostración. Sea $\alpha \in \text{ON}$ y $\beta \in \alpha$. Como α es transitivo, $\beta \subseteq \alpha$. La restricción de buen orden estricto a cualquier subconjunto de su dominio es un buen orden estricto. Por lo tanto, β está estrictamente bien ordenado por $\in$. Para mostrar que β es conjunto transitivo, asumamos $\gamma \in \beta$ y $\delta \in \gamma$. Se necesita probar que $\delta \in \beta$. Por la transitividad de α, ambos $\gamma, \delta \in \alpha$. Más aún, como α está estrictamente bien ordenado por $\in$, se cumple la ley de tricotomía:

$$\delta \in \beta \vee \beta \in \delta \vee \beta = \gamma,$$

de los cuales, los últimos dos casos son imposibles. Así pues, $\beta \in \text{ON}$ y se concluye lo deseado. □

1.11 Definición. Sea X un conjunto no vacio. Sea $x \in X$ y $Y \subseteq X$. Asumimos que W es una relación bien fundada en X. El conjunto $\{z \in X | \langle z, x \rangle \in W \wedge z \neq x\}$ es llamada segmento inicial de $\langle X, W \rangle$ determinado por x, y denotado por $I_W(x)$. Decimos que x es W-minimal para Y si

$$x \in Y \wedge I_W(x) \cap Y = \varnothing.$$

Si x es W-minimal para x, entonces decimos que x es W-minimal.

1.12 Corolario. *Cada segmento inicial de un ordinal es un ordinal.*

Demostración. Sea $\alpha \in \text{ON}$ y sea $I \subseteq \alpha$ un segmento inicial del buen orden estricto $\langle \alpha, \in \rangle$. Si $I = \alpha$, entonces no hay nada que probar. Si I es un segmento inicial propio de $\langle \alpha, \in \rangle$, entonces $I = I_{\in}(\zeta)$ para algún $\zeta \in \alpha$. Pero como el buen orden estricto es $\in$, tenemos que

$$I_{\in}(\zeta) = \{\beta \in \alpha | \beta \in \zeta\}.$$

Por transitividad de α, el último conjunto es igual a

$$\{\beta | \beta \in \zeta\} = \zeta.$$

Como $\zeta \in \alpha$, del lema anterior tenemos que $\zeta \in \text{ON}$ □

1.13 Definición. Sea $\langle X, \preceq \rangle$ un orden parcial. Un subconjunto $I \subseteq X$ es llamado un segmento inicial de $\langle X, \preceq \rangle$ si

$$(\forall y \in I)(\forall x \in X)(x \preceq y \Longrightarrow x \in I).$$

Si Y es cualquier subconjunto de X, entonces se denota el conjunto

$$\text{DC}(Y) = \{x \in X | (\exists y \in Y)(x \preceq y)\}$$

el cuál es llamado la cerradura inferior de Y o el segmento inicial de $\langle X \preceq \rangle$ generado por Y.

En *teoría de conjuntos*, se demuestra el hecho presentado a continuación.

1.14 Proposición. *Si $\langle X, \preceq \rangle$ es un buen orden y Y es un segmento inicial de X, entonces*

$$I(Y) = X \vee DC(Y) = T_{\preceq}(x_o),$$

donde x_o es el elemento mínimo de $X \backslash DC(Y)$.

1.15 Lema.

$$(\forall \alpha, \beta \in ON)(\alpha \in \beta \vee \beta \in \alpha \vee \alpha = \beta)$$

Demostración. Sea $\alpha, \beta \in \text{ON}$. Por *teoría de conjuntos*, sabemos que $\langle \alpha, \in \rangle$ es isomorfo (bajo orden) a un segmento inicial de $\langle \beta, \in \rangle$, o $\langle \beta, \in \rangle$ es isomorfo a un segmento inicial de $\langle \alpha, \in \rangle$. Sin perdida de generalidad, asumimos lo primero y sea $F : \alpha \longrightarrow \beta$ una función inyectiva que mapea α a un segmento inicial I de β tal que

$$(\forall \xi, \eta \in \alpha)(\xi \in \eta \Longleftrightarrow F(\xi) \in F(\eta)) \qquad (*)$$

Por el corolario anterior, $\text{rng}(F)$ es un ordinal. En particular, el rango de F es un conjunto transitivo. Se tiene que (*) es la misma condición que (M) para la función colapsante de $\langle \alpha, \in \rangle$. Por lo tanto, $\text{rng}(F)$ es el colapso de Mostowski de $\langle \alpha, \in \rangle$. Por el teorema 3, $\text{rng}(F) = \alpha$. Si F es sobreyectiva, entonces $\alpha = \text{rng}(F) = \beta$. En caso contrario, $\alpha = \text{rng}(F) = I_{\in}(\zeta) = \zeta$, para algún $\zeta \in \beta$. En otras palabras, $\alpha \in \beta$. □

1.16 Corolario. *La clase relacional $\in \cap (ON \times ON)$ bien ordena estrictamente ON.*

Demostración. Por simplicidad, escribiremos *in* en lugar de $in \cap \text{ON} \times \text{ON}$. Procederemos explicado dos casos:

- Cualquier conjunto (no vacio) de ON tiene elemento mínimo: Sea X un conjunto (no vacio) cuyos elementos son ordinales. Denotamos:

$$\alpha := \bigcap X.$$

Por demostrar $(\alpha \in X) \wedge (\forall \beta \in X)(\alpha \in \beta \vee \alpha = \beta)$: Lo segundo es inmediato ya que, por como se definió α,

$$(\forall \beta \in X)(\alpha \subseteq \beta).$$

Luego, por el lema anterior, si $\beta \in \alpha$, tenemos que

$$\beta \in \beta,$$

lo cuál es absurdo. Luego, tenemos que

$$\alpha \in \beta \vee \alpha = \beta.$$

Por otro lado, consideremos que α no es elemento de X; por lo anteriormente mostrado, dado cualquier β elemento de X, tenemos que $\alpha \in \beta$, luego, como está en todos, está en la intersección:

$$\alpha \in \bigcap_{\beta \in X} \beta = \bigcap X = \alpha.$$

Como α es conjunto, esto es una contradicción, luego $\alpha \in X$. Así, α como fue definido es nuestro primer elemento bajo la relación $\in$.

- Cualquier clase (no vacia) de ON tiene elemento mínimo: Consideremos la clase (no vacia) $\mathcal{X}$ definida por la formula (de teoría de conjuntos) $\varphi(x)$ y cuyos elementos son todos ordinales. Tomemos α tal que $\varphi(\alpha)$ (es decir, α pertenece a la clase $\mathcal{X}$). Tenemos dos casos:

$$(\forall \beta \in \alpha)(\neg\varphi(\beta)),$$

es decir, β no es miembro de la clase $\mathcal{X}$, entonces no hay nada que demostrar y α es elemento mínimo de $\mathcal{X}$. Si, por otro lado,

$$X = \{\beta \in \alpha | \varphi(\beta)\} \neq \varnothing,$$

tenemos que X es conjunto (dado que α lo es) y, por el punto anterior, este posee elemento mínimo, que será el elemento mínimo de todo $\mathcal{X}$.

□

1.17 Definición. Se define la relación $<$ sobre ON como sigue:

$$\alpha < \beta \iff \alpha \in \beta.$$

Teniendo en cuenta resultadoa anteriores, se tiene de inmediato lo siguiente:

$$\alpha \leqslant \beta \iff \alpha \text{ es segmento inicial de } \beta.$$

1.18 Proposición. *Sean $\alpha, \beta \in ON$. Entonces*

$$\alpha \leqslant \beta \iff \alpha \subseteq \beta.$$

Demostración. Sean $\alpha, \beta \in \text{ON}$. Por un lema anterior, $(\forall \xi \in \text{ON})(\xi \subseteq \text{ON})$, entonces denotamos:

$$\alpha = \{\gamma \in \text{ON} | \gamma < \alpha\} \wedge \beta = \{\gamma \in \text{ON} | \gamma < \beta\}.$$

Es evidente que

$$\alpha \leqslant \beta \Longrightarrow \alpha \subseteq \beta.$$

Asumiendo entonces $\alpha \subseteq \beta$:

- Si $\alpha = \beta$, no hay nada que probar.
- Si $\alpha \neq \beta$, y tomamos $\gamma \in \beta \backslash \alpha$; como $\beta \notin \alpha$, tenemos que

$$\alpha = \gamma \lesssim \alpha \in \gamma \in \beta.$$

  Como β es transitivo, en ambos casos $\alpha \leqslant \beta$.

□

Supongamos que $\langle X, \preceq \rangle$ es un buen orden, y asumimos $y \notin X$. Por *teoría de conjuntos*, si $Y = X \cup \{y\}$ y $\preceq_Y = \preceq \cup \{\langle x, y \rangle | x \in Y\}$, entonces $\langle Y, \preceq_Y \rangle$ está también bien ordenado.

1.19 Proposición.

$$\alpha = \text{ot}(\langle X, \preceq \rangle) \Longrightarrow S(\alpha) = \text{ot}(\langle Y, \preceq_Y \rangle).$$

La propiedad anterior muestra que, para cualquier ordinal α, su sucesor $S(\alpha)$ también es un ordinal. Más aún, como $S(\alpha) = \alpha \cup \{\alpha\}$, tenemos que $\alpha \in S(\alpha)$, y si $\beta \in S(\alpha)$, entonces $\beta \in \alpha \lesssim \beta = \alpha$. Por lo tanto, $S(\alpha)$ es el más pequeño ordinal, mayor que α; por lo que $S(\alpha)$ es el sucesor inmediato de α en ON.
El conjunto vacio es un ordinal. Esto se ve de que $\varnothing$ satisface la defínción, o porque $\varnothing$ es el colapso de Mostowski de $\langle \varnothing, \varnothing \rangle$. Más aún, como $\varnothing$ no contiene elementos, este debería ser el ordinal más pequeño. Los siguientes ordinales son $S(\varnothing), S(S(\varnothing)), \ldots$, etcetera. En la teoria de conjuntos, se denota al $n-$ésimo sucesor de $\varnothing$ por $\tilde{n}$ y se identifica por el número natural n. Entonces, ahora vemos que cada $\tilde{n}$ es un ordinal; más aún, la relación $<$ restringida a los ordinales $\tilde{n}$ restringida a los ordinales $\tilde{n}$ es el orden estricto usual de los números naturales, y $\tilde{n} = \text{ot}(\langle \{0, 1, \ldots, n-1\}, < \rangle)$. Así, los números naturales son los ordinales finitos.

1.20 Proposición. *Muestre que un ordinal α es un conjunto finito si, y sólo si es un número natural.*

Observemos que el más pequeño de los ordinales infinitos es el conjunto ω de todos los números naturales (pues no hay números naturales que sean infinitos). Así mismo, ω es el colapso de Mostowski de $\langle \omega, < \rangle$.

1.21 Lema. *(ZF): ω es el más pequeño ordinal α tal que*

1. $\alpha \neq 0$.
2. $(\forall \beta \in \alpha)(S(\beta) \in \alpha)$.

Demostración. Consideremos que existe un ordinal $\alpha < \omega$, no cero, y tal que

$$(\forall \beta \in \alpha)(S(\beta) \in \alpha).$$

Como $\alpha \in \omega$, entonces α se identifica por un número natural n. Por como se definió α y como $n-1 \in n = \alpha$, entonces $S(n-1) \in \alpha = n$, luego $n \in n$, lo cuál es absurdo. □

1.22 Teorema. *Sea A un conjunto de ordinales, entonces:*

1. $\bigcup A \in ON$
2. $(\forall \alpha \in A)(\exists \beta \in A)(\alpha < \beta) \implies (\bigcup A$ *es el más pequeño ordinal mayor a cada elemento de* $A)$

Demostración. Tomamos A un conjunto de ordinales:

1. Inmediato (del hecho de que $\in$ bien ordena los ordinales, y que en ON se cumple la tricotomía).
2. Sea A un conjunto de ordinales y sea $\delta = \bigcup A$. Entonces,

$$\delta = \{\alpha | (\exists \beta \in A)(\alpha \in \beta)\}.$$

Asumiendo que para cada $\alpha \in A$, existe $\beta \in A$ tal que $\alpha < \beta$, esto implica que $\alpha \in \delta$, para cada $\alpha \in A$. Por otro lado, si $\alpha \in \delta$, entonces $\alpha \in \beta$ para algún $\beta \in A$. Por lo tanto, no hay ordinales más pequeños que δ que contenga todos los elementos de A.

□

Si se satisface la hipótesis del segundo inciso en el teorema anterior, es decir, si

$$(\forall \alpha \in A)(\exists \beta \in A)(\alpha < \beta), \tag{H}$$

entonces escribiremos $\sup(A)$ en lugar de $\bigcup A$. Si $A = \{\alpha_\beta | \beta < \gamma\}$ y $\alpha_\beta \leqslant \alpha_{\beta'}$ para cada $\beta < \beta' < \gamma$, entonces se escribe con frecuencia

$$\lim_{\beta \to \gamma} \alpha_\beta$$

en lugar de $\sup\{\alpha_\beta | \beta < \gamma\}$.

1.23 Corolario. *ON es una clase propia*

Demostración. Primero, notemos que no existe un ordinal mayor a todos, pues si α es cualquier ordinal, entonces $S(\alpha)$ es un ordinal mayor. Ahora, supongamos que ON es un conjunto; como ON no tiene elemento máximo, (H) se satisface. Pero entonces, $\bigcup$ON es un ordinal que es mayor a cualquier otro ordinal, lo cuál es contradictorio. □

1.24 Definición. Una clase $X \subseteq$ ON se dice *cofinal* en ON si

$$(\forall \alpha \in \text{ON})(\exists \beta \in X)(\alpha \leqslant \beta).$$

Un ordinal α es llamado *ordinal sucesor* si existe un ordinal β tal que $\alpha = S(\beta)$. Un ordinal el cual no es sucesor es llamado *ordinal límite*. Denotatemos la clase de ordinales sucesores por SUCC y la clase de ordinales limite por LIM.

Observemos que los números naturales son ordinales sucesores (empezando por el 1), mientras que 0 y ω son ordinales límite. Por otro lado, si $\alpha \in \mathrm{ON}$, entonces $\alpha < S(\alpha) \in \mathrm{SUCC}$, por lo que $SUCC$ es cofinal en ON. Por otro lado, LIM es cofinal en ON.

1.25 Proposición. *Si un conjunto de ordinales A satisface* (H)*, entonces $\bigcup A$ es un ordinal límite.*

1.26 Teorema. *Cada subclase cofinal de ON es propia. En particular, SUCC y LIM son ambas clases propias.*

Los siguientes resultados muestran la relación entre los ordinales y los buenos ordenes, entre otros conceptos asociados.

1.27 Definición. Sea Z un conjunto arbitrario, sea W una relación bien fundada sobre Z, y sea $\langle X, \prec \rangle$ un buen orden estricto. Una función $\mathrm{rk} : Z \longrightarrow X$ es llamada una función rango para W con respecto a $\prec$ si

$$(\forall z \in Z)(\mathrm{rk}(z) = \sup^{+} \mathrm{rng}(\mathrm{rk}|I(z))).$$

1.28 Proposición.

1. *Sea W una relación bien fundada sobre un conjunto Z, $\langle X, \prec \rangle$ un buen orden estricto, y $rk : Z \longrightarrow X$ una función rango para W con respecto a $\prec$. Sea $\alpha = \mathrm{ot}(\langle X, \prec \rangle)$, y sea $F : X \longrightarrow \alpha$ el isomorfismo de orden entre $\langle X, \prec \rangle$ y $\langle \alpha, \in \rangle$. Muestre que la composición $F \circ rk : Z \longrightarrow \alpha$ es una función rango para W con respecto a $\in$.*

2. *Para cada relación bien fundada, existe una única función rango con respecto a $\in$ cuyo rango es un ordinal.*

1.29 Definición. R es una relación bien fundada en X si es una relación y

$$(\forall Y \subseteq X)(\exists y \in Y)(\nexists r \in Y)(rRy).$$

1.30 Proposición. *Sea x cualquier conjunto. Cada función de x en un ordinal α es la función rango de una relación estrictamente bien fundada en x.*

Demostración. Sea x un conjunto, sea $\alpha \in \mathrm{ON}$ y sea $f : x \longrightarrow \alpha$ una función. Definimos la relación R_f sobre x como

$$R_f = \{\langle y, z \rangle | f(y) < f(z)\}.$$

Mostremos que R_f está estrictamente bien fundada: en caso contrario, existe una sucesión $\langle y_n \rangle_{n \in \omega}$ de elementos de x tales que $\langle y_{n+1}, y_n \rangle \in R_f$ para toda $n \in \omega$. Por definición de R_f, esto significa que $f(y_{n+1}) \in f(y_n)$, para toda $n \in \omega$, lo cual es imposible, por el axioma de fundación. □

1.31 Teorema. *(ZF): Para cada conjunto x, existe un ordinal $\alpha > 0$ tal que x no puede mapearse en α.*

Demostración. Se sigue de la proposición anterior. □

1.32 Proposición. *Existe una formula $\Psi(r, \alpha)$ de L_s con dos variables libres tal que $\Psi(r, \alpha)$ es valida si, y sólo si r es una relación de buen oriden estricto en x y α es el rango de la función rango para r.*

1.33 Corolario. *Para cada conjunto x, existe un ordinal α tal que α no puede ser mapeado en x por una función inyectiva.*

Demostración. Si $x = \varnothing$, ningún ordinal $\beta > 0$ puede mapearse en x. Si $x \neq \varnothing$, sea $\alpha > 0$ un ordinal tal que x no puede ser mapeado en α. Luego α no puede mapearse en x por una función inyectiva. □

1.34 Lema. *(ZF) Si cada conjunto no vacio admite estructura de grupo, entonces cada conjunto puede ser bien ordenado.*

Demostración. Asumimos que cada conjunto admite estructura de grupo, y sea x cualquier conjunto. Sea $\alpha > 0$ un ordinal tal que no hay una inyección de α en x. Consideremos el conjunto $y = x \cup \alpha$. Como $\alpha > 0$, por hipótesis y admite estructura de grupo, es decir, tenemos $e \in y$ y una operación $* : y \times y \longrightarrow y$ con la cuál $\langle y, *, e\rangle$ es un grupo. Fijamos $e, *$. Afirmamos

$$(\forall z \in x)(\exists \beta \in \alpha)(z * \beta \in \alpha).$$

En efecto, fijamos $z \in x$ y consideremos la función $f : \alpha \longrightarrow y$ dada por la formula $f(\beta) = z * \beta$. Como $z^{-1} * f(\beta) = \beta$, para cada $\beta \in \alpha$, la función f es intectiva. Por la elección de α, el rango de f no está contenido en x. Pero, si $f(\beta) \in y\backslash x$, entonces $f(\beta) \in \alpha$, lo que prueba la proposición. Ahora, sea $\preceq_a$ la orden antilexicográfica sobre $\alpha \times \alpha$. Ahora, claro que $\preceq_a$ es una relación de buen orden. Definimos una función $g : x \longrightarrow \alpha \times \alpha$ siendo $g(z)$ el $\preceq_a$-elemento mínimal $\langle \beta, \gamma\rangle$ de $\alpha \times \alpha$ tal que $z * \beta = \gamma$. Notemos que si $g(z) = \langle \beta, \gamma\rangle$, entonces $z = \gamma * \beta^{-1}$. Así, g es una función inyectiva. Luego, definimos la relación $\preceq$ sobre x por:

$$z \preceq z' \Longleftrightarrow g(z) \preceq_a g(z').$$

Ahora, $\preceq$ es una relación de buen orden sobre x. Esto prueba el teorema. □

1.35 Teorema. *(Principio de inducción sobre un conjunto bien fundado)*
Sea X un conjunto no vacio, sea $Y \subseteq X$ y sea W una relación bien fundada sobre X. Si la implicación

$$I_W(x) \subseteq Y \Longrightarrow x \in Y, \tag{Ind}$$

es valida para cada $x \in X$, entonces $X = Y$.

Demostración. Sea X, Y y W como en el enunciado y asumimos que (Ind) es valida para cada $x \in X$. Supongamos $C = X\backslash Y \neq \varnothing$. Por la bien fundación de W, existe un elemento $W-$mínimal de C. Pero, si x_o es un elemento $W-$mínimal de C, entonces $I_W(x_o) \subseteq Y$, y de (Ind) (considerada con x_o) se sigue que $x_o \in Y$, lo cuál es imposible, pues $x_o \in X\backslash Y$, lo cuál es una contradicción. □

1.36 Teorema. *(Principio de Definición Recursiva Generalizado)*
Sean $X, Z \neq \varnothing$, y sea W una relación bien fundada sobre Z. Además, suponganse que G es una función con valores en X tal que $dom(G)$ consiste de todos los pares de la forma $\langle f, z\rangle$, donde $z \in Z$ y f es una función que mapea $I_W(z)$ en X. Entonces, existe exactamente una función $F : Z \longrightarrow X$ tal que

$$(\forall z \in Z)(F(z) = G(F|I_W(z), z)) \tag{R}$$

1.37 Teorema. *(Principio de Construcción Recursiva Generalizado)*
Sean $X, Z \neq \varnothing$, y sea W una relación bien fundada sobre Z. Además, suponganse que G^* es una función con valores en $\mathscr{P}(X)\backslash\{\varnothing\}$ tal que $dom(G^*)$ consiste de todos los pares de

la forma $\langle f, z\rangle$*, donde* $z \in Z$ *y* f *es una función que mapea* $I_W(z)$ *en* X*. Entonces, existe una función* $F : Z \longrightarrow X$ *tal que*

$$(\forall z \in Z)(F(z) \in G^*(F|I_W(z), z)) \tag{R*}$$

Consideremos un ordinal arbitrario α. Como $\in$ es una relación bien fundada sobre α, son validos los teoremas anteriores. La inducción y recursión sobre $\in$ en ordinales son comúnmente referenciadas como **inducción transfinita** y **recursión transfinita**.

1.38 Teorema. *(ZF) Sea* X *un conjunto, sea* C *una familia de subconjuntos de* X *que es cerrado bajo uniones de subfamilias que son inealmente ordenados por inclusión, y sea* $f : C \longrightarrow C$ *una función con*

$$(\forall c \in C)(c \subseteq f(c)).$$

Entonces, existe un $c_o \in C$ *tal que* $f(c_o) = c_o$*.*

Demostración. Sea X, C y f como en la hipótesis, y sea $\alpha > 0$ un ordinal que no puede mapearse en C por una función inyectiva. Definimos por recursión transfinita una función $F : \alpha \longrightarrow \mathscr{P}(X)$ como sigue:
Supongamos $\beta \in \alpha$ y $F(\gamma)$ está definida para toda $\gamma < \beta$. Definimos:

$$F(\beta) = \begin{cases} f\left(\bigcup \{F(\gamma)|\gamma < \beta\}\right) & \text{si } \bigcup \{F(\gamma)|\gamma < \beta\} \in C, \\ X & \text{en cualquier otro caso.} \end{cases}$$

Afirmamos que

$$(\forall \gamma < \beta < \alpha)(F(\gamma) \subseteq F(\beta)). \tag{P}$$

En efecto, sea $\gamma < \beta < \alpha$. Si $F(\beta) = X$, entonces la inclusión $F(\gamma) \subseteq F(\beta)$ se sigue del hecho de que $F(\gamma) \in \mathscr{P}(X)$. Si $F(\beta) \neq X$, entonces $\bigcup \{F(\delta)|\delta < \beta\} \in C$, y por como asumimos f, tenemos

$$F(\gamma) \subseteq \bigcup \{F(\delta)|\delta < \beta\} \subseteq f\left(\bigcup \{F(\delta)|\delta < \beta\}\right) = F(\beta).$$

Por otro lado, afirmamos

$$(\forall \beta \in \alpha)(F(\beta) \in C). \tag{Q}$$

En efecto, por inducción sobre β: sea $\beta < \alpha$, y supongase $F(\gamma) \in C$, para cada $\gamma < \beta$. Consideramos $\mathcal{F} = \{F(\gamma)|\gamma < \beta\}$. Por hipótesis de inducción, $\mathcal{F} \subseteq C$. La proposición (P) muestra que $\mathcal{F}$ está linealmente ordenado por inclusión. Así, la hipótesis sobre C implica que $\bigcup \mathcal{F} \in C$. Como el rango de f está contenido en C, se tiene $F(\beta) = f\left(\bigcup \mathcal{F}\right) \in C$. Así, continuando con la Demostración principal, de (Q), F mapea α en C. Por la elección de α, existen $\gamma < \beta < \alpha$ tal que $F(\gamma) = F(\beta)$. Fijamos γ, β. Si $F(\beta) = X$, entonces $X \in C$, y $f(X) = X$ por la hipótesis sobre f, por lo que en ese caso $C = X$ atestigua que el teorema se cumple. Si $F(\beta) \neq X$, entonces sea $c_o = \bigcup \{F(\delta)|\delta < \beta\}$. La definición de F implica que $c_o \in C$. Más aún,

$$F(\beta) = F(\gamma) \subseteq \bigcup \{F(\delta)|\delta < \beta\} \subseteq f\left(\bigcup \{F(\delta)|\delta < \beta\}\right) = F(\beta).$$

Se sigue que $f(c_o) = c_o$, lo que prueba el teorema. □

1.2. Aritmética ordinal

Continuando con la sección anterior, se dará a continuación una estructura aritmética sobre los ordinales, que nos permitirá operar con ellos como con cualquier otro conjunto de números, teniendo en cuenta unas cuantas excepciones a lo que comúnmente se hace al operar con otros conjuntos. [1]

1.39 Definición. Sea $\alpha \in \text{ON}$. Por recursión sobre $\beta \in \text{ON}$, definimos un ordinal $\alpha + \beta$ como:

- $\alpha + 0 = \alpha$;
- $\alpha + \beta = S(\alpha + \gamma)$, si $\beta = S(\gamma)$;
- $\alpha + \beta = \bigcup_{\gamma \in \beta}(\alpha + \gamma)$, si β es un ordinal límite mayor a cero.

1.40 Lema. *Sea $\alpha, \beta \in ON$. Entonces,*

$$\alpha + \beta = \alpha \cup \{\alpha + \gamma | \gamma < \beta\} \tag{1}$$

Demostración. Procedemos por inducción sobre β:

- Si $\beta = 0$ entonces lo de la derecha de (1) es $\alpha \cup \varnothing = \alpha$. Lo de la izquierda es $\alpha + 0$, lo cual es igual a α por defínción.
- Asumiendo la ecuación (1) valida para γ y $\beta = S(\gamma)$. Entonces,

$$\alpha \cup \{\alpha + \delta | \delta < \beta\} = \alpha \cup \{\alpha + \delta | \delta < \gamma\} \cup \{\alpha + \gamma\} \text{ (y por hipótesis inductiva)}$$

$$= \alpha + \gamma \cup \{\alpha + \gamma\} = S(\alpha + \delta) \text{ (y por la definición 1.39)}$$

$$= \alpha + \beta.$$

- Ahora, asumimos que β es un ordinal límite y que (1) es valida para cada $\gamma < \beta$. Entonces, para cada $\delta < \beta$ existe una γ tal que $\delta < \gamma < \beta$, y también:

$$\alpha \cup \{\alpha + \delta | \delta < \beta\} = \alpha \cup \bigcup_{\gamma < \beta} \{\alpha + \delta | \delta < \gamma\}$$

$$= \bigcup_{\gamma < \beta} (\alpha \cup \{\alpha + \delta | \delta < \gamma\}) \text{ (y por hipótesis de inducción)}$$

$$= \bigcup_{\gamma < \beta} (\alpha + \gamma) \text{ (y por la definición 1.39)}$$

$$= \alpha + \beta.$$

□

1.41 Corolario. *Supongase que $\alpha, \beta, \gamma, \delta$ son ordinales tales que $\gamma < \beta$. Entonces,*

$$\alpha \leqslant \alpha + \gamma < \alpha + \beta.$$

1.42 Corolario. *Sean $\alpha, \beta \in ON$ tales que $\alpha < \beta$. Entonces, existe exactamente un ordinal γ_o tal que $\alpha + \gamma_o = \beta$.*

Demostración. Fijamos α, β como en la hipótesis, y sea $F_\alpha(\gamma) = \alpha + \gamma$. Se sigue del corolario 1.41 que F_α es una clase funcional inyectiva. Por el corolario 1.33, existe un ordinal δ tal que $F_\alpha(\delta) \notin \beta$. Fijamos pues a δ. Como $F_\alpha(\delta) = \alpha + \delta \in \text{ON}$, por el lema 1.15, tenemos que $\alpha + \delta = \beta$, o $\beta \in \alpha + \delta$. En el primer caso, $\gamma_o = \beta$ es lo requerido. En el segundo, por el lema 1.40, $\beta \in \{\alpha + \gamma | \gamma < \delta\}$, lo cuál nuevamente produce el resultado deseado. □

1.43 Definición. Sea $\langle A, \leq_A \rangle$ y $\langle B, \leq_B \rangle$ órdenes parciales. El orden suma $\langle A, \leq_A \rangle \oplus \langle B, \leq_B \rangle$ es el orden parcial $\langle C, \leq \rangle$, donde

$$C = A \times \{0\} \cup B \times \{1\},$$

y la relación $\leq$ está dada por

$$\langle a, b \rangle \leq \langle c, d \rangle \iff \begin{cases} b = 0 \wedge d = 1 \text{ ó} \\ b = d = 0 \wedge a \leq_A c \text{ ó} \\ b = d = 1 \wedge a \leq_B c \end{cases}$$

1.44 Teorema. *Sean $\langle X, \leq_X \rangle$ y $\langle Y, \leq_Y \rangle$ buenos ordenes, y sea $\alpha = \text{ot}(\langle X, \leq_X \rangle)$, $\beta = \text{ot}(\langle Y, \leq_Y \rangle)$. Entonces, $\alpha + \beta = \text{ot}(\langle X, \leq_X \rangle \oplus \langle Y, \leq_Y \rangle)$.*

Demostración. Sea $f : X \longrightarrow \alpha$ un isomorfismo de orden entre $\langle X, \prec_X \rangle$ y $\langle \alpha, \in \rangle$, y sea $g : Y \longrightarrow \beta$ un isomorfismo de orden entre $\langle Y, \prec_Y \rangle$ y $\langle \beta, \in \rangle$. Definimos una función $h : X \times \{0\} \cup Y \times \{1\} \longrightarrow \alpha + \beta$ por:

$$h(x, 0) = f(x); h(y, 1) = \alpha + g(y).$$

Se sigue del lema 1.40 que el rango de h es $\alpha + \beta$, y el corolario 1.41 implica que h preserva orden. Luego, h es un isomorfismo de orden, y hemos probado el teorema. □

Vale la pena recalcar que la suma de ordinales no es conmutativa. Esto se observa del siguiente hecho:

$$1 + \omega = \omega < S(\omega) = \omega + 1.$$

1.45 Proposición.

$$(\forall \alpha, \beta, \gamma \in ON)(\alpha \leqslant \beta \Longrightarrow \alpha + \gamma \leqslant \beta + \gamma).$$

1.46 Proposición.

$$(\forall \alpha, \beta, \gamma \in ON)((\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)).$$

Demostración. Se sigue del teorema 1.44 y las propiedades de la suma de ordenes. □

1.47 Definición. Sea $\alpha \in \text{ON}$. Por recursión sobre $\beta \in \text{ON}$ definimos un ordinal $\alpha \cdot \beta$ como sigue:

- $\alpha \cdot 0 = 0$;
- $\alpha \cdot \beta = (\alpha \cdot \gamma) + \alpha$, si $\beta = S(\gamma)$;
- $\alpha \cdot \beta = \bigcup_{\gamma \in \beta} (\alpha \cdot \gamma)$, si β es un límite ordinal no cero.

Observemos que

$$2 \cdot \omega = \bigcup_{n \in \omega} (2 \cdot n) = \omega < \omega + \omega = \omega \cdot 2.$$

De aquí se sigue que el producto de ordinales no es conmutativo.

1.48 Lema. *Sea $\alpha, \beta \in ON$. Entonces,*

$$\alpha \cdot \beta = \{\alpha \cdot \xi + \eta | \xi < \beta \wedge \eta < \alpha\} \tag{2}$$

Demostración. Procedemos por inducción sobre β:

- Si $\beta = 0$, entonces

$$\alpha \cdot \beta = \alpha \cdot 0 = 0 = \varnothing = \{\alpha \cdot \xi + \eta | \xi < \beta \wedge \eta < \alpha\}.$$

- Si (2) se mantiene para γ, y si $\beta = S(\gamma)$, entonces

$$\alpha \cdot \beta = \alpha(\gamma + 1) = \alpha \cdot \gamma + \alpha \text{ (por el lema 1.40)}$$

$$= \alpha \cdot \gamma \cup \{\alpha \cdot \gamma + \eta | \eta < \alpha\} \text{ (por hipótesis de inducción)}$$

$$= \{\alpha \cdot \xi + \eta | \xi < \gamma \wedge \eta < \alpha\} \cup \{\alpha \cdot \gamma + \eta | \eta < \alpha\}$$

$$= \{\alpha \cdot \xi + \eta | \xi < \beta \wedge \eta < \alpha\}.$$

- Si (2) se mantiene para cada $\gamma < \beta$, con β un ordinal límite:

$$\alpha \cdot \beta = \bigcup_{\gamma \in \beta} (\alpha \cdot \gamma) \text{ (por hipótesis de inducción)}$$

$$= \bigcup_{\gamma \in \beta} \{\alpha \cdot \xi + \eta | \xi < \gamma \wedge \eta < \alpha\}$$

$$= \{\alpha \cdot \xi + \eta | \xi < \beta \wedge \eta < \alpha\}.$$

□

1.49 Corolario. *Sean $\alpha, \beta, \gamma \in ON$ tales que $\alpha > 0$ y $\beta < \gamma$. Entonces, $\alpha \cdot \beta < \alpha \cdot \gamma$.*

1.50 Corolario. *(Algoritmo de la división)*
Supongase $\alpha, \beta \in ON$ tales que $1 \leqslant \alpha < \beta$. Entonces, existe un único par de ordinales $\langle \xi, \eta \rangle$ tales que

$$\eta < \alpha \wedge \beta = \alpha \cdot \xi + \eta \tag{3}$$

Demostración. Sean α, β como en la hipótesis. La existencia de ξ y de η como en (3) se sigue del lema 1.48. Para mostrar la unicidad, suponemos:

$$\alpha \cdot \xi + \eta = \alpha\xi' + \eta' \wedge \eta, \eta' < \alpha \tag{4}$$

I Supongamos $\xi = \xi'$. Entonces, $\alpha \cdot \xi = \alpha \cdot \xi'$, y se sigue del corolario 1.41 que $\eta = \eta'$.

II Supongamos $\xi \neq \xi'$. Sin perdida de generalidad, $\xi < \xi'$. Entonces, $\xi + 1 \leqslant \xi'$, y $\alpha \cdot \xi + \eta < \alpha\xi + \alpha = \alpha \cdot (\xi + 1) \leqslant \alpha\xi' \leqslant \alpha \cdot \xi' + \eta'$, lo cuál contradice (4).

□

1.51 Teorema. *Sea* $\langle X, \preceq_X \rangle$ *y* $\langle Y, \preceq_Y \rangle$ *un buen orden, y sea* $\alpha = \mathrm{ot}(\langle X, \preceq_X \rangle)$, $\beta = \mathrm{ot}(\langle Y, \preceq_Y \rangle)$. *Entonces,*

$$\alpha \cdot \beta = \mathrm{ot}(\langle X, \preceq_X \rangle \otimes^a \langle Y, \preceq_Y \rangle),$$

con $\otimes^a$ *el producto antilexicográfico.*

1.52 Corolario. *Sea* $\alpha, \beta, \gamma \in ON$. *Entonces,*

- $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$
- $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$

1.53 Definición. Sea $\alpha \in \mathrm{ON}$. Por recursión sobre β, definimos un ordinal α^β como sigue:

- $\alpha^0 = 1$;
- $\alpha^\beta = \alpha^\gamma \cdot \alpha$, si $\beta = \gamma + 1$;
- $\alpha^\beta = \bigcup_{\gamma<\beta} \alpha^\gamma$, si β es un ordinal límite mayor a cero.

A continuación presentaremos un ordinal importante:

1.54 Definición. Consideremos la siguiente notación:

$$\omega_0 = \omega \wedge \omega_{n+1} = \omega^{\omega_n}.$$

Luego, definimos el siguiente ordinal:

$$\varepsilon_0 = \bigcup_{n\in\omega} \omega_n.$$

Así mismo, cabe señalar que ε_0 es un conjunto numerable.

1.55 Ejemplo. Consideremos los ordinales 2,3 y $1 \leqslant \omega$, entonces

$$2^\omega = 3^\omega.$$

1.56 Proposición. *Sean* $\alpha, \beta, \gamma \in ON$. *Entonces,*

- $(1 < \alpha \wedge \beta < \gamma) \Longrightarrow \alpha^\beta < \alpha^\gamma$;
- $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$;
- $\alpha^{\beta\cdot\gamma} = (\alpha^\beta)^\gamma$.

1.3. Ultrafiltros

A continuación presentaremos algunos resultados importantes sobre las estructuras conocidas como ultrafiltros, los cuales serán muy importantes en el desarrollo de capítulos posteriores.[2]

1.57 Definición. Sea X un conjunto. Un ultrafiltro sobre X es una familia $u \in \mathscr{P}(X)$ que satisface para cada $A, B \in \mathscr{P}(X)$:

- $A \cap B \in u \Longleftrightarrow (A \in u \wedge B \in u)$

- $A \cup B \in u \iff (A \in u \vee B \in u)$
- $A \in u \iff X \backslash A \notin u$

1.58 Observación. *Dado que toda conectiva lógica se puede poner en terminos de el trazo de Sheffer, podemos encontrar una equivalencia con la definición de ultrafiltro, como una familia que satisface que, para cada $A, B \in \mathscr{P}(X)$,*

$$X \backslash (A \cap B) \in u \iff \textit{no ambos } A \in u \wedge B \in u.$$

Una cosa que es buena tener en cuenta es que no existen ultrafiltros sobre $\varnothing$.

1.59 Proposición. *Cada ultrafiltro es cerrado por arriba. Esto es, si X es un conjunto y u es un ultrafiltro sobre X, entonces*

$$(A \in u \wedge A \subseteq B \subseteq X) \Longrightarrow B \in u.$$

En particular, $X \in u$.

Demostración. Supongase que $A \in u$ y $A \subseteq B \subseteq X$. Como $A \in u$, tenemos que $A \in u$ o $B \in u$. Entonces, por 1.57, tenemos que $B = A \cup B \in u$. □

1.60 Proposición. *Sea X un conjunto y sea u un ultrafiltro sobre X. Si $A \in u$ y $A = A_1 \cup \cdots \cup A_n$, entonces existe un indice $i \in [\![1, n]\!]$ tal que $A_i \in u$; más aún, si todos los A_j son disjuntos a pares, entonces i es único. En particular, para cada partición finita de X, sólo un elemento de dicha partición pertenece a u.*

Demostración. La primera parte de la proposición es por inducción, donde el caso base $n = 2$ se sigue directamente de la definición 1.57. Para la segunda parte, observemos que si los A_j son disjuntos a pares, y tenemos $A_i, A_k \in u$, para $i \neq k$, entonces tenemos también que $\varnothing = A_i \cap A_k \in u$, lo cuál contradice la proposición 1.59. □

1.61 Observación. *Observemos que para cualquier conjunto no vacio X y para cualquier elemento x de este conjunto, la familia $\{A \in \mathscr{P}(X) | x \in A\}$ es un ultrafiltro sobre X. En efecto, pues para $A, B \in \mathscr{P}(X)$:*

$$A \cap B \in u \iff x \in A \cap B \iff (x \in A \wedge x \in B) \iff (A \in u \wedge B \in u)$$

$$A \cup B \in u \iff x \in A \cup B \iff (x \in A \vee x \in B) \iff (A \in u \vee B \in u)$$

$$A \in u \iff x \in A \iff x \notin X \backslash A \iff X \backslash A \notin u$$

1.62 Definición. Sean X un conjunto. Un ultrafiltro u sobre X es llamado **principal** si existe un elemento x de X tal que

$$u_x := \{A \in \mathscr{P}(X) | x \in A\} = u.$$

En otro caso, u es **no principal**.

1.63 Teorema. *Sea X un conjunto y u un ultrafiltro sobre X. Entonces, u es principal si y sólo si existe un conjunto finito $F \in \mathscr{P}(X)$ tal que $F \in u$.*

Demostración. Si u es principal, entonces existe $x \in X$ tal que $u = u_x$. En particular, $\{x\} \in u_x$, lo que demuestra esa implicación. Inversamente, supongamos $F \subseteq X$ es un conjunto finito; digamos $F = \{x_1, \ldots, x_n\}$, tal que $F \in u$. Entonces, $F = \{x_1\} \cup \cdots \{x_n\}$ y por la proposición 1.60, existe un indice $i \in [[1, n]]$ tal que $\{x_i\} \in u$. Así, afirmamos $u = u_{x_1}$. En efecto, sea $A \in u$ y tenemos que $\{x_i\} \in u$, entonces por la definición 1.57, $A \cap \{x_i\} \in u$. Observemos que para $Y \in \mathscr{P}(X)$:

$$Y \cap \{x_i\} = \begin{cases} \{x_i\} & \text{si } x_i \in Y \\ \varnothing & \text{en cualquier otro caso.} \end{cases}$$

Y como $\varnothing \notin u$, se sigue que si $A \in u$, entonces $x_i \in A$, por lo que $u = u_{x_i}$. □

El teorema anterior tiene una consecuencia inmediata, y es que si tenemos un ultrafiltro no principal, todos sus elementos son infinitos. Sin embargo, aún no hemos demostrado o garantizado la existencia de dichos ultrafiltros.

1.64 Definición. Diremos que una familia $\mathcal{F}$ de subconjuntos de X es buena si es no vacía, cerrada bajo intersecciones y $\varnothing \notin \mathcal{F}$.

1.65 Lema. *Sea $\mathcal{M}$ una familia buena maximal. Si un conjunto $A \in \mathscr{P}(X)$ inersecta cada elemento de $\mathcal{M}$, entonces $A \in \mathcal{M}$. En particular, $\mathcal{M}$ es cerrado por arriba.*

Demostración. Como $\{X\} \cup \mathcal{M}$ es también una buena familia que contiene a $\mathcal{M}$, entonces por maximalidad tenemos $\mathcal{M} = \mathcal{M} \cup \{X\}$ y también $X \in \mathcal{M}$. Ahora, supongamos que $A \in \mathscr{P}(X)$ intersecta cada $B \in \mathcal{M}$. Entonces, la familia

$$\{A \cap B | B \in \mathcal{M}\} \cup \mathcal{M}$$

es buena y contiene a $\mathcal{M}$, por lo que, por maximalidad, $\mathcal{M} = \mathcal{M} \cup \{A \cap B | B \in \mathcal{M}\}$ y, en particular (como $X \in \mathcal{M}$), $A = A \cap X \in \mathcal{M}$. Esto demuestra la primera parte. Para la segunda parte, si $A \in \mathcal{M}$ y $A \subseteq B$, entonces para cada $C \in \mathcal{M}$ tenemos que $A \cap C \subseteq B \cap C$, con ambos siendo elementos de $\mathcal{M}$; y como $\varnothing \notin \mathcal{M}$, tenemos que $B \cap C \neq \varnothing$. Por la primera parte, se sigue que $B \in \mathcal{M}$. □

1.66 Lema. *Una familia de subconjuntos de X es buena maximal si, y sólo si es un ultrafiltro.*

Demostración. Primero demostremos la implicación inversa. Si u es un ultrafiltro, inmediatamente u es una familia buena. Supongamos que $\mathcal{F}$ es otra familia buena con $u \subseteq \mathcal{F}$. Si la inclusión fuera propia, tomando $A \in \mathcal{F} \backslash u$ tendríamos que $X \backslash A \in u \subseteq \mathcal{F}$, y por lo tanto $\varnothing = A \cap (X \backslash A) \in \mathcal{F}$, una contradicción. Luego $u = \mathcal{F}$ y hemos terminado.
Ahora, para la implicación, sea $\mathcal{M}$ una buena familia maximal. Podemos usar la caracterización de ultrafiltros por el trazo de Sheffer, esto es, probaremos que $\mathcal{M}$ es un ultrafiltro mostrando que, para $A, B \in \mathscr{P}(X)$, tenemos $X \backslash (A \cap B) \in \mathcal{M}$ si, y sólo si se cumple que no ambos A y B pertenecen a $\mathcal{M}$. Primero supongamos que $X \backslash (A \cap B) \in \mathcal{M}$; como $\varnothing \notin \mathcal{M}$ y $\mathcal{M}$ es cerrado bajo intersecciones, esto significa que $A \cap B \notin \mathcal{M}$. Por el lema 1.65 esto implica que existe $C \in \mathcal{M}$ que es disjunto a $A \cap B$. Si $A \in \mathcal{M}$, entonces $A \cap C \in \mathcal{M}$ es disjunto a B; como $\mathcal{M}$ es cerrado bajo intersecciones y no contiene a $\varnothing$, tenemos que $B \notin \mathcal{M}$. El caso para $B \in \mathcal{M}$ es completamente análogo, concluyendo que $B \notin \mathcal{M}$; por lo que se ha probado que A y B no pertenecen ambos a $\mathcal{M}$. Inversamente, supongamos que no se cumple que ambos $A \in \mathcal{M}$ y $B \in \mathcal{M}$. Asumimos que $A \notin \mathcal{M}$ (complemtanete análogo si suponemos $B \notin \mathcal{M}$).Por el lema 1.65 hay un C en $\mathcal{M}$ que es disjunto a A, lo cuál implica que $C \subseteq X \backslash A$. Como $X \backslash A \subseteq X \backslash (A \cap B)$ y $\mathcal{M}$ es cerrado por arriba por el lema 1.65, concluimos que $X \backslash (A \cap B) \in \mathcal{M}$, y hemos terminado. □

1.67 Teorema. *Si X es un conjunto infinito, entonces existe un ultrafiltro no principal sobre X.*

Demostración. Dado X, un conjunto, observemos que la familia de los subconjuntos cofinitos de X,

$$\mathscr{P}_{\text{cf}}(X) = \{A \in \mathscr{P}(X) | X \backslash A \text{ es finito}\}$$

es una familia buena. Por lo tanto, por el lema de Zorn, existe un ultrafiltro u con $\mathscr{P}_{\text{cf}}(X) \subseteq u$. Claramente u es no principal, pues en caso contrario existiría un conjunto finito F con $F \in u$ por 1.63, y como $X \backslash F \in \mathscr{P}_{\text{cf}}(X) \subseteq u$, lo que significa que $\varnothing = F \cap (X \backslash F) \in u$, una contradicción. □

1.4. Lógica de primer orden

En el siguiente espacio presentaremos conceptos básicos de lógica, con la intención de usarlos en capítulos siguientes despreocupadamente. Por esta misma razón, lo que siguiente será ya enfocado al lenguaje de la **aritmetica de Peano**. [3]

1.68 Definición. *(Lenguaje)*
El lenguaje de la aritmetica de Peano consta del siguiente alfabeto:
Símbolos lógicos:

- variables: $v_1, \ldots, v_n, \ldots$;
- conectivas lógicas: $\neg, \Longrightarrow, \wedge, \vee$;
- cuantificadores: $\forall, \exists$;
- igualdad: $=$.

Símbolos no lógicos:

- símbolo de constante: $\mathfrak{o}$;
- símbolos de funciones: $+, \cdot, S$;
- símbolo de relación: $<$

y se denota por:

$$\mathcal{L}_{PA} = \{\mathfrak{o}, +, \cdot, S, <\}\,.$$

1.69 Definición. Un término de $\mathcal{L}_{PA}$ es una sucesión finita de símbolos del alfabeto de $\mathcal{L}_{AP}$ que proviene de las cláusuras siguientes:

1. Para cada n, v_n es un término;
2. $\mathfrak{o}$ es un término;
3. si t_1 y t_2 son términos, entonces $t_1 + t_2$, $t_1 \cdot t_2$ y St_1 son todos términos.

1.70 Definición. Una fórmula es una sucesión fínita de símbolos de alfabeto de $\mathcal{L}_{AP}$, que proviene de alguna de las siguientes cláusuras:

1. Si t_1 y t_2 son términos, entonces $t_1 = t_2$ es una fórmula;

2. si t_1 y t_2 son términos, entonces $t_1 < t_2$ es una fórmula;

3. si φ es fórmula, $\neg\varphi$ es también fórmula;

4. si φ y ψ son fórmulas, $\varphi \Longrightarrow \psi$ es también fórmula;

5. si φ es una fórmula y v_i es una variable, $\forall v_i \varphi$ también lo es.

1.71 Definición. Diremos que una generalización para la formula φ es cualquier fórmula de la forma $\forall x\varphi$, con x una variable.

1.72 Observación. *Consideremos el conjunto de las variables de nuestro lenguaje, el cuál denotaremos por var, el conjunto de términos de nuestro lenguaje, el cuál denotaremos por Term, el conjunto de tuplas con entradas $\{0,1\} \cup var$, denotado por tup, y consideremos la operación de concatenación de tuplas (es decir, pegar tuplas y volverlas una más grande) mediante el símbolo $\oplus$. Observemos entonces la función:*

$$Fr\text{: } Term \longrightarrow tup$$

Definida por las siguientes reglas:
$Fr(C_k) = \varnothing$ *(es decir, la tupla vacía),*
$Fr(V_k) = (V_k, 1), \qquad Fr(F_k t_1 \cdots t_n) = Fr(t_1) \oplus \cdots \oplus Fr(t_n).$

Esta función simplemente recoge las variables que aparecen en un cierto termino, en orden y con repeticiones, y pone un 1 inmediatamente después de cada una. Ahora, consideremos el conjunto de formulas, al cuál denotaremos por Form. Consideremos la siguiente función:

$$Op\text{:}tup \times var \longrightarrow tup$$

Dada por: $Op((x_\alpha)_{\alpha\in[[1,k]]}, v_i) = (y_\alpha)_{\alpha\in[[1,k]]}$, *donde:*

$$y_\alpha = \begin{cases} 0, x_{\alpha-1} = v_i; \\ x_\alpha, \textit{en otro caso.} \end{cases}$$

Ahora, consideremos la siguiente función:

$$Free\text{:}Form \longrightarrow tup$$

Definida por:

- $Free(t_1 t_2) = Free(t_1) \oplus Free(t_2)$
- $Free(R_k t_1, \ldots, t_n) = Free(t_1) \oplus \cdots \oplus Free(t_n)$
- $Free\ (\neg\varphi) = Free\ (\varphi)$
- $Free\ (\Rightarrow \varphi\psi) = Free(\varphi) \oplus Free(\psi)$
- $Free(\forall V_k \varphi) = Op(Free(\varphi), V_k)$.

El anterior es simplemente un bosquejo, pues una formalización de dichos conceptos requeriría un mayor desarrollo que después no será útil en este trabajo.

1.73 Definición. Sea una variable v_i tal que $v_i = (\text{Free}(\varphi))_j$, para algún $j \in \omega$. Diremos que v_i es libre en φ si $(\text{Free}(\varphi))_{j+1} = 1$. En caso contrario, es decir, $(\text{Free}(\varphi))_{j+1} = 0$, diremos que está ligada en φ.

1.74 Observación. *Denotaremos por $\varphi\,[t/x]$ al resultado de sustituir (en φ) cada aparición libre de x con el termino t.*

1.75 Definición. Diremos que t es sustituible por x en φ si cada aparición de t en $\varphi\,[t/x]$ contiene únicamente variables libres.

1.76 Observación. *La expresión $\varphi[\psi \rightsquigarrow \xi]$ hace referencia a cualquier función que tenga la misma estructura de φ, solo sustituyendo algunas (pero no necesariamente todas) las apariciones de ψ en φ, por ξ. Así mismo, $\varphi[\psi \leftrightsquigarrow \xi]$ es lo mismo, sólo que se pueden sustituir algunas apariciones de ψ por ξ y viceversa.*

1.77 Definición. *(Los axiomas de la lógica de primer orden)*
Consideraremos los siguientes axiomas:
Axiomas de lógica proposicional:

1. $\varphi \Longrightarrow (\psi \Longrightarrow \varphi)$;
2. $\varphi \Longrightarrow ((\psi \Longrightarrow \neg\varphi) \Longrightarrow \neg\psi)$;
3. $\varphi \Longrightarrow \varphi[\psi \leftrightsquigarrow \neg\neg\psi]$;
4. $\varphi \Longrightarrow \varphi[\psi \Longrightarrow \chi \leftrightsquigarrow \neg\chi \Longrightarrow \neg\psi]$;
5. $\varphi \Longrightarrow \varphi[\neg\psi \Longrightarrow \psi \leftrightsquigarrow \psi]$;
6. $(\varphi \Longrightarrow (\chi \Longrightarrow \psi)) \Longrightarrow ((\varphi \Longrightarrow \chi) \Longrightarrow (\varphi \Longrightarrow \psi))$;
7. la regla de inferencia **Modus Ponens**:

$$\frac{\varphi \Longrightarrow \psi \qquad \varphi}{\therefore \psi}$$

Las generalizaciones de esquemas de axiomas de primer orden:

1. $(\forall x)(\varphi \Longrightarrow \psi) \Longrightarrow (\forall x\varphi \Longrightarrow \forall x\psi)$;
2. $\varphi \Longrightarrow (\forall x\varphi)$, si x no aparece libre en φ;
3. $x = x$;
4. $x = y \Longrightarrow (\varphi \Longrightarrow \varphi')$, si φ es atómica y donde φ' resulta de reemplazar algunas apariciones de x por y en φ;
5. $\forall x\varphi \Longrightarrow (\varphi\,[t/x])$ si t es un término, sustituible por x en φ.

1.78 Definición. *(demostración)*

- Una demostración de φ a partir de Σ es una sucesión finita de formulas $(\varphi_1, \ldots, \varphi_n)$ tal que φ_i es elemento de Σ, axioma lógico o existen $j, k < i$ tales que φ_k es la fórmula $\varphi_j \Longrightarrow \varphi_i$.

- $\Sigma \vdash \varphi$ significa que existe una demostración formal de φ a partir de Σ.
- Σ es consistente si no hay ψ tal que

$$\Sigma \vdash \psi \wedge \neg\psi.$$

No prestaremos mayor importancia al cálculo deductivo, pues sale de las intenciones de este trabajo; sin embargo, por completitud, presentaremos algunas reglas de inferencia a continuación. Claramente no presentaremos prueba de todas ellas, sólo de algunas para ejemplificar.

Modus Tollens:

$$\frac{\begin{array}{c}\varphi \Longrightarrow \psi \\ \neg\psi\end{array}}{\therefore \varphi}$$

La prueba de dicha regla va como sigue:

1.	$\varphi \Longrightarrow \psi$	premisa
2.	$\neg\psi$	premisa
3.	$(\varphi \Longrightarrow \psi) \Longrightarrow (\neg\psi \Longrightarrow \neg\varphi)$	inst. Del axioma 4 de lógica prop.
4.	$\neg\psi \Longrightarrow \neg\varphi$	Modus Ponens con 3 y 1
5.	$\neg\varphi$	Modus Ponens con 4 y 2

Equivalencia de la conjunción:

$$\frac{\varphi \wedge \psi}{\therefore \neg(\varphi \Longrightarrow \neg\psi)}$$

$$\frac{\neg(\varphi \Longrightarrow \neg\psi)}{\therefore \varphi \wedge \psi}$$

Equivalencia de la disyunción:

$$\frac{\varphi \vee \psi}{\therefore \neg\varphi \Longrightarrow \psi}$$

$$\frac{\neg\varphi \Longrightarrow \psi}{\therefore \varphi \vee \psi}$$

Adición:

$$\frac{\varphi}{\therefore \varphi \vee \psi}$$

Simplificación:

$$\frac{\varphi \wedge \psi}{\therefore \psi}$$

Conjugación:

$$\frac{\begin{array}{c}\varphi \\ \psi\end{array}}{\therefore \varphi \wedge \psi}$$

Silogismo disyuntivo:

$$\frac{\begin{array}{c}\varphi \vee \psi \\ \neg\varphi\end{array}}{\therefore \psi}$$

Dobles negaciones:

$$\frac{\varphi}{\therefore \varphi[\psi \leftrightsquigarrow \neg\neg\psi]}$$

Transposición:

$$\frac{\varphi \Longrightarrow \psi}{\therefore \neg\psi \Longrightarrow \neg\varphi}$$

Leyes de Morgan:

$$\frac{\neg(\varphi \wedge \psi)}{\therefore \neg\varphi \vee \neg\psi}$$

La prueba de dicha regla va como sigue:

1.	$\neg\neg(\varphi \Longrightarrow \neg\psi)$	Equivalencia de la conjunción
2.	$\varphi \Longrightarrow \neg\psi$	Doble negación
3.	$\neg\neg\varphi \Longrightarrow \neg\psi$	Doble negación
4.	$\neg\varphi \vee \neg\psi$	Equivalencia de la disyunción

$$\frac{\neg(\varphi \vee \psi)}{\therefore \neg\varphi \wedge \neg\psi}$$

La prueba de dicha regla va como sigue:

1.	$\neg(\neg\varphi \Longrightarrow \psi)$	Equivalencia de la disyunción
2.	$\neg(\neg\varphi \Longrightarrow \neg\neg\psi)$	Doble negación
3.	$\neg\varphi \wedge \neg\psi$	Equivalencia de la conjunción

Mencionaremos dos teoremas antes de dar las últimas reglas de inferencia.

1.79 Teorema. *(de deducción)*
Sean φ y ψ formulas y Σ un conjunto de fórmulas. Entonces,

$$\Sigma \cup \{\varphi\} \vdash \Longleftrightarrow \Sigma \vdash (\varphi \Longrightarrow \psi).$$

1.80 Teorema. *Sea φ una fórmula, y sea Σ un conjunto de fórmulas. Entonces,*

$$\Sigma \cup \{\neg\varphi\} \vdash \psi \wedge \neg\psi \Longrightarrow \Sigma \vdash \varphi.$$

Instanciación universal:

$$\frac{\forall x\varphi}{\therefore \varphi[t/x]} \qquad \text{(siempre que } t \text{ sea sustituible).}$$

La prueba de dicha regla va como sigue:

1.	$\forall x\varphi$	premisa
2.	$\forall x\varphi \Longrightarrow \varphi[t/x]$	axioma 5 de primer orden
3.	$\varphi[t/x]$	Modus Ponens

Generalización existencial:

$$\frac{\varphi[t/x]}{\therefore \exists x\varphi} \qquad \text{(siempre que } t \text{ sea sustituible).}$$

La prueba de dicha regla va como sigue:

	1.	$\varphi[t/x]$	premisa
→	2.	$\forall x \neg\varphi$	premisa extra
	3.	$\neg\varphi[t/x]$	Instanciación universal
	4.	$\varphi[t/x] \wedge \neg\varphi[t/x]$	conjunción
	5.	$\neg\forall x \neg\varphi$	contradicción de 2 a 4

Generalización universal:

$$\frac{\varphi}{\therefore \forall x\varphi}$$ (siempre que x no aparezca libre en alguna premisa).

Cambio de variable:

$$\frac{\forall x\varphi}{\therefore \forall z\varphi[z/x]}$$ (si z no aparece libre en φ ni en ninguna premisa).

La prueba de dicha regla va como sigue:

1.	$\forall x\varphi$	premisa
2.	$\varphi[z/x]$	Instanciación universal
3.	$\forall z\varphi[z/x]$	Generalización universal

1.81 Teorema. *(Instanciación existencial)*
Sean φ y ψ dos fórmulas y sea Σ un conjunto de fórmulas. Sea w una variable que no aparece libre en ningún elemento de Σ ni tampoco en las fórmulas $\exists x\varphi$ ni en ψ. Suponga además que la variable x no aparece libre en ningún elemento de Σ. Si $\Sigma \cup \{\varphi[w/x]\} \vdash \psi$, entonces $\Sigma \cup \{\exists x\varphi\} \vdash \psi$.

Demostración. La hipótesis, junto con el teorema de la deducción, implican que $\Sigma \vdash \varphi[w/x] \Longrightarrow \psi$. Entonces, considere la siguiente demostración por contradicción a partir de $\Sigma \cup \{\exists x\varphi\}$.

→	1.	$\neg\psi$	suposición extra
	2.	$\varphi[w/x] \Longrightarrow \psi$	demostrable a partir de Σ
	3.	$\neg\varphi[w/x]$	Modus Ponens de 2 y 1
	4.	$\forall w \neg\varphi[w/x]$	generalización universal
	5.	$\forall x \neg\varphi$	cambio de variable en 4
	6.	$\neg\forall x \neg\varphi$	premisa
	7.	$\forall x \neg\varphi \wedge \neg\forall x \neg\varphi$	conjunción 5 y 6
	8.	ψ	contradicción de 1 a 7

□

1.82 Lema.

$$\Sigma \cup \{\forall x\varphi\} \vdash \forall z\varphi[z/x],$$

siempre que z sea sustituible por x en φ y z no aparezca libre en ningún elemento de $\Sigma \cup \{\forall x\varphi\}$.

Demostración.

1.	$\forall x\varphi$	premisa
2.	$\forall x\varphi \Longrightarrow \forall z\forall x\varphi$	axioma 2 de primer orden
3.	$\forall z\forall x\varphi$	Modus Ponens de 2 y 1

□

1.83 Teorema. *Sea φ una fórmula y Σ un conjunto de fórmulas. Si $\Sigma \vdash \varphi$, y x no aparece libre en ningún elemento de Σ, entonces $\Sigma \vdash \forall x\varphi$.*

Demostración. Sea $\Gamma = \{\psi | \Sigma \vdash \forall x\psi\}$. Afirmamos:

- Si ψ es axioma lógico, o $\psi \in \Sigma$, entonces $\psi \in \gamma$.
- Si $\psi \in \Gamma$ y $\psi \Longrightarrow \xi \in \Gamma$, entonces $\xi \in \Gamma$; es decir, Γ es cerrado bajo Modus Ponens.

Con esto, podría concluir que si $\Gamma \vdash \psi$, entonces $\psi \in \Gamma$ y hemos terminado. Así pues,

- El conjunto de axiomas lógico es *cerrado bajo generalizaciones*, luego si ψ es axioma lógico, entonces $\forall x\psi$ también lo es y $\Sigma \vdash \forall x\psi$, luego $\psi \in \Sigma$. Por otro lado, si $\psi \in \Sigma$, entonces,

1.	ψ	premisa
2.	$\psi \Longrightarrow \forall x\psi$	axioma 2 de primer orden (x no aparece libre en)$\psi \in \Sigma$
3.	$\forall x\psi$	Modus Ponens de 2 y 1

  Por lo tanto, $\Sigma \vdash \forall x\psi$; luego

$$\psi \in \Gamma.$$

- Supongamos $\psi \Longrightarrow \xi, \psi \in \Gamma$. Entonces,

$$\Sigma \vdash \forall x(\psi \Longrightarrow \xi) \wedge \Sigma \vdash \forall x\psi,$$

1.	$\forall x(\psi \Longrightarrow \xi)$	demostrable en Σ
2.	$\forall x\psi$	demostrable en Σ
3.	$\forall x(\psi \Longrightarrow \xi) \Longrightarrow (\forall x\psi \Longrightarrow \forall x\xi)$	axioma 1 de primer orden
4.	$\forall x\psi \Longrightarrow \forall x\xi$	Modus Ponens de 3 y 1
5.	$\forall x\xi$	Modus Ponens de 4 y 2

□

1.84 Teorema. *Si $\Sigma \cup \{\varphi[w/x]\} \vdash \psi$, entonces $\Sigma \cup \{\exists x\varphi\} \vdash \psi$ siempre y cuando w no aparezca libre en ningún elemento de Σ, ni en ψ, ni en $\exists x\varphi$, ni x aparezca libre en ningún elemento de Σ.*

Demostración. Por hipótesis y el teorema de la deducción 1.79,

$$\Sigma \vdash \{\varphi[w/x]\} \Longrightarrow \psi.$$

Considere la siguiente demostración a partir de $\Sigma \cup \{\exists x\varphi\}$:

→	1.	$\neg\psi$	premisa extra
	2.	$\varphi[w/x] \Longrightarrow \psi$	demostrable en Σ
	3.	$\neg\varphi[w/x]$	Modus Tollens de 2 y 1
	4.	$\exists x\varphi$	premisa
	5.	$\forall w\neg\varphi[w/x]$	Generalización universal
	6.	$\forall x\neg\varphi$	cambio de variable en 5
	7.	$\neg\exists x\varphi$	equivalente a 6
	8.	$\exists x\varphi \wedge \neg\exists x\varphi$	conjunción
	9.	ψ	Contradicción de 1 a 8

□

Por completud, mencionaremos la siguiente regla de inferencia:
Sustitución:

$$\frac{\begin{array}{c} x = y \\ \varphi \end{array}}{\therefore \varphi'}$$

Donde φ' es como en la definición 1.77.

1.5. Semantica en la lógica de primer orden

A continuación, presentaremos la útilidad de la sección anterior, mediante los resultados más significativos. Así mismo, omitiremos varias demostraciones. [3]

1.85 Definición. *(Modelo)*
Sea $\mathcal{L}_{PA} = \{\mathfrak{o}, +, \cdot, S, <\}$ el lenguaje de la aritmetica de Peano previamente definido. Un modelo para $\mathcal{L}_{PA}$ es una tupla de la forma

$$(A, O, \oplus, \odot, s, \prec)$$

tal que

1. A es conjunto no vacío;
2. $O \in A$;
3. $<$ es un símbolo de relación binaria tal que $\prec \subseteq A^2$;
4. $+, \cdot$ son símbolos de funcion binaria tal que $\oplus, \odot : A^2 \longrightarrow A$ y S es símbolo de función unaria tal que $s : A \longrightarrow A$.

1.86 Definición. *(interpretación)*
Sea $\mathcal{L}_{PA}$ el lenguaje de la aritmetica de Peano, y sea

$$\mathcal{A} = (A, O, \oplus, \odot, s, \prec)$$

un modelo para $\mathcal{L}_{PA}$. Una interpretación para $\mathcal{A}$ es una función

$$\iota : \{v_i \mid i \in \omega\} \longrightarrow A.$$

1.87 Teorema. *Sea el lenguaje $\mathcal{L}_{PA}$, el modelo $\mathcal{A}$ para $\mathcal{L}_{PA}$ y dada una interpretación $\iota : \{v_i \mid i \in \omega\} \longrightarrow A$, existe una única función $\hat{\iota}$, a la que llamatemos una extensión de ι:*

$$\hat{\iota} : \{t \mid t \text{ es un } \mathcal{L} - \text{término}\} \longrightarrow A$$

tal que

- $\hat{\iota}(v_i) = \iota(v_i)$;
- $\hat{\iota}(\mathfrak{o}) = O$;
- *si t_1 y t_2 son términos,*

$$\hat{\iota}(+t_1t_2) = \oplus(\hat{\iota}(t_1), \hat{\iota}(t_2));$$
$$\hat{\iota}(\cdot t_1t_2) = \odot(\hat{\iota}(t_1), \hat{\iota}(t_2));$$
$$\hat{\iota}(St_1) = s(\hat{\iota}(t_1)).$$

1.88 Definición. *(satisfacción)*
Sea $\mathcal{L}_{PA}$ el lenguaje de la aritmetica de Peano. Sea

$$\mathcal{A} = (A, O, \oplus, \odot, s, \prec)$$

un modelo para $\mathcal{L}_{PA}$ y sea ι una interpretación. Dada una fórmula φ, definimos $\mathcal{A} \vDash \varphi[\iota]$, leido como $\mathcal{A}$ satisface φ de acuerdo a la interpretación ι, por recursión sobre φ:

1. $\mathcal{A} \vDash (t_1 = t_2)[\iota] \iff \hat{\iota}(t_1)$ es lo mismo que $\hat{\iota}(t_2)$;
2. $\mathcal{A} \vDash \prec t_1 t_2[\iota] \iff (\hat{\iota}(t_1), \hat{\iota}(t_2)) \in \prec$;
3. $\mathcal{A} \vDash (\neg\varphi)[\iota] \iff \mathcal{A} \nvDash \varphi[\iota]$;
4. $\mathcal{A} \vDash (\varphi \Longrightarrow \psi)[\iota] \iff (\mathcal{A} \nvDash \varphi[i] \precsim \mathcal{A} \vDash \psi[i])$;
5. $\mathcal{A} \vDash (\forall v_i \varphi)[\iota] \iff \forall a \in A \;\; \mathcal{A} \vDash \varphi[\iota(a/v_i)]$.

1.89 Lema. *Sea $\mathcal{L}_{PA}$ el lenguaje de la aritmetica de Peano, $\mathcal{A}$ un modelo para $\mathcal{L}_{PA}$, sean ι e ι' dos interpretaciones y sean $v_{i_1}, \ldots, v_{i_k}$ tales que*

$$\forall j \quad (\iota(v_{i_j}) = \iota'(v_{i_j})).$$

1. *Si t es un término y todas las varaibles que aparecen en t se encuentran entre $v_{i_1}, \ldots, v_{i_k}$, entonces*
$$\hat{\iota}(t) = \hat{\iota}'(t);$$
2. *Si φ es una fórmula con todas sus variables libres entre $v_{i_1}, \ldots, v_{i_k}$; entonces*
$$\mathcal{A} \vDash \varphi[\iota] \iff \mathcal{A} \vDash \varphi[\iota'].$$

1.90 Definición. *(consecuencía lógica)*

$$\Sigma \vDash \varphi \iff (\forall \mathcal{A})(\forall \iota)(\mathcal{A} \vDash \Sigma[\iota] \Longrightarrow \mathcal{A} \vDash \varphi[\iota]).$$

1.91 Teorema. *(de correctud del cálculo proposicional)*
Sea φ una fórmula y sea Σ un conjunto de fórmulas. Entonces,

$$\Sigma \vdash \varphi \Longrightarrow \Sigma \vDash \varphi.$$

1.92 Definición. Un conjunto de fórmulas Σ es satisfacible si existe un módelo $\mathcal{A}$ y una interpretación ι tal que $\mathcal{A} \vDash \Sigma[\iota]$.

1.93 Teorema. *(de completud de Gödel)*
Si Σ es un conjunto de fórmulas consistentes, entonces es satisfacible.

1.94 Corolario. *Σ satisfacible $\Longrightarrow$ Σ consistente.*

Demostración. Si Σ fuera inconsistente, tendríamos $\Sigma \vdash \psi \wedge \neg\psi$. Por correctud,

$$\Sigma \vDash \psi \wedge \neg\psi,$$

entonces, si $\mathcal{A} \vDash \Sigma[\iota]$, entonces $\mathcal{A} \vDash \psi \wedge \neg\psi$, lo que es absurdo. Por lo tanto, Σ es consistente. □

1.95 Teorema. Σ *es consistente* $\iff \Sigma$ *es satisfacible.*

1.96 Teorema.

$$\Sigma \vdash \varphi \iff \Sigma \vDash \varphi.$$

1.97 Corolario. *(teorema de compacidad)*
Si $\Sigma \vDash \varphi$*, entonces existe* $\Delta \subseteq \Sigma$*, con* Δ *finito, tal que*

$$\Delta \vDash \varphi.$$

Demostración. Si $\Sigma \vDash \varphi$, entonces $\Sigma \vdash \varphi$; sea $(\varphi_1, \ldots, \varphi_n)$ una demostración y $\Delta = \{\varphi_1, \ldots, \varphi_n\} \cap \Sigma$. Entonces, Δ es finito y $\Delta \vdash \varphi$. Por lo tanto, $\Delta \vDash \varphi$. □

1.6. Teoría de la computabilidad

En la siguiente sección abordaremos la teoría de computabilidad, cuyos principales contribuidores fueron *Alan Turing* mediante su *máquina de Turing*, *Kurt Gödel* mediante la *teoría de la recursión* y *Alonzo Church* mediante el $\lambda-$*cálculo.* En esta ocasión nos quedaremos principalmente con ideas intuitivas sobre máquinas de Turing y más formalmente sobre recursión, todo esto con la intención de presentar el concepto de función computable. [4]

1.98 Definición. Una maquina de Turing consta de:

- un alfabeto, es decir, un conjunto finito L;
- un conjunto finito S de estados;
- una función de transición con dominio subconjunto de $(S \cup \{s_o\}) \times (L \cup \{*\})$ y codominio $S \times (L \cup \{*\}) \times \{<, >, -\}$.

1.99 Observación. *Toda maquina de Turing especifica de manera única una función cuyo dominio y rango son subconjuntos del conjunto de sucesiones finitas de* L*.*

1.100 Ejemplo. Consideremos

$$L = \{1\}, \qquad S = \{s_1, s_f\},$$

y la función de transición:

$$\begin{gathered}(s_0, 1, s_0, 1, >)\\ (s_0, *, s_1, *, <)\\ (s_1, 1, s_0, 1, <)\\ (s_1, *, s_f, 1, -);\end{gathered}$$

esta es la función sucesor en lenguaje unario.

1.101 Definición. Una función $f : A \longrightarrow \omega^p$, con $p \in \omega$, es computable si existe un algoritmo tal que al recibir el input n, eventualmente termina si, y sólo si $n \in A$, en cuyo caso el output es $f(n)$.

1.102 Ejemplo. La función *busy beaver* no es computable:

- Fijamos el alfabeto $\{1\}$,

- para cada n,
$$A_n := \{f | f \in C\},$$
donde C es la colección de funciones computables por una máquina de Turing con a lo más n estados (más, quizá, el estado final).

$$A_1 := \{\varnothing, n \mapsto n+1, n \mapsto n, n \mapsto n-1, 0, 1\}.$$

Cada A_n es finito (tiene a lo sumo $2^{2(n+1)(n+1)\cdot 2\cdot 3}$ de elementos). La función **busy beaver** está dada por:

$$\sigma : \omega \longrightarrow \omega$$
$$\sigma(n) = \text{máx}\{f(0) | 0 \in \text{dom}(f), f \in A_n\}.$$

1.103 Definición. *(máquina universal de Turing)*
Llamamos así a la función $\Phi : A \longrightarrow \omega$, con $A \subseteq \omega \times \omega$. $\Phi(e, n)$ es el resultado de introducir el imput n en la $e-$ésima máquina de Turing.

Por la tesis de Church-Turing, la función Φ es computable.

1.104 Observación. *Para toda función computable f, existe e tal que*

$$f(n) = \Phi(e, n).$$

1.105 Lema. *Para toda función computable f, existen una infinidad de e tales que*

$$f(n) = \Phi(e, n).$$

1.106 Definición. *(función total)*
Una función computable se dice total si para cualquier número natural como input, la función se detiene, es decir, el cálculo de su output se puede obtener en un número finito de pasos.

1.107 Teorema. *El conjunto*

$$e \in \omega | \Phi(e, -) \text{ es una función total}$$

no es computable. Es decir, no existe un algoritmo que, dado e, decida si la $e-$ésima función computable es total.

Demostración. Supongamos que este conjunto si es computable, entonces hay una función computable

$$l \mapsto f_l,$$

la $l-$ésima función computable.

```
input(l);
j=0;
for(i=0;j<l;i++){
    if(Phi(i,-) es total)
        j++;
}return i;
```

Por lo tanto, la función

$$u : \omega^2 \longrightarrow \omega$$
$$(a, b) \mapsto f_a(b)$$

es total computable. Sea $g : \omega \longrightarrow \omega$, dada para cada $k \in \omega$ por

$$g(k) = u(k, k) + 1.$$

Tenemos que g es computable, por lo tanto, existe l tal que $g = f_l$. Entonces,

$$u(l, l) = f_l(l) = g(l) = u(l, l) + 1,$$

lo cuál es una contradicción. □

1.108 Definición. *(conjunto computable)*
Sea $X \subseteq \omega^k$. Decimos que X es computable si $\chi_X : \omega^k \longrightarrow \{0, 1\}$ es una función total computable. Es decir, X es computable si existe un algoritmo con imput n, tal que determina si $n \in X$ o no.

1.7. Problema de la detención

También conocido por su nombre en alemán *entscheindungsproblem*, o en inglés *halting problem*, este concepto es de importancia capitál para entender las límitaciones de la computabilidad, lo cuál eventualmente nos llevará a la incompletitud. [4]

1.109 Teorema. *(problema de la detención)*
El conjunto

$$\{(e, n) | \Phi(e, n) \text{ está definida}\}$$

no es computable. Es decir, no existe un algoritmo que diga cuáles algoritmos se detienen.

Demostración. Basta demostrar que $D = \{e \in \omega | \Phi(e, e) \text{ está definido}\}$ no es computable. Supongamos que D es computable. Entonces, la función

$$f : \omega \longrightarrow \omega$$
$$f(n) = \begin{cases} 1 & n \notin D \\ \text{indefinido} & n \in D \end{cases}$$

es computable. Está es representada por el siguiente pseudocodigo:

```
input(n)
if(chi_D(n)==0)
    return 1;
else
    for(i=1; ;i++)
```

Por lo tanto, sea e tal que

$$f = \Phi(e, -).$$

Entonces,

$$\begin{aligned}\Phi(e,e) &= f(e)\\ &= \begin{cases}1 & e \notin D\\ \text{indefinido} & e \in D\end{cases}\\ &= \begin{cases}1 & \Phi(e,e) \text{ no está definido}\\ \text{indefinido} & \Phi(e,e) \text{ está definido}\end{cases},\end{aligned}$$

lo cuál es absurdo, luego D no es computable. □

1.110 Proposición. *Si X y Y son computables, entonces*

$$X \cup Y, \qquad X \cap Y, \qquad X\backslash Y$$

también lo son.

Demostración.

- $\chi_{X\cup Y} = \max\{\chi_X, \chi_Y\}$;
- $\chi_{X\cap Y} = \min\{\chi_X, \chi_Y\} = \chi_X \cdot \chi_Y$;
- $X\backslash Y = X \cap (\omega\backslash Y)$, $\chi_{\omega\backslash Y} = 1 - \chi_Y$, entonces $\chi_{X\backslash Y} = \chi_X \cdot (1 - \chi_Y)$.

□

1.111 Proposición. *Si $X \subseteq \omega^2$ es computable, entonces:*

1. *Dado n,*
$$Y = \{m \in \omega | \exists k < n((m,k) \in X)\}$$
es computable.
2. *En general,*
$$Z = \{m \in \omega | \exists k((m,k) \in X)\}$$
no es computable.

Demostración. 1. La demostración se sigue del siguiente pseudocodigo:

```
input(m)
for(k=0;k<n;k++)
    if(Xx(m,k))
        return 1;
return 0;
```

2. Recordemos que
$$D = \{e | \Phi(e,e) \text{ está definido}\}$$
no es computable. Sea
$$X = \{(m,k) | \Phi(m,m) \text{ se detiene a lo más en } k \text{ pasos}\},$$
entonces X es computable. Note que:
$$\{m | \exists k((m,k) \in X)\} = \{m | \Phi(m,m) \text{ se detiene eventualmente}\} = D,$$
que no es computable.

□

1.112 Definición. *(conjunto computablemente enumerable)*
Un conjunto $X \subseteq \omega$ es computablemente enumerable (también listable o c.e.) si existe una función total computable $f : \omega \longrightarrow \mathcal{P}(\omega)$ tal que:

1. $f(0) = \varnothing$,
2. $\forall n(|f(n+1) \backslash f(n)| \leqslant 1 \wedge f(n) \subseteq f(n+1))$,
3. $X = \bigcup_{n \in \omega} f(n)$.

1.113 Ejemplo.

1. $D = \{n | \Phi(n, n)$ está definido$\}$ es c.e.:

```
for(i=0; ;i++)
    for(j=0;j<=i;j++)
        correr Phi(j,j) i pasos
        si se detiene, print j;
```

2. $H = \{(a, b) | \Phi(a, b)$ está definido$\}$ es c.e.

1.114 Proposición. *Todo conjunto computable es c.e.*

Demostración. Si X es computable, entonces

```
for(n=0; ;n++)
    if(chi_X(n))
        print n;
```

□

1.115 Observación. *El reciproco en general es falso, y el contraejemplo viene en los últimos ejemplos dados.*

1.116 Proposición. *Si X y Y son computablemente enumerables, entonces:*

- *$X \cup Y$ también lo es,*
- *$X \cap Y$ también lo es.*

Demostración. Si A_X y A_Y son algoritmos que imprimen a X y Y respectivamente. Entonces,

```
for(n=1; ;n++)
    correr A_X n pasos
    correr A_Y n pasos
```

la cuál imprime a $X \cup Y$. Por otro lado,

```
for(n=1; ;n++)
    correr A_X n pasos, determinando L;
    correr A_Y n pasos, determinando L';
    print(L intersección L')
```

□

1.117 Teorema. *Para $X \subseteq \omega$, los siguientes enunciados son equivalente:*

1. *X es c.e.*
2. *La función semicaracteristica de X, denotada σ_X, es computable. Esta función viene dada por la regla de asignación:*

$$\sigma_X(n) = \begin{cases} 1 \text{ si } n \in X \\ \uparrow \text{ en otro caso} \end{cases} .$$

3. *Existe una función computable f tal que $\mathrm{dom}(f) = X$.*
4. *Existe un $Y \subseteq \omega \times \omega$ computable tal que*

$$X = \{n \in \omega | \exists k \in \omega((n,k) \in Y)\}.$$

Demostración. 1. $\Longrightarrow$ 2. :
Sea A_X el algoritmo que imprime a X. Entonces, el siguiente algoritmo calcula a σ_X:

```
input(n)
correr A_X
    if(se imprimió n)
        return 1;
```

2. $\Longrightarrow$ 3. :
Inmediato tomando $f = \sigma_X$.
3. $\Longrightarrow$ 4. :
Sea $Y = \{(n,k)|$el algoritmo que calcula $f(x)$ se detiene en, a lo más, k pasos$\}$. Notemos que Y es computable, con input (n,k). Se corre el algoritmo para $f(n)$ k pasos; si alcanza a detenerse, devuelve 1, en caso contrario devuelve 0. $\pi[Y] = X$, ya que $n \in X$ si, y sólo si $f(x)$ está definido si, y sólo si para algún k, el cálculo de $f(n)$ termina en k pasos si, y sólo si $(n,k) \in Y$.
4. $\Longrightarrow$. :
Supongamos Y como en la hipótesis, es decir, hay un algoritmo que calcula χ_Y, entonces el siguiente algoritmo imprime a X:

```
for(n=0; ;n++)
    sean a y b tales que n=2^a(2*b+1)
    if(chi__Y(a,b))
        print a;
```

□

1.118 Teorema. *(Kleene)*
Sea $X \subseteq \omega$. Entonces,

$$X \text{ es computable} \Longleftrightarrow (X \text{ y } \omega \backslash X \text{ son c.e.}).$$

Demostración.
$\Longrightarrow$): si X es computable, entonces $\omega\backslash X$ también lo es. Luego, X y $\omega\backslash X$ son c.e.
$\Longleftarrow$): sean A_X y $A_{\omega\backslash X}$ los algoritmos que imprimen a X y $\omega\backslash X$, respectivamente. El siguiente algoritmo calcula χ_X:

```
input(n)
correr A_X y A_{C(X)} en paralelo, esperar a que se imprima $n$
    si A_X lo imprimió
        return 1;
    si A_{C(X)} lo imprimió
        return 0;
```

□

1.119 Observación. *Ni $\omega\backslash D$, ni $\omega^2\backslash H$ son c.e. (pues por el teorema de Kleene, D y H serían numerables).*

1.120 Teorema. *Sea $f : A \longrightarrow \omega$ tal que $A \subseteq \omega$. Entonces,*

$$f \text{ es computable} \iff Gr(f) \text{ es c.e.}$$

Demostración.
$\Longleftarrow$) Si $A_{Gr(f)}$ es el algoritmo que imprime a $Gr(f)$, entonces:

```
input(n)
correr A_{Gr(f)} tal que se imprima una pareja (x,y) tal que x=n
en tal caso, return y;
```

es un algoritmo que calcula a f.
$\Longrightarrow$) Considere el algoritmo:

```
for(n=0; ;n++)
    for(k=0;k<=;k++)
        corrar f(k) n pasos
        si se obtiene una respuesta y
            print(k,y);
```

□

1.121 Teorema. *Sea $X \subseteq \omega$, con $X \neq \varnothing$. Entonces,*

$$X \text{ es c.e.} \iff (\exists f : \omega \longrightarrow \omega)(f \text{ es total computable} \wedge X = \operatorname{ran}(f)).$$

Demostración.
$\Longleftarrow$) Si hay un algoritmo para f, entonces

```
for(n=0; ;n++)
    print f(n)
```

es un algoritmo que imprime $\operatorname{ran}(f) = X$.
$\Longrightarrow$) Sea $x_o \in X$ arbitrario. Considere el siguiente algoritmo:

```
input(n)
correr el algoritmo que imprime a X n pasos
    si no se imprime nada, return x_o;
    en caso contrario, si y es el último número impreso
    return y;
```

esta última función es total y $\text{ran}(f) = X$. □

1.8. Los teoremas de incompletitud de Gödel

A continuación se presentarán dos de los resultados más importantes en la historia de las matemáticas, así como varios resultados previos que desembocaron en estos teoremas que dieron fama mundial a Kurt Gödel y que sustentan la existencia de proposiciones indemostrables. [4]

1.122 Observación. *Sea $\mathcal{S}$ el conjunto de sucesiones finitas de símbolos de $\mathcal{L}$. Entonces, los siguientes conjuntos son computables:*

$$Term = \{t \in \mathcal{S} | t \text{ es término}\},$$

$$Form = \{\varphi \in \mathcal{S} | \varphi \text{ es una fórmula}\},$$

$$\{(\varphi, x) \in \mathcal{S} \times variables | x \text{ es variable libre de } \varphi\},$$

$$Sent = \{\varphi \in \mathcal{S} | \varphi \text{ es un enunciado}\},$$

$$\{\varphi \in \mathcal{S} | \varphi \text{ es axioma lógico}\},$$

$$\{(a_1, a_2, a_3) \in \mathcal{S}^3 | a_1 \equiv a_2 \Rightarrow a_3 \vee a_2 \equiv a_1 \Rightarrow a_3\},$$

$$Dem = \{(\varphi_1, \ldots, \varphi_n) | (n \in \omega)(\varphi_i \text{ es fórmula}) \wedge (\varphi_1, \ldots, \varphi_n) \text{ es demostración formal}\}.$$

Por otro lado, el conjunto

$$Teor = \{\varphi \in \mathcal{S} | \text{ existe una demostración de } \varphi\}$$

no es computable, pero es computablemente enumerable.

1.123 Proposición. *Sea Σ un conjunto de $\mathcal{L}-$fórmulas.*

$$Dem(\Sigma) = \{(\varphi_1, \ldots, \varphi_n) | (n \in \omega)(\varphi_i \text{ fórmula}) \wedge (\varphi_1, \ldots, \varphi_n) \text{ demostración a partir de } \Sigma\}.$$

Si Σ es computable, entonces $Dem(\Sigma)$ también lo es. Por otro lado,

$$\begin{aligned} Teor &= \{\varphi \in \mathcal{S} | \text{existe una demostración de } \varphi \text{ a partir de } \Sigma\} \\ &= \{\varphi \in \mathcal{S} | \Sigma \vdash \varphi\} \end{aligned}$$

es computablemente enumerable.

1.124 Definición. (completud)
Un conjunto de fórmulas Σ es completo si para cada fórmula φ,

$$\Sigma \vdash \varphi \vee \Sigma \vdash \neg\varphi.$$

1.125 Observación. *Si Σ es completo y computable, entonces Teor(Σ) es computable. Si Σ es completo, entonces*

$$\mathcal{S}\backslash Teor(\Sigma) = \{\varphi | \varphi \text{ no es fórmula } \vee \Sigma \vdash \neg\varphi\}.$$

Tenemos el siguiente hecho: *Ningún Σ en $\mathcal{L}_A = \{+, \cdot, \mathbf{0}, S, <\}$, que sea un intento razonable de axiomatizar ω, puede ser completo y computable.*

1.126 Definición. Un conjunto $X \subseteq \omega^k$ es definible si existe una formula $\varphi(x_1, \ldots, x_k)$ tal que

$$X = \{(a_1, \ldots, a_k) | \omega \vDash \varphi[a_1, \ldots, a_k]\}.$$

1.127 Observación. *Señalaremos una nueva forma de códificar parejas:*

$$(a, b) \text{ se codifica por } (a + b)^2 + a.$$

Dadp n, me fijo en la sucesión de cuadrados perfectos $(n^2)_{n\in\omega}$, y encuentro m tal que $m^2 \leqslant n < (m + 1)^2$. Hacemos $a = n - m^2$, $b = m - a$, y n codifica (a, b). Notemos:

$$''n \text{ codifica } (a, b)'' \Longleftrightarrow \omega \vDash ((x + y) * (x + y) + x = z)[a, b, n].$$

Ahora, para codificar tuplas: Para cada i, $q_i = código(m_i, i)$. Sea

$$n = \text{máx}\{q_0, \ldots, q_{k-1}\},$$

y sea

$$u = \prod_{i<k}(1 + (q_i + 1)n!);$$

entonces,

$$(m_0, \ldots, m_{n-1}) \text{ se codifica como } (u + n!)^2 + u = código(u, n!).$$

1.128 Lema. *Si $q < r < n$, entonces $(1 + (q + 1)n!)$ es primo relativo con $(1 + (r + 1)n!)$.*

Demostración. Supongamos que p es primo y

$$p|1 + (q + 1)n! \wedge p|1 + (r + 1)n!,$$

entonces

$$p|n!(r - q)$$

pero $p \not| n!$ (en tal caso, $p = 1$ lo cuál es absurdo), por lo tanto,

$$p|r - q.$$

Como $(p, i) = 1$, para todo $i < n$ y $r - q < n$, esto es una contradicción. □

1.129 Lema. *Si $q < n$, entonces*

$$(1 + (q + 1)n!)|u \Longleftrightarrow q = q_j, \text{ para algún } j.$$

Demostración. Por el lema anterior, si $q < n$ es distinto de $q_0, \ldots, q_{k-1}$, entonces

$$(\forall l \in [[0, k - 1]])((1 + (q + 1)n!, 1 + (q_l + 1)n!) = 1).$$

Luego,

$$1 + (q + 1)n! \text{ es primo relativo con } \prod_{j<k}(1 + (q_j + 1)n!) = u.$$

□

1.130 Lema. *Para cada i, m_i es el mínimo m tal que*

$$1 + (\textit{código}(m, i) - 1)n!|u \tag{R}$$

Demostración. m_i sí satisface (R), falta ver que ningún $m < m_i$ satisface (R). Supongamos que $m < m_i$ satisface (R), entonces sea $q = \text{código}(m, i)$.Entonces, $(1 + (q + 1)n!)|u$, pero por el lema anterior

$$q = q_j, \text{ para algún } j.$$

Luego, $q = q_i$, es decir, $m = m_i$, lo cuál es absurdo. □

1.131 Observación. *a es la $i-$ésima entrada de la tupla codificada por t.*

$$(\exists u < t \wedge \exists v < t)[(t \textit{ códifica a } (u, v) \wedge \exists z(z \textit{ codifica a } (a, i)) \wedge 1 + (z + 1)v|u)]$$

$$\wedge(\textit{además, } a \textit{ es el mínimo con esa propiedad}).$$

$$(\exists a)\psi(a, i, t) \wedge \forall j > i \exists a \psi(a, i, t)$$

"la sucesión codificada por t es de longitud i".

1.132 Observación. *T máquina de Turing.*
Estados $\{s_i, s_f\}$.
$T = \{(0, s_i, 1, s_i, >), (1, s_i, 1, s_i, >), (*, s_i, *, s_f, -)\}$.
En cada paso, tenemos la foto instantanea

$$(i, j, k)$$

donde,

- *i es el estado actual,*
- *j es la posición,*
- *k es lo que hay escrito en la cinta.*

Así pues,

- *"(x, y, z) es una foto instantanea valida" $(FI(x, y, z))$:*
  $(x = \mathbf{0} \vee x = S\mathbf{0}) \wedge \forall u(\exists l(u < l \wedge long(l, z))(\exists l(long(l, z) \wedge y \leqslant l) \implies \exists v(Tupla(v, n, z) \implies (v = \mathbf{0} \vee v = S\mathbf{0} \vee v = SS\mathbf{0}))))$.

- *"(x_1, y_1, z_1) es la foto instantanea inmeadiatamente posterior a (x_2, y_2, z_2)"*
  $T(x_1, y_1, z_1, x_2, y_2, z_2)$:
  $(\text{"}(x_1, y_1, z_1) \textit{ es toto inst. valida}\text{"}) \wedge \exists s \left(\text{Tupla}(s, y_1, z_1) \wedge \left((s = \mathbf{0} \wedge x_2 = x_1) \vee (s = S\mathbf{0} \wedge x_2 = x_1) \wedge y_2 = y_1 + S\mathbf{0} \wedge \exists l \left(\text{long}(l, z_1) \wedge \text{long}(l, z_2) \wedge \forall u < l \left(u \neq y_1 \Rightarrow \exists t \left(\text{Tupla}(t, v, z_1) \wedge \cdots \wedge \text{Tupla}(t, u, z_2) \wedge (s = \mathbf{0} \wedge \text{Tupla}(S\mathbf{0}, y_1, z_2) \vee s = S\mathbf{0} \wedge \text{Tupla}(S\mathbf{0}, y_1, z_2) \vee (\text{long}(y_1, z_1) \wedge x_2 = S\mathbf{0} \wedge y_2 = y_1)\right.\right.\right.\right.\right.\right.\right.$.

- *"si yo corro T con input x, entonces la máquina se detiene y el output es y" $C(x, y)$:*
  $\exists s \exists l \big(\text{long}(l, s) \wedge (\exists w)\,(l = SSS\mathbf{0}w \wedge \text{Tupla}(\mathbf{0}, \mathbf{0}, s) \wedge \text{Tupla}(\mathbf{0}, S\mathbf{0}, s) \wedge \text{Tupla}(x, SS\mathbf{0}, s)$
  $\wedge \forall u < w\,(\exists x_1 \exists y_1 \exists z_1 \exists x_2 \exists y_2 \exists z_2\; T(x_1, y_1, z_1, x_2, y_2, z_2) \wedge \text{Tupla}(x_1, z \cdot w, s) \wedge \text{Tupla}(y_1, Sz \cdot w, s) \wedge \text{Tupla}(z_1, SSz \cdot w, s) \wedge \text{Tupla}(x_2, SSSz \cdot w, s) \wedge \text{Tupla}(y_2, SSSSz \cdot w, s) \wedge \text{Tupla}(z_2, SSSSSz \cdot w, s)) \wedge \exists \alpha\, SSS\alpha = l \wedge \text{Tupla}(S\mathbf{0}, \alpha, s) \wedge \text{Tupla}(y, SS\alpha, s)$

1.133 Teorema. *Si $f : \omega \longrightarrow \omega$ es parcialmente computable, entonces*

$$Gr(f) = \{(n, f(n))|n \in \mathrm{dom}(f)\}$$

es definible.

Demostración. Existen las siguientes formulas:

- $\mathrm{Par}(x, y, z)$ que es $''z$ codifica $(x, y)''$.
- $\mathrm{Tupla}(x, y, z)$ que es $''x$ es la $y-$ésima entrada de la tupla codificada por z''.
- $\mathrm{Long}(y, z)$ que es $''$la longitud de la tupla codificada por z es y''.
- $\mathrm{FI}(x, y, z)$.
- $T(x_1, y_1, z_1, x_2, y_2, z_2)$.
- $C(x, y)$.

Por lo que se tiene el teorema. □

A partir de ahora y hasta que acabe el capítulo, consideraremos a $\mathcal{N}$ como el módelo o la teoría de los números naturales. Se definirá más adeltante de forma correcta y formal a este modelo, pero por ahora basta esta intuición para terminar con los prerrequisitos.

1.134 Teorema. *(Indecibilidad de la Aritmética)*
El conjunto $Th(\mathcal{N}) = \{\mathcal{N} \vDash \varphi\}$ no es computable.

Demostración. Supongamos que sí es decidible, es decir, existe una enumeración efectiva de las formulas $\varphi_1, \ldots, \varphi_n, \ldots$ y un algoritmo que calcula correctamente

$$\chi_{\mathrm{Th}(\mathcal{N})}(n) = \begin{cases} 1, & \text{si } \mathcal{N} \vDash \varphi_n \\ 0, & \text{si } \mathcal{N} \nvDash \varphi_n \end{cases}.$$

Por el teorema anterior,

$$\{(n, 0)|\mathcal{N} \nvDash \varphi_n\} \cup \{(n, 1)|\mathcal{N} \vDash \varphi_n\}$$

es definible, luego, existe una fórmula $\varphi(x, y)$ tal que

$$(\mathcal{N} \vDash \varphi[n, 0] \Longleftrightarrow \mathcal{N} \nvDash \varphi_n) \wedge (\mathcal{N} \vDash \varphi[n, 1] \Longleftrightarrow \mathcal{N} \vDash \varphi_n).$$

Sea $\psi(x) \equiv \varphi(x, S\mathbf{0})$. Entonces,

$$\mathcal{N} \vDash \psi[m] \Longleftrightarrow \mathcal{N} \vDash \varphi_m.$$

Sea e tal que $\neg\psi$ es φ_e, entonces

$$\mathcal{N} \vDash \varphi_e[e] \Longleftrightarrow \mathcal{N} \vDash \psi[e] \Longleftrightarrow \mathcal{N} \vDash \neg\psi[e],$$

lo cuál es absurdo. □

1.135 Teorema. *(Indefinibilidad de la verdad de Tarski)*
$Th(\mathcal{N})$ no es definible.

Demostración. Si fuera definible, entonces existiría

$$\mathcal{N} \vDash \psi[m] \Longleftrightarrow \mathcal{N} \vDash \varphi_m.$$

Sea e tal que $\neg\psi$ es φ_e, entonces

$$\mathcal{N} \vDash \varphi_e[e] \Longleftrightarrow \mathcal{N} \vDash \psi[e] \Longleftrightarrow \mathcal{N} \vDash \neg\psi[e],$$

lo cuál es absurdo. □

1.136 Corolario. *Si $\Sigma \subseteq Th(\mathcal{N})$ es computable, entonces es incompleto.*

Demostración. De lo contrario, si $\Sigma \subseteq \mathrm{Th}(\mathcal{N})$ es computable y compacto, entonces:

$$\mathrm{Teor}(\Sigma) = \{\varphi | \Sigma \vdash \varphi\}.$$

sería computable. Pero,

$$\mathrm{Th}(\mathcal{N}) \subseteq \mathrm{Teor}(\Sigma) \subseteq \mathrm{Th}(\mathcal{N});$$

ambas contenciones se tienen de los siguientes hechos:

- Si $\varphi \notin \mathrm{Teor}(\Sigma)$, entonces $\Sigma \nvdash \varphi$ por completud, $\Sigma \vdash \neg\varphi$ por lo tanto $\mathcal{N} \vDash \neg\varphi \implies \mathcal{N} \nvDash \varphi$.
- Por el teorema de correctud: $\mathcal{N} \vDash \Sigma$ así que si $\Sigma \vdash \varphi$, $\Sigma \vDash \varphi$, luego $\mathcal{N} \vDash \varphi$.

Pero, $\mathrm{Teor}(\Sigma)$ es computable y $\mathrm{Th}(\mathcal{N})$ no lo es, lo cuál es una contradicción. □

1.137 Definición. *(Aritmética de Robinson)*
El conjunto Q (RA) consta de las siguientes formulas:

1. $\forall x \ \neg(\mathbf{0} = Sx)$;
2. $\forall x \forall y \ (Sx = Sy \implies x = y)$;
3. $\forall x \ \neg(x < \mathbf{0})$;
4. $\forall x \forall y \ (x < Sy \implies (x < y \vee x = y))$;
5. $\forall x \forall y \ (x < y \vee x = y \vee y < x)$;
6. $\forall x \ (x + \mathbf{0} = x)$;
7. $\forall x \forall y \ (x + Sy = S(x + y))$;
8. $\forall x \ (x \cdot \mathbf{0} = \mathbf{0})$;
9. $\forall x \forall y \ (x \cdot Sy = x \cdot y + x)$.

1.138 Observación. *Q es un conjunto finito.*

1.139 Definición. 1. $\mathbf{n} := \underbrace{S \ldots S}_{n-\text{veces}} \mathbf{0}$.

2. Un conjunto $X \subseteq \omega^k$ es $\Sigma-$representable si existe una fórmula φ tal que:

$$(n_1, \ldots, n_k) \in X \Longleftrightarrow \Sigma \vdash \varphi[x_1/\mathbf{n}_1, \ldots, x_k/\mathbf{n}_k]$$

y

$$(n_1, \ldots, n_k) \notin X \Longleftrightarrow \Sigma \vdash \neg\varphi[x_1/\mathbf{n}_1, \ldots, x_k/\mathbf{n}_k].$$

3. Un conjunto $X \subseteq \omega^k$ es débilmente $\Sigma-$representable si existe una fórmula φ tal que:

$$(n_1, \ldots, n_k) \in X \Longleftrightarrow \Sigma \vdash \varphi[x_1/\mathbf{n}_1, \ldots, x_k/\mathbf{n}_k].$$

1.140 Teorema.

1. *Toda función computable es $Q-$representable.*
2. *Todo conjunto computable es $Q-$representable.*

Demostración.

1. Análoga a la demostración de

$$\text{"}f \text{ es computable } \Longrightarrow \ f \text{ es definible"}.$$

2. Sea A computable y sea $\varphi(x, y)$ la fórmula que $Q-$representa a χ_A. Es decir,

$$(n, m) \in \mathrm{Gr}(\chi_A) \Longleftrightarrow Q \vdash \varphi[\mathbf{n}/x, \mathbf{m}/y] \wedge (n, m) \notin \mathrm{Gr}(\chi_A) \Longleftrightarrow Q \vdash \neg\varphi[\mathbf{n}/x, \mathbf{m}/y].$$

Sea $\psi(x) \equiv (y = S\mathbf{0} \wedge \varphi(x, y))$. Afirmamos que ψ representa a A:

$$\begin{aligned} n \in A &\Longleftrightarrow \chi_A(n) = 1 \\ &\Longleftrightarrow (n, 1) \in \mathrm{Gr}(\chi_A) \\ &\Longleftrightarrow Q \vdash \varphi[\mathbf{n}/x, S\mathbf{0}/y] \\ &\Longleftrightarrow Q \vdash (y = S\mathbf{0} \wedge \varphi(x, y))[\mathbf{n}/x]; \end{aligned}$$

y

$$\begin{aligned} n \notin A &\Longleftrightarrow \chi_A(n) = 0 \\ &\Longleftrightarrow (n, 1) \notin \mathrm{Gr}(\chi_A) \\ &\Longleftrightarrow Q \vdash \neg\varphi[\mathbf{n}/x, \mathbf{1}/y] \\ &\Longleftrightarrow Q \vdash \neg(y = S\mathbf{0} \wedge \psi(x, y))[\mathbf{n}/x]. \end{aligned}$$

□

1.141 Teorema. *(Primer teorema de incompletitud de Gödel)*
Si Σ es cualquier conjunto de fórmulas compatible con Q, es decir, tal que $\Sigma \cup Q$ es consistente; entonces,

1. *Teor(Σ) no es conjunto computable;*
2. *si Σ es computable, entonces es incompleto.*

Demostración.

1. Probemos que $\text{Teor}(\Sigma \cup Q)$ no es computable. Sea $\varphi_1(x), \varphi_2(x), \ldots, \varphi_n(x), \ldots$ una enumeración efectiva de las fórmulas con una variable libre. Sea

$$X = \{m \in \omega | \Sigma \cup Q \vdash \varphi_m[\mathbf{m}/x]\}.$$

Si $\text{Teor}(\Sigma \cup Q)$ fuera computable, X también lo sería, luego X sería $Q-$representable y X también sería $(\Sigma \cup Q)-$representable, es decir, existe una formila $\psi(x)$ tal que para cada $m \in \omega$,

$$m \in X \Longleftrightarrow \Sigma \cup Q \vdash \psi[\mathbf{m}/x],$$

y

$$m \notin X \Longleftrightarrow \Sigma \cup Q \vdash \neg\psi[\mathbf{m}/x].$$

Sea e tal que $\neg\psi$ es la formula φ_e. Entonces,

$$\begin{aligned} e \in X &\Longleftrightarrow \Sigma \cup Q \vdash \varphi_e[\mathbf{e}/x] \quad \text{(definición de } X\text{)} \\ &\Longleftrightarrow \Sigma \cup Q \vdash \psi[\mathbf{e}/x] \quad \text{(definición de } \psi\text{)} \\ &\Longleftrightarrow \Sigma \cup Q \vdash \neg\varphi_e[\mathbf{e}/x], \end{aligned}$$

lo cuál es una contradicción. Por lo tanto, $e \notin X$, pero

$$\begin{aligned} e \notin X &\Longleftrightarrow \Sigma \cup Q \nvdash \varphi_e[\mathbf{e}/x] \quad \text{(definición de } X\text{)} \\ &\Longleftrightarrow \Sigma \cup Q \vdash \neg\psi[\mathbf{e}/x] \quad \text{(definición de } \psi\text{)} \\ &\Longleftrightarrow \Sigma \cup Q \vdash \varphi_e[\mathbf{e}/x], \end{aligned}$$

por lo tanto, $\text{Teor}(\Sigma \cup Q)$ es no computable. Ahora, supongamos que $\text{Teor}(\Sigma)$ es computable. Sea $\mathcal{O}$ la conjunción de todos los elementos de Q. Entonces, el conjunto $\{\varphi | \Sigma \vdash (\mathcal{O} \implies \varphi)\}$ también lo sería. Pero

$$\begin{aligned} \{\varphi | \Sigma \vdash (\mathcal{O} \implies \varphi)\} &= \{\varphi | \Sigma \cup \{\mathcal{O}\} \vdash \varphi\} \\ &= \{\varphi | \Sigma \cup Q \vdash \varphi\} \\ &= \text{Teor}(\Sigma \cup Q), \end{aligned}$$

lo cuál es una contradicción.

2. φ_e como en el punto anterior no se puede demostrar.

□

1.142 Corolario. *El problema de la validez es indecidible, es decir,* $\{\varphi | \vdash \varphi\}$ *no es computable.*

1.143 Observación. *Sea* $\varphi_1, \varphi_2, \ldots, \varphi_n, \ldots$ *una enumeración efectiva de los enunciados de* $\mathcal{L}_A$. $\psi_1(x), \ldots, \psi_n(x)$ *de las fórmulas. Dado un enunciado* ψ *denotamos por*

$$\ulcorner\psi\urcorner = \ulcorner e\urcorner \Longleftrightarrow \psi \text{ es } \varphi_e,$$

donde $\ulcorner\psi\urcorner$ *es el número de Gödel de* ψ.

1.144 Lema. *Para cada fórmula* $\theta(y)$, *existe un enunciado* η *tal que*

$$Q \vdash \theta[\ulcorner\eta\urcorner/y] \Longleftrightarrow \eta.$$

Demostración. Dada la fórmula $\theta(y)$, consideraremos la función

$$m \mapsto \ulcorner \psi_m[\mathbf{m}/x] \urcorner.$$

Esta función es computable, luego es $Q-$representable, es decir, existe la fórmula $\psi(x,y)$ tal que

$$Q \vdash \psi[\mathbf{m}/x, \mathbf{n}/y] \iff n = \ulcorner \psi_m[\mathbf{m}/x] \urcorner,$$

y

$$Q \vdash \neg\psi[\mathbf{m}/x, \mathbf{n}/y] \iff n \neq \ulcorner \psi_m[\mathbf{m}/x] \urcorner.$$

Definimos

$$\chi(x) \equiv \forall y(\psi(x,y) \implies \theta(y)).$$

Hacemos

$$\eta \equiv \chi[\ulcorner \chi \urcorner / x].$$

Entonces,

$$Q \vdash \psi[\ulcorner \chi \urcorner / x, y] \iff y = \ulcorner \chi[\ulcorner \chi \urcorner / x] \urcorner,$$

es decir,

$$Q \vdash \psi[\ulcorner \chi \urcorner / x, y] \iff y = \ulcorner \eta \urcorner. \tag{*}$$

Por otra parte,

$$\eta \equiv \forall y(\psi[\ulcorner \chi \urcorner / x, y] \implies \theta(y)). \tag{**}$$

De (*) y (**) tenemos que

$$Q \vdash \eta \iff \forall y(y = \ulcorner \eta \urcorner \implies \theta(y));$$

por lo tanto,

$$Q \vdash \eta \iff \theta[\ulcorner \eta \urcorner / y].$$

□

1.145 Definición. *(Aritmética de Peano)*

$$\mathrm{PA} = Q \cup \{(\varphi[\mathbf{0}/x] \wedge \forall x(\varphi(x) \implies \varphi[Sx/x])) \implies \forall x\varphi(x) | \varphi(x) \text{ es fórmula}\}.$$

Esta definición coinscide con la que daremos en el capítulo 3, sin embargo, es importante señalarla ahora para los últimos resultados.

1.146 Observación. *Sea Σ computable tal que $Q \subseteq \Sigma$. Consideramos*

$$\mathit{Teor}(\Sigma) = \{m | \Sigma \vdash \varphi_n\},$$

el cuál es computablemente enumerable. Por lo tanto, este conjunto es débilmente representable en Q, es decir, existe $\psi(x)$ tal que para cada $m \in \mathbf{n}$,

$$m \in \mathit{Teor}(\Sigma) \iff Q \vdash \psi[\mathbf{m}/x].$$

Cabe recalcar que esta última $\psi(x)$ se puede entender por "x es demostrable".

1.147 Definición. Definimos $\mathrm{Con}(\Sigma)$ como el enunciado $\neg\psi[\ulcorner \mathbf{0} = S\mathbf{0} \urcorner / x]$.

1.148 Teorema. *(Segundo teorema de incompletitud de Gödel)*
Si Σ *es consistente, computable y PA*$\subseteq \Sigma$*, entonces*

$$\Sigma \vdash Con(\Sigma).$$

Demostración. Le aplicamos el lema de la autorreferencia a $\neg\psi$, obtenemos η tal que

$$Q \vdash \eta \Longleftrightarrow \neg\psi[\ulcorner\eta\urcorner/x].$$

Sea e tal que $\eta \equiv \varphi_e$ ($\ulcorner\eta\urcorner = e$). Supongamos que $\Sigma \vdash \eta$, es decir, $\Sigma \vdash \varphi_e$. Entonces, $e \in \text{Teor}(\Sigma)$ lo que implica $Q \vdash \psi[\mathbf{e}/x]$. Por otra parte, $\Sigma \vdash \eta \Longleftrightarrow \neg\psi[\ulcorner\eta\urcorner/x]$, $Q \vdash \psi[\mathbf{e}/x]$, por lo tanto:

$$\Sigma \vdash \neg\psi[\ulcorner\eta\urcorner/x] \wedge \Sigma \vdash \psi[\mathbf{e}/x],$$

$$\Sigma \vdash \psi[\mathbf{e}/x] \wedge \Sigma \vdash \psi[\mathbf{e}/x].$$

Esto contradice la consistencia de Σ. Luego,

$$\Sigma \nvdash \eta.$$

□

Podemos observar que en el teorema anterior, la proposición η se puede entender como *"yo no soy demostrable"*.

Capítulo 2

Sucesiones e hidras

En este capítulo se presentan las sucesiones de Goodstein, y el teorema central que protagonizan dichas sucesiones.[1] Así mismo, se presentan las hidras y un teorema similar al de Goodstein, que determina como deben abordarse las hidras para evitar catastrofes.[5]

2.1. Sucesiones de Goodstein

2.1 Teorema. *(Forma normal de Cantor)*
Sean $\alpha, \beta \in ON$ tales que $1 < \alpha \leqslant \beta$. Entonces existe una única k y únicos $\gamma_0, \ldots, \gamma_{k-1}$ y $\delta_0, \ldots, \delta_{k-1}$ con $\gamma_0 > \gamma_1 > \cdots > \gamma_{k-1}$ y $0 < \delta_i < \alpha$ para $i < k$ tal que

$$\beta = \alpha^{\gamma_0} \cdot \delta_0 + \alpha^{\gamma_1} \cdot \delta_1 + \cdots + \alpha^{\gamma_{k-1}} \cdot \delta_{k-1} \tag{5}$$

Demostración. Sea $\alpha > 0$, fijo. Por inducción sobre $\beta \geqslant 0$, mostremos la existencia de una expansión como en (5). Si $\beta = 1$, entonces $\alpha^0 \cdot 1$ es la expansión deseada. Asumamos que $\beta > 1$, y que una expansión como en (5) existe para cada η tal que $1 \leqslant \eta < \beta$. SEa $\Gamma = \{\gamma | \alpha^\gamma \leqslant \beta\}$.
Afirmamos que el conjunto Γ tiene un elemento máximal. En efecto, supongase que no lo tiene y sea $\gamma_0 = \bigcup \Gamma$. Como se satisface (H), γ_0 es un ordinal límite y $\gamma_0 \notin \Gamma$. Por otro lado, por definición:

$$\alpha^{\gamma_0} = \bigcup \{\alpha^\gamma | \gamma \in \gamma_0\} = \bigcup \{\alpha^\gamma | \gamma \in \Gamma\} \subseteq \beta.$$

Por la proposición 1.18, $\alpha^{\gamma_0} \leqslant \beta$, y entonces $\gamma_0 \in \Gamma$, lo cuál es una contradicción. Ahora, sea γ_0 el ordinal más grande en Γ. Por el corolario 1.50, existen los ordinales $\delta_0 > 0$ y $\beta_1 < \beta$ tal que $\beta = \alpha^{\gamma_0} \cdot \delta_0 + \beta_1$. Notemos que $\delta_0 < \alpha$, pues en caso contrario

$$\beta = \alpha^{\gamma_0} \cdot \delta_0 + \beta_1 \geqslant \alpha^{\gamma_0} \cdot \delta_0 \geqslant \alpha^{\gamma_0 + 1},$$

lo que contradice la elección de γ_0. Ahora bien, si $\beta_1 = 0$, entonces $\alpha^{\gamma_0} \cdot \delta_0$ es la expansión deseada. Por otro lado; si $\beta > 0$, entonces, por hipótesis de inducción, β_1 tiene una expansión como en (5); es decir, $\beta_1 = \alpha^{\gamma_1} \cdot \delta_1 + \cdots + \alpha^{\gamma_{k-1}} \cdot \delta_{k-1}$ con $\gamma_1 > \gamma_2 > \cdots > \gamma_{k-1}$ y $0 < \delta_i < \alpha$, para $0 < i < k$. Notemos que $\alpha^{\gamma_1} \leqslant \beta_1 < \beta$, por lo que $\gamma_1 \in \Gamma$, luego $\gamma_1 < \gamma_0$. Así, añadiendo el termino $\alpha^{\gamma_0} \cdot \delta_0$ a la izquierda de la expansión β_1, obtenemos la expansión deseada para β. Ahora, mostremos la unicidad: supongamos las siguientes expansiones:

$$\beta = \alpha^{\gamma_0} \cdot \delta_0 + \alpha^{\gamma_1} \cdot \delta_1 + \cdots + \alpha^{\gamma_{k-1}} \cdot \delta_{k-1};$$

$$\beta = \alpha^{\gamma_0} \cdot \delta'_0 + \alpha^{\gamma_1} \cdot \delta'_1 + \cdots + \alpha^{\gamma_{k-1}} \cdot \delta'_{k-1},$$

donde $\gamma_0 > \gamma_1 > \cdots > \gamma_{k-1}$, $\alpha > \delta_i, \delta'_i$ para $i < k$, y máx $\{\delta_0, \delta'_0\} > 0$ (pues, por asumir que $\delta_i = \delta'_i = 0$, podemos asumir que la secuencia de exponentes es la misma en ambas expansiones), Más aún, si $\delta_0 = \delta'_0$, entonces $\beta_1 = \beta = \alpha^{\gamma_0} \cdot \delta'_0 + \alpha^{\gamma_1} \cdot \delta'_1 + \cdots + \alpha^{\gamma_{k-1}} \cdot \delta'_{k-1}$ es el más pequeño ordinal con dos expansiones diferentes, lo cuál contradice la elección de β, por lo que podemos suponer $\delta_0 \neq \delta'_0$. Sin perdida de generalidad, $\delta_0 < \delta'_0$. Pero entonces:

$$\begin{aligned}
\beta &= \alpha^{\gamma_0} \cdot \delta_0 + \alpha^{\gamma_1} \cdot \delta_1 + \cdots + \alpha^{\gamma_{k-1}} \cdot \delta_{k-1} \\
&< \alpha^{\gamma_0} \cdot \delta_0 + \alpha^{\gamma_1} \cdot \delta_1 + \cdots + \alpha^{\gamma_{k-1}} \cdot \alpha \text{ (pues } \delta_{k-1<\alpha}) \\
&= \alpha^{\gamma_0} \cdot \delta_0 + \alpha^{\gamma_1} \cdot \delta_1 + \cdots + \alpha^{\gamma_{k-1}+1} \\
&\leqslant \alpha^{\gamma_0} \cdot \delta_0 + \alpha^{\gamma_1} \cdot \delta_1 + \cdots + \alpha^{\gamma_{k-2}} \cdot \delta_{k-2} + \alpha^{\gamma_{k-2}} \text{ (pues } \gamma_{k-1} + 1 \leqslant \gamma_{k-2}) \\
&= \alpha^{\gamma_0} \cdot \delta_0 + \alpha^{\gamma_1} \cdot \delta_1 + \cdots + \alpha^{\gamma_{k-2}} (\delta_{k-2} + 1) \\
&\leqslant \alpha^{\gamma_0} \cdot \delta_0 + \alpha^{\gamma_1} \cdot \delta_1 + \cdots + \alpha^{\gamma_{k-2}} \alpha \text{ (pues } \delta_{k-2} + 1 \leqslant \alpha) \\
&\leqslant \cdots \leqslant \alpha^{\gamma_0} \cdot (\delta_0 + 1) \leqslant \alpha^{\gamma_0} \cdot \delta'_0 \text{ (pues } \delta_0 + 1 \leqslant \delta'_0) \\
&\leqslant \alpha^{\gamma_0} \cdot \delta'_0 + \alpha^{\gamma_1} \cdot \delta'_1 + \cdots + \alpha^{\gamma_{k-1}} \cdot \delta'_{k-1} = \beta;
\end{aligned}$$

lo que es una contradicción. □

Un concepto útil será el de **super base** n, donde en ninguna parte de la expansión aparecen números mayores a n, es decir, si tenemos una representación en base 2:

$$27 = 2^4 + 2^3 + 2^1 + 2^0;$$

entonces, la representación en super base 2 es:

$$27 = 2^{(2^2)} + 2^{(2^1+1)} + 2^1 + 2^0.$$

2.2 Definición. (Operador salto de base)
Para cada $n < \omega$, con $n \geqslant 2$, sea $S_n : \omega \longrightarrow \omega$ la función definida por recursividad:

$$S_n(k) = k, \text{ si } k < n;$$

$$S_n(k \cdot n^t + b) = k(n+1)^{S_n(t)} + S_n(b), \text{ si } k < n, b < n^t, t \geqslant 1.$$

2.3 Definición. Para cada $n < \omega$, con $n \geqslant 2$, sea $f_n : \omega \longrightarrow \omega_1$ la función definida por recursividad:

$$f_n(k) = k, \text{ para } k < n$$

$$f_n(k \cdot n^t + b) = \omega^{f_n(t)} \cdot k + f_n(b), \text{ para } k < n, b < n^t, t \geqslant 1.$$

2.4 Proposición. *Para $m, n, k \in \omega$,*

- $k < m \Longrightarrow f_n(k) < f_n(m)$.
- $(\forall n, k < \omega \wedge n \geqslant 2)(f_{n+1}(S_n(k)) = f_n(k))$.

2.5 Definición. (Sucesiones de Goodstein)
Para cada $n < \omega$, con $n \geqslant 1$, definimos $g_n : \omega \longrightarrow \omega$ dada por:

$$g_1(m) = m;$$

$$g_{n+1}(m) = \begin{cases} S_{n+1}(g_n(m)) - 1, & \text{si } g_n(m) > 0 \\ 0, & \text{cualquier otro caso.} \end{cases}$$

2.6 Teorema. *(Goodstein)*

$$(\forall m < \omega)(\exists n \geqslant 1)(g_n(m) = 0)$$

Demostración. Sea $m < \omega$, fijo. Consideremos la sucesión:

$$(f_{n+1}(g_n(m)))_{1 \leqslant n < \omega}.$$

Como $g_{n+1}(m) > 0$, de acuerdo con la definición de $g_{n+1}(m)$, tenemos que

$$f_{n+2}(g_{n+1}(m)) = f_{n+2}(S_{n+1}(g_n(m)) - 1).$$

Por el primer inciso de la proposición 2.4, tenemos:

$$f_{n+2}(S_{n+1}(g_n(m) - 1)) < f_{n+2}(S_{n+1}(g_n(m))),$$

y del segundo inciso de la proposición 2.4, tenemos

$$f_{n+2}(S_{n+1}(g_n(m))) = f_{n+1}(g_n(m)).$$

Entonces,

$$f_{n+2}(g_{n+1}(m)) < f_{n+1}(g_n(m)).$$

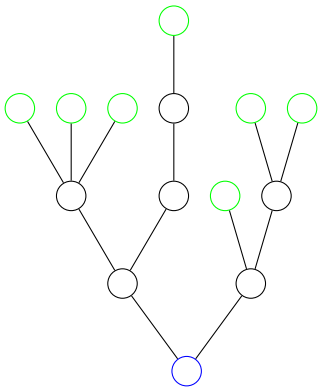
Como no hay secuencias decrecientes infinitas de ordinales, para una n suficientemente grande, tendremos $g_n(m) = 0$. □

2.2. Hidras asociadas a ordinales

A continuación presentaremos un concepto el cuál es de suma importancia para el estudio de los ordinales y, sobre todo, de las sucesiones de Goodstein.

2.7 Definición. Una *hidra* es un árbol fínito el cuál puede entenderse como una colección de aristas, cada uno unido a dos nodos, para los cuales cada nodo está conectado por un único camino de aristas a un nodo fijo llamado *raíz*. Un *nodo cima* de una hidra es uno el cuál es un nodo conectado a una sola arista, y no es la raíz. Una *cabeza* de la hidra es un nodo cima junto con su arista adjunta.

2.8 Ejemplo. Observemos el siguiente ejemplo de hidra:



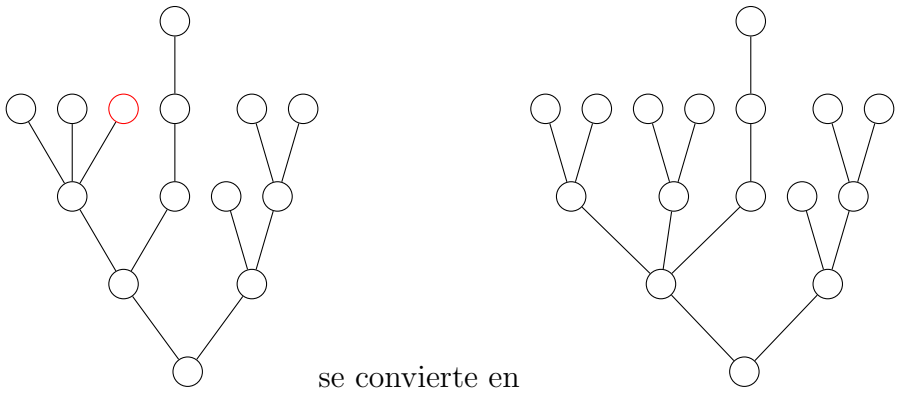
ejemplo de hidra

Donde el nodo azul es la raíz y los verdes los nodos cima, los cuales, junto con sus respectivas únicas aristas, forman las cabezas de la hidra.

Siguiendo la metafora con respecto a la mitología griega, en la batalla de Hercules contra la hidra; en la instancia n, después de Hercules cortar una cabeza de la hidra, de esta creceran n nuevas cabezas. Así pues, al trabajar con nuestras hidras, tendremos un comportamiento similar.

2.9 Definición. (Algoritmo del crecimiento de una cabeza)
Al cortarle una cabeza a una hidra, la hidra se comportará de la siguiente manera:
Desde el nodo que solía estar conectado a la cabeza que acaba de ser cortada, avanza un arista hacia la raíz hasta alcanzar el siguiente nodo de la red. Desde este nodo, brotan n réplicas de la parte de la hidra (después de la decapitación) que está *por encima* de la arista recién recorrida; en otras palabras, aquellos nodos y aristas por los cuales, para llegar a la raíz, sería necesario atravesar dicha arista. Si la cabeza recién cortada tenía la raíz como uno de sus nodos, no se genera una nueva cabeza.

2.10 Ejemplo. Observemos el lo que pasa al cortar la cabeza de una hidra:



ejemplo del cambio al cortar una cabeza de una hidra

En este caso, se ha cortado la cabeza asociada al nodo cima señalado en rojo.

Hercules gana la batalla si, después de un número finito de instancias, no queda nada de la hidra más que su raíz.

2.11 Definición. Una estrategia es una función la cuál determina cuál cabeza será cortada en cada instancia de cualquier batalla. Una estrategia se dice ganadora si, en un número finito de instancias, no queda nada más de la hidra que su raíz.

Ahora, la razón por la que las hidras son un concepto importante en nuestro estudio viene del hecho de que podemos asignarle a cada hidra un ordinal.

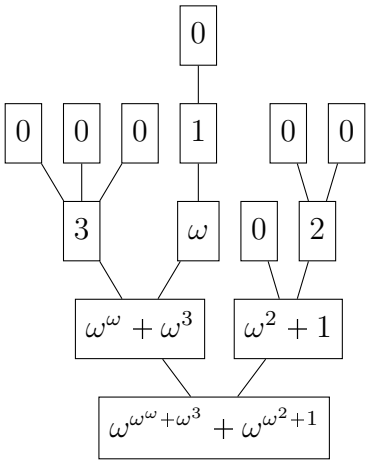
2.12 Definición. El ordinal asociado a un hidra viene dado por las siguientes reglas:

I A cada nodo cima le asignamos el 0

II Al resto de nodos les asignamos $\omega^{\alpha_1} + \cdots + \omega^{\alpha_n}$, donde $\alpha_1 \geqslant \cdots \geqslant \alpha_n$ son los ordinales asignados a los nodos inmediatamente *superiores* (es decir, por los que habría que pasar para llegar a un nodo cima).

III El ordinal asociado a la hidra será el asignado a su raíz.

2.13 Ejemplo. A continuación, mostremos cuál es el ordinal del ejemplo 2.8:

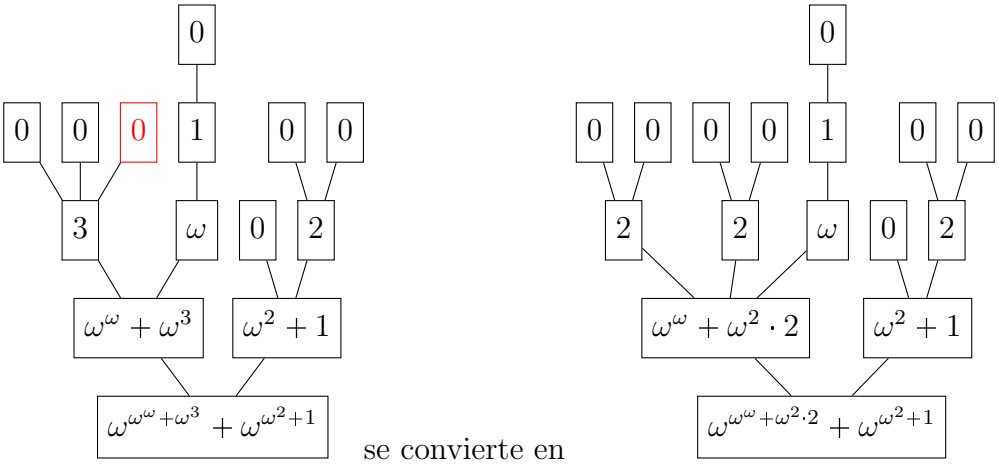


ejemplo de asignación de ordinales a una hidra

Así pues, el ordinal asociado a la hidra del ejemplo 2.8 es $\omega^{\omega^{\omega}+\omega^3}+\omega^{\omega^2+1}$.

En particular, cada uno de estos ordinales tiene que ser menor a ε_0, por el hecho de que las hidras son árboles finitos. Por otro lado, observemos lo que pasa con el ordinal asociado cuando se corta una cabeza de una hidra.

2.14 Ejemplo. El cambio en el ordinal después de cortar una cabeza:



ejemplo del cambio al cortar una cabeza de una hidra

En este caso, al cortar la cabeza asociada al nodo rojo, hemos obtenido el sigueinte cambio:

$$\omega^{\omega^{\omega}+\omega^3}+\omega^{\omega^2+1} \longrightarrow \omega^{\omega^{\omega}+\omega^2\cdot 2}+\omega^{\omega^2+1}.$$

Así mismo, es importante observar que el ordinal resultante es estrictamente menor que el original. Si bien esto no es una prueba, es un preambulo de un resultado futuro.

2.15 Definición. Para cualquier estrategia σ, definimos una operación $G_\sigma : \varepsilon_0 \times \omega \longrightarrow \varepsilon_0$, explicitamente escrita como $G_\sigma(\alpha, n)$, la cuál mapea el ordinal asociado a la hidra después de su instancia $n-1$, al ordinal de la hidra después después de la instancia n, donde σ es la estrategia utilizada.

Ahora, demostraremos un lema de suma importancia en el entendimiento de las estrategias contra las hidras.

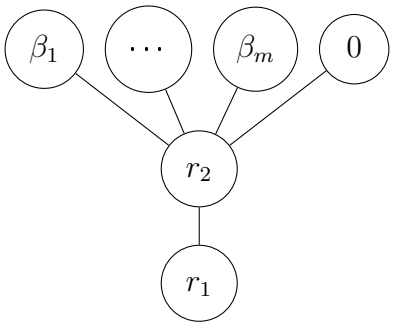
2.16 Lema. *Para toda estrategia σ, para todo ordinal $0 < \alpha < \varepsilon_0$, y para toda $n \in \omega$, tenemos*

$$G_\sigma(\alpha, n) < \alpha.$$

Demostración. Sea $\alpha \in \mathrm{ON}$ y σ una estrategía. Observemos que si nuestra hidra está asociada a un ordinal finito, todos los nodos que no son raices son nodos cima, por lo que al cortar una cabeza, no crecerá ninguna más, luego, para cada n:

$$G_\sigma(\alpha, n) = \alpha - 1 < \alpha.$$

Por otro lado, consideremos el caso en el que crecerán ramas cuando una cabeza es cortada: en tal caso, sólo es necesario fijarnos en nodo a partir de cuál crecerán las copias. Esto es de la forma siguiente:



Donde el nodo asociado al 0 es la cabeza que se cortará (siguiendo la estrategía σ), r_1 el nodo a partir del cuál crecerán las copias y los m nodos de la izquierda están asociados a m ordinales menores que ε_0. Sin perdida de generalidad, asumimos que estos ordinales están en orden de tal forma que

$$r_2 = \omega^{\beta_1} + \cdots + \omega^{\beta_m} + 1.$$

Luego,

$$r_1 = \omega^{\omega^{\beta_1} + \cdots + \omega^{\beta_m} + 1} = \omega^{\omega^{\beta_1} + \cdots + \omega^{\beta_m}} \cdot \omega.$$

Así pues, para cada $n \in \omega$, tenemos:

$$G_\sigma(r_1, n) = \omega^{\omega^{\beta_1} + \cdots + \omega^{\beta_m}} \cdot (n+1) < \omega^{\omega^{\beta_1} + \cdots + \omega^{\beta_m}} \cdot \omega.$$

Así, $G_\sigma(r_1, n) < r_1$. De aquí, si r_1 es raíz, hemos terminado. En caso de que r_1 no sea raíz, al menos hay un nodo abajo de r_1, de tal forma que en el ordinal asociado a α, aparezca un sumando (o un exponente) de la forma ω^{r_1} y en la de $G_\sigma(\alpha, n)$ uno de la forma $\omega^{G_\sigma(r_1, n)}$. Luego, como el orden se preserva por potencias (o sumandos) se tiene lo que se quería demostrar. □

2.17 Teorema. *Toda estrategía es una estrategía ganadora.*

Demostración. Consideremos la función $A_{(\alpha,\sigma)} : \omega \longrightarrow \varepsilon_0$, dada por:

$$A_{(\alpha,\sigma)}(n) = G_\sigma(\alpha, n).$$

Del lema2.16, tenemos que $A_{(\alpha.\sigma)}$ es una sucesión decreciente de ordinales. Ahora, del hecho de que no hay secuencias decrecientes infinitas de ordinales, para un m suficientemente grande, $A_{(\alpha,\sigma)}(m)$ es la hidra que consta únicamente de su raíz. Esto concluye el teorema. □

Capítulo 3

Sistema axiomatico

En el presente capítulo presentaremos el sistema axiomatico propuesto por Peano, el cuál es el sistema en el que pretendemos demostrar que el teorema de Goodstein es indemostrable. Así mismo, en este capítulo demostraremos todo aquello que tiene que ver con el modelo de los números naturales que sea importante para nuestros obejtivos.

3.1. Los axiomas de Peano

En la siguiente sección se formalizarán algunos resultados ya vistos en el capítulo 3, así como se explicará su importancia fundamental en el trabajo al señalar lo que es un modelo estandar y un modelo no estandar. [6]

3.1 Definición. La siguiente lista de proposiciones son conocidos como **los axiomas de Peano**, *la axiomatica de Peano* o los axiomas de *la aritmética de Peano (PA)*:

1. $\forall x \quad \neg(\mathfrak{o} = Sx)$,
2. $\forall x \forall y \quad (Sx = Sy \Longrightarrow x = y)$,
3. $\forall x \quad \neg(x < \mathfrak{o})$,
4. $\forall x \forall y \quad (x < Sy \Longrightarrow (x < y \vee x = y))$,
5. $\forall x \forall y \quad (x < y \vee x = y \vee y < x)$,
6. $\forall x \quad (x + \mathfrak{o} = x)$,
7. $\forall x \forall y \quad (x + Sy = S(x + y))$,
8. $\forall x \quad (x \cdot \mathfrak{o} = \mathfrak{o})$,
9. $\forall x \forall y \quad (x \cdot Sy = x \cdot y + x)$,
10. $(\varphi[\mathfrak{o}/x] \wedge \forall x(\varphi \Longrightarrow \varphi[Sx/x])) \Longrightarrow \forall x \varphi$; con $\varphi(x)$ una formula.

3.2 Observación. *La lista anterior consiste de 9 axiomas y un esquema de axioma, es decir, una infinidad de axiomas (pues existen una infinidad de formulas en el lenguaje de la aritmetica).*

3.3 Definición. Consideremos la estructura

$$\mathcal{N} = (\omega, +, \cdot, S, <, 0),$$

la cuál llamaremos *los números naturales*. También se le conoce como *modelo estandar de la axiomatica de Peano.*

Consideremos que esta estrucutra se define en función de los axiomas de Peano, de forma en que satisfaga todos.

3.4 Observación. *Vale la pena mencionar que cualquier otro modelo que satisfaga PA será llamado un* ***modelo no estandar*** *de la axiomatica de Peano.*

3.5 Definición. *(Jerarquia de Kleene-Mostowski)*

- Si una fórmula ϕ tiene o bien cuantificadores acotados, o ningún tipo de cuantificadores, entonces decimos que ϕ es del tipo Σ_0, Π_0 y Δ_0.
- Si una fórmula ϕ que es equivalente a una fórmula $\exists m_1 \exists m_2 \cdots \exists m_k \psi$, donde ψ es Δ_0, entonces ϕ es del tipo Σ_1.
- Si una fórmula ϕ que es equivalente a una fórmula $\forall m_1 \forall m_2 \cdots \forall m_k \psi$, donde ψ es Δ_0, entonces ϕ es del tipo Π_1.
- Si una formula ϕ es tanto Σ_1 como Π_1, entonces ϕ también es Δ_1.

Notese que en la definición anterior, dicha k puede valer 0, por lo que $\Delta_0 \subseteq \Sigma_1 \cap \Pi_1$.

3.2. Ultraproductos

En este espacio mostraremos las estructuras conocidas como ultraproductos y mostraremos como construir modelos no estandar de la axiomatica de Peano utilizando dichas estructuras. Así mismo, presentaremos el teorema fundamental de los ultraproductos sustentar afirmaciones sobre dichos modelos.[7]

3.6 Definición. Sea X un conjunto. Entonces el producto directo de $\{\omega\}_{x \in X}$ está dado por

$$\prod_{x \in X} \omega := \{f : X \longrightarrow \omega\}$$

3.7 Definición. Definimos la relación $\sim$ en $\prod_{x \in X} \omega$ de la siguiente forma: para cada $f, g \in \prod_{x \in X} \omega$,

$$f \sim g \Longleftrightarrow \{x \in X | f(x) = g(x)\} \in u$$

3.8 Proposición. *La relación $\sim$ es una relación de equivalencia.*

Demostración. Consideremos $f, g, h \in \prod_{x \in X} \omega$. Entonces,

- Reflexividad: observemos que

  $$\{x \in X | f(x) = f(x)\} = X \in u,$$

  por ser u ultrafiltro. Luego $f \sim f$.

- Simetría:

$$f \sim g \Longrightarrow \{x \in X | f(x) = g(x)\} \in u \Longrightarrow \{x \in X | g(x) = f(x)\} \in u \Longrightarrow g \sim f$$

- Transitividad: notemos que

$$(f \sim g \wedge g \sim h) \Longrightarrow (\{x \in X | f(x) = g(x)\} \in u \wedge \{x \in X | g(x) = h(x)\} \in u).$$

Luego, $\{x \in X | f(x) = g(x)\} \cap \{x \in X | g(x) = h(x)\} \in u$, pero

$$\{x \in X | f(x) = g(x)\} \cap \{x \in X | g(x) = h(x)\} \subseteq \{x \in X | f(x) = h(x)\},$$

y como u es cerrado por arriba, por ser ultrafiltro, tenemos que

$$\{x \in X | f(x) = h(x)\} \in u.$$

□

3.9 Definición. Sea X un conjunto y u un ultrafiltro sobre X. Definimos el ultraproducto de ω sobre u como:

$$\prod {}^{\omega}\!/_{u} := {}^{(\Pi_{x \in X}\, \omega)}\!/_{\sim}$$

3.10 Definición. Definimos la función

$$\begin{array}{c} c_n : X \longrightarrow \omega \\ x \longrightarrow n, \end{array}$$

es decir, la función constante n.

3.11 Proposición. *La función*

$$\begin{array}{c} \iota : \omega \longrightarrow \prod {}^{\omega}\!/_{u} \\ n \mapsto [c_n]_{\sim}, \end{array}$$

es inyectiva.

Demostración. Sean $n, m \in \omega$ tal que $n \neq m$. Entonces,

$$(\forall x \in X)(c_n(x) \neq c_m(x)),$$

es decir,

$$\{x \in X | c_n(x) = c_m(x)\} = \varnothing.$$

Luego, $\varnothing \notin u$, por lo que $c_n \not\sim c_m$, es decir;

$$[c_n]_{\sim} \neq [c_m]_{\sim}.$$

□

La proposición anterior nos permite hablar de elementos de ω en el ultraproducto, refiriendonos realmente a la imagen de los elementos de ω encajados en el ultraproducto.

3.12 Teorema. *La función sucesor en el ultraproducto, dada por*

$$\begin{array}{c} S_{\sim} : \prod {}^{\omega}\!/_{u} \longrightarrow \prod {}^{\omega}\!/_{u} \\ [f]_{\sim} \mapsto [S \circ f]_{\sim}, \end{array}$$

está bien definida.

Demostración. Sean $f, g \in \prod_{x\in X} \omega$ tales que $f \sim g$, es decir,

$$\{x \in X | f(x) = g(x)\} \in u.$$

Luego, notemos que si $y \in X$ es tal que $f(y) = g(y)$, entonces también se cumple que $S(f(y)) = S(g(y))$. Luego,

$$\{x \in X | f(x) = g(x)\} \subseteq \{x \in X | S \circ f(x) = S \circ g(x)\}. \tag{S}$$

Así, como los ultrafiltros son cerrador por arriba,

$$\{x \in X | S \circ f(x) = S \circ g(x)\} \in u,$$

es decir, $[S \circ f]_\sim = [S \circ g]_\sim$, justo lo que se quería demostrar. □

Nos referiremos como S indistintamente a S como a $S_\sim$, por simplicidad.

3.13 Teorema. *La función suma en el ultraproducto, dada por*

$$\begin{array}{c} +_\sim : \left(\prod {}^{\omega}\!/_{u}\right)^2 \longrightarrow \prod {}^{\omega}\!/_{u} \\ ([f]_\sim, [g]_\sim) \mapsto [f+g]_\sim, \end{array}$$

está bien definida.

Demostración. Sean $f, g, h, k \in \prod_{x\in X} \omega$ tales que $f \sim h$ y $g \sim k$. Observemos que si $y, z \in X$ son tales que $f(y) = h(y)$ y $g(z) = k(z)$, entonces

$$f(y) + g(z) = h(y) + k(z).$$

Consideremos los conjuntos:

$$\{x \in X | f(x) = h(x)\} \wedge \{x \in X | g(x) = k(x)\}.$$

Ambos conjuntos están en u (por como se tomaron las funciones). Afirmamos que:

$$\{x \in X | f(x) = h(x)\} \cap \{x \in X | g(x) = k(x)\} \subseteq \{x \in X | (f+g)(x) = (h+k)(x)\}$$

En efecto, sea $x \in \{x \in X | f(x) = h(x)\} \cap \{x \in X | g(x) = k(x)\}$, entonces

$$f(x) = h(x) \wedge g(x) = k(x).$$

Luego, tenemos que $f(x) + g(x) = h(x) + k(x)$, y por lo tanto,

$$x \in \{x \in X | (f+g)(x) = (h+k)(x)\}.$$

Así, recordando que los ultrafiltros son cerrados por intersecciones, tenemos que

$$\{x \in X | f(x) = h(x)\} \cap \{x \in X | g(x) = k(x)\} \in u,$$

más aún, recordando que los ultrafiltros son cerrador por arriba, tenemos que

$$\{x \in X | (f+g)(x) = (h+k)(x)\} \in u,$$

es decir

$$[f+g]_\sim = [h+k]_\sim,$$

justo lo que se quería demostrar. □

3.14 Teorema. *La función producto en el ultraproducto, dada por*

$$\begin{aligned} \cdot_\sim : \left(\prod {}^{\omega}\!/_{u}\right)^2 &\longrightarrow \prod {}^{\omega}\!/_{u} \\ ([f]_\sim, [g]_\sim) &\mapsto [f \cdot g]_\sim, \end{aligned}$$

está bien definida.

Demostración. La prueba es completamente análoga a la del teorema anterior. □

3.15 Definición. Definimos la relación $<_\sim$ una relación en $\prod {}^{\omega}\!/_{u}$ de la siguiente forma: para cada $[f]_\sim, [g]_\sim \in \prod {}^{\omega}\!/_{u}$,

$$[f]_\sim <_\sim [g]_\sim \iff \{x \in X | f(x) < g(x)\} \in u$$

3.16 Proposición. *La relación $<_\sim$ es una relación de orden parcial total estricto.*

Demostración. Demostramos las siguientes propiedades:

- Antireflexivo: Sea $[f]_\sim \in \prod {}^{\omega}\!/_{u}$, entonces
$$\{x \in X | f(x) < f(x)\} = \varnothing$$
Luego, como $\varnothing \notin u$, tenemos que $[f]_\sim \not<_\sim [f]_\sim$.
- Transitividad: Sean $[f]_\sim, [g]_\sim, [h]_\sim \in \prod {}^{\omega}\!/_{u}$. Si $[f]_\sim <_\sim [g]_\sim$ y $[g]_\sim <_\sim [h]_\sim$, tenemos que:
$$\{x \in X | f(x) < g(x)\} \in u \wedge \{x \in X | g(x) < h(x)\} \in u.$$
Ahora, afirmamos que:
$$\{x \in X | f(x) < g(x)\} \cap \{x \in X | g(x) < h(x)\} \subseteq \{x \in X | f(x) < h(x)\}.$$
En efecto, pues si x es tal que $f(x) < g(x)$ y $g(x) < h(x)$, entonces x es tal que $f(x) < h(x)$. Esto demuestra la contención que queríamos. Luego, como u es cerrado bajo intersecciones,
$$\{x \in X | f(x) < g(x)\} \cap \{x \in X | g(x) < h(x)\} \in u,$$
y, nuevamente, como u es cerrado por arriba, tenemos que
$$\{x \in X | f(x) < h(x)\} \in u.$$
Luego,
$$[f]_\sim < [h]_\sim.$$
- Tricotomía: Sean $[f]_\sim, [g]_\sim \in \prod {}^{\omega}\!/_{u}$. Si $[f]_\sim = [g]_\sim$, entonces hemos terminado. En caso contrario,
$$\{x \in X | f(x) = g(x)\} \notin u.$$
Es decir,
$$\{x \in X | f(x) \neq g(x)\} \in u,$$
Pero, tenemos que
$$\{x \in X | f(x) < g(x)\} \cup \{x \in X | g(x) < f(x)\} = \{x \in X | f(x) \neq g(x)\}.$$
Por propiedades de ultrafiltros, tenemos que:
$$\{x \in X | f(x) < g(x)\} \in u \vee \{x \in X | g(x) < f(x)\} \in u;$$
es decir,
$$[f]_\sim <_\sim [g]_\sim \vee [g]_\sim <_\sim [f]_\sim.$$

Esto concluye la demostración. □

Nos referiremos como $<$ indistintamente a $<$ como a $<_\sim$, por simplicidad.

3.17 Definición. Definimos la estructura

$$\left(\prod {}^{\omega}\!/_{u}, +_\sim, \cdot_\sim, S_\sim, <_\sim, [c_1]_\sim\right),$$

como la del ultraproducto de los naturales con respecto a u, o como la de *la aritmética del ultraproducto de* ω.

Antes de proseguir con el siguiente teorema importante, se mostrará un resultado que ayudará a mostrar la idea intuitiva de dicho teorema.

3.18 Proposición.

$$\left(\forall [f]_\sim \in \prod {}^{\omega}\!/_{u}\right)\left(\forall [g]_\sim \in \prod {}^{\omega}\!/_{u}\right)\left(S\left([f]_\sim\right) = S\left([g]_\sim\right) \Longrightarrow [f]_\sim = [g]_\sim\right)$$

Demostración. Sean $[f]_\sim, [g]_\sim \in \prod {}^{\omega}\!/_{u}$ tales que:

$$\{x \in X | S \circ f(x) = S \circ g(x)\} \in u,$$

es decir, $S([f]_\sim) = S([g]_\sim)$. Pero, si $x \in X$ es tal que

$$S(f(x)) = S(g(x)),$$

entonces, un teorema conocido es que $f(x) = g(x)$. Luego, tenemos que:

$$\{x \in X | S \circ f(x) = S \circ g(x)\} \subseteq \{x \in X | f(x) = g(x)\} \tag{S'}$$

Y como los ultrafiltros son cerrador por arriba, tenemos que:

$$\{x \in X | f(x) = g(x)\} \in u$$

Esto concluye el teorema. □

3.19 Observación. *De las ecuaciones* S *y* S' *se sigue que:*

$$\{x \in X | S \circ f(x) = S \circ g(x)\} = \{x \in X | f(x) = g(x)\}$$

El teorema anterior se podría interpretar como que la estructura del ultraproducto hereda el teorema de la estructura de los naturales. Esto pareciera indicar que la estructura de los ultraproductos heredará algunos cuantos teoremas de los naturales. El siguiente teorema nos indicará que tanto es esto verdad.

Observese que de los teoremas 3.12, 3.13 y 3.14 se sigue que lso términos en una estructura son términos en la otra, mientra que de la proposición 3.11 se sigue que el cero es término en ambas estructuras.

3.20 Teorema. *(Fundamental de los ultraproductos) (de Łoś)[7]*
Para cada φ*, formula en el lenguje de PA, con* $f_1, \ldots, f_n \in \prod_{x \in X} \omega$*:*

$$\left(\prod {}^{\omega}\!/_{u}, +_\sim, \cdot_\sim, S_\sim, <_\sim, [c_1]_\sim\right) \vDash \varphi[[f_1]_\sim, \ldots, [f_n]_\sim]$$

si, y sólo si

$$\{x \in X | (\omega, +, \cdot, S, <, 1) \vDash \varphi[f_1(x), \ldots, f_n(x)]\} \in u$$

Demostración. Procedemos por inducción sobre la complejidad de la fórmula φ (si bien, es probable que la fórmula φ contenga términos, los obviaremos para agilizar la escritura y lectura):
Primero, demostremos para las formulas atómicas:

- $\varphi \equiv t_1 = t_2$:
  Se sigue de la definición de la relación de equivalencia $\sim$.

- $\varphi \equiv t_1 < t_2$:
  Se sigue de la definición de la relación $<_\sim$.

Ahora supongamos que toda fórmula de complejidad menor a φ ya satisface el teorema, entonces los casos faltantes son:

- $\varphi \equiv \neg\psi$, para alguna fórmula ψ:
  Entonces, tenemos que:
  $$\left(\prod {}^{\omega}\!/_{u}, +_\sim, \cdot_\sim, S_\sim, <_\sim, [c_1]_\sim\right) \vDash \varphi,$$
  es equivalente a
  $$\left(\prod {}^{\omega}\!/_{u}, +_\sim, \cdot_\sim, S_\sim, <_\sim, [c_1]_\sim\right) \nvDash \psi,$$
  que también es equivalente, por hipótesis de inducción, a
  $$\{x \in X | (\omega, +, \cdot, S, <, 1) \vDash \psi(x)\} \notin u,$$
  y por propiedades del ultrafiltro (con respecto a los complementos), tenemos que esto es equivalente a
  $$\{x \in X | (\omega, +, \cdot, S, <, 1) \nvDash \psi(x)\} \in u,$$
  lo cuál, finalmente, es equivalente a
  $$\{x \in X | (\omega, +, \cdot, S, <, 1) \vDash \varphi(x)\} \in u.$$

- $\varphi \equiv (\psi_1 \vee \psi_2)$, para dos fórmulas ψ_1 y ψ_2:
  Entonces, tenemos que:
  $$\left(\prod {}^{\omega}\!/_{u}, +_\sim, \cdot_\sim, S_\sim, <_\sim, [c_1]_\sim\right) \vDash \psi_1 \vee \psi_2,$$
  lo cuál es equivalente a
  $$\left(\prod {}^{\omega}\!/_{u}, +_\sim, \cdot_\sim, S_\sim, <_\sim, [c_1]_\sim\right) \vDash \psi_1 \vee \left(\prod {}^{\omega}\!/_{u}, +_\sim, \cdot_\sim, S_\sim, <_\sim, [c_1]_\sim\right) \vDash \psi_2,$$
  y por hipótesis de inducción, tenemos que:
  $$\{x \in X | (\omega, +, \cdot, S, <, 1) \vDash \psi_1(x)\} \in u \vee \{x \in X | (\omega, +, \cdot, S, <, 1) \vDash \psi_2(x)\} \in u,$$
  pero, por propiedades de ultrafiltro, tenemos que:
  $$\{x \in X | (\omega, +, \cdot, S, <, 1) \vDash \psi_1(x)\} \cup \{x \in X | (\omega, +, \cdot, S, <, 1) \vDash \psi_2(x)\} \in u,$$
  pero, el conjunto de x que satisfacen ψ_1 o ψ_2 cumple
  $$\{x \in X | (\omega, +, \cdot, S, <, 1) \vDash \psi_1(x)\} \cup \{x \in X | (\omega, +, \cdot, S, <, 1) \vDash \psi_2(x)\}$$
  $$\subseteq \{x \in X | (\omega, +, \cdot, S, <, 1) \vDash \psi_1(x) \vee \psi_2(x)\},$$
  por lo que se concluye, dado que los ultrafiltros están cerrados por arriba:
  $$\{x \in X | (\omega, +, \cdot, S, <, 1) \vDash \psi_1(x) \vee \psi_2(x)\} \in u.$$

- $\varphi \equiv (\psi_1 \implies \psi_2)$, para dos fórmulas ψ_1 y ψ_2:
  Se sigue de que $\psi_1 \implies \psi_2 \equiv \neg\psi_1 \vee \psi_2$.

- $\varphi \equiv \exists y\psi(y)$, para alguna fórmula ψ:
  Supongamos que
  $$\left(\prod {}^{\omega}\!/_{u}, +_{\sim}, \cdot_{\sim}, S_{\sim}, <_{\sim}, [c_1]_{\sim}\right) \vDash \varphi,$$
  esto significa que existe alguna y tal que
  $$\left(\prod {}^{\omega}\!/_{u}, +_{\sim}, \cdot_{\sim}, S_{\sim}, <_{\sim}, [c_1]_{\sim}\right) \vDash \psi(y),$$
  y por hipótesis de inducción, esto significa que
  $$\left\{x \in X | (\omega, +, \cdot, S, <, 1) \vDash \psi(\iota^{-1}(y))\right\} \in u,$$
  lo cuál implica que:
  $$\{x \in X | (\omega, +, \cdot, S, <, 1) \vDash \varphi\} \in u.$$
  Por otro lado, si suponemos
  $$\{x \in X | (\omega, +, \cdot, S, <, 1) \vDash \varphi\} \in u,$$
  esto implica que podemos elegir una $y \in \prod {}^{\omega}\!/_{u}$ tal que:
  $$\left\{x \in X | (\omega, +, \cdot, S, <, 1) \vDash \psi(\iota^{-1}(y))\right\} \in u,$$
  y ya, esto implica de inmediato que:
  $$\left(\prod {}^{\omega}\!/_{u}, +_{\sim}, \cdot_{\sim}, S_{\sim}, <_{\sim}, [c_1]_{\sim}\right) \vDash \psi(y),$$
  lo cuál, finalmente, implica,
  $$\left(\prod {}^{\omega}\!/_{u}, +_{\sim}, \cdot_{\sim}, S_{\sim}, <_{\sim}, [c_1]_{\sim}\right) \vDash \varphi.$$

- $\varphi \equiv \forall y\psi(y)$, para alguna ψ:
  Se sigue de que $\forall y\psi(y) \equiv \neg\exists y\neg\psi(y)$.

□

Observemos la fuerza de este teorema; consideremos:

$$(\omega, +, \cdot, S, <, 1) \vDash (\nexists n \in \omega)(0 = S(n)).$$

Luego, para cada x en X,

$$(\omega, +, \cdot, S, <, 1) \vDash \left(\nexists f \in \prod_{x \in X} \omega\right)(0 = S(f(x))),$$

es decir,

$$X = \left\{x \in X | (\omega, +, \cdot, S, <, 1) \vDash \left(\nexists f \in \prod_{x \in X} \omega\right)(0 = S(f(x)))\right\} \in u$$

Por lo que, tenemos que:

$$\left(\prod {}^{\omega}\!/_{u}, +_{\sim}, \cdot_{\sim}, S_{\sim}, <_{\sim}, [c_1]_{\sim}\right) \vDash \left(\nexists f \in \prod_{x\in X} \omega\right) ([c_0]_{\sim} = [f]_{\sim})$$

Si se pone atención, este teorema permite heredar todas las formulas que se cumplen en los números naturales a la estrucutra del ultraproducto. Es decir, desde propiedades de los exponentes, hasta los axiomas de Peano, se satisfacen todos en la estructura de $\prod {}^{\omega}\!/_{u}$ (mientras que no hayan variables libres). Así, se tiene que $\prod {}^{\omega}\!/_{u}$ es un *modelo no estandar* de los axiomas de Peano.

3.21 Teorema. *Si u es un ultrafiltro principal sobre X, entonces*

$$\left(\prod {}^{\omega}\!/_{u}, +_{\sim}, \cdot_{\sim}, S_{\sim}, <_{\sim}, [c_1]_{\sim}\right) \cong (\omega, +, \cdot, S, <, 1)$$

Demostración. Dado que u es principal, existe $x_o \in X$ tal que:

$$u = \{A \in \mathscr{P}(X) | x_o \in A\}$$

Consideremos

$$\begin{aligned} \kappa : \prod {}^{\omega}\!/_{u} &\longrightarrow \omega \\ [f]_{\sim} &\mapsto f(x_o), \end{aligned}$$

y también consideremos las función definida en 3.11. Antes que nada, demostremos κ está bien definida: sean $f, g \in \prod {}^{\omega}\!/_{u}$ tales que $f \sim g$. Entonces, observemos que:

$$\{x \in X | f(x) = g(x)\} \in u \Longrightarrow x_o \in \{x \in X | f(x) = g(x)\} \Longrightarrow f(x_o) = g(x_o)$$

Por lo tanto, κ no depende de los representantes. Observemos que, $c_{f(x_o)} \sim f$. Luego, para cada $f \in \prod {}^{\omega}\!/_{u}$:

$$\iota \circ \kappa([f]_{\sim}) = \iota(\kappa([f]_{\sim})) = \iota(f(x_o)) = [c_{f(x_o)}]_{\sim} = [f]_{\sim}$$

Es decir,

$$\iota \circ \kappa = \mathrm{id}_{\prod {}^{\omega}\!/_{u}}.$$

Por otro lado, para cada $n \in \omega$,

$$\kappa \circ \iota(n) = \kappa(\iota(n)) = \kappa([c_n]_{\sim}) = c_n(x_o) = n,$$

luego,

$$\kappa \circ \iota = \mathrm{id}_{\omega}.$$

Esto nos demuestra que κ es la inversa de ι. Más aún, sean $n, m \in \omega$, entonces

$$(\forall x \in X)(c_{n+m}(x) = n + m = c_n + c_m),$$

y

$$(\forall x \in X)(c_{n\cdot m}(x) = n \cdot m = c_n \cdot c_m);$$

por lo que,

$$\iota(n + m) = [c_{n+m}]_{\sim} = [c_n + c_m]_{\sim} = [c_n]_{\sim} + [c_m]_{\sim} = \iota(c_n) + \iota(c_m),$$

y

$$\iota(n \cdot m) = [c_{n\cdot m}]_\sim = [c_n \cdot c_m]_\sim = [c_n]_\sim \cdot [c_m]_\sim = \iota(c_n) \cdot \iota(c_m).$$

Por lo que ι es isomorfismo bajo la suma y el producto. Más aún, para n elemento de ω,

$$(\forall x \in X)(c_{S(n)}(x) = S(n) = n + 1 = c_n(x) + c_1(x) = S(c_n(x)) = S \circ c_n(x)),$$

por lo que,

$$\iota(S(n)) = [c_{S(n)}]_\sim = [S \circ c_n]_\sim = S([c_n]_\sim) = S(\iota(n)).$$

Por lo que ι es isomorfismo bajo la función sucesora. Más aún, para cualesquiera $n, m \in \omega$ tales que $n < m$, tenemos que:

$$\{x \in X | c_n(x) < c_m(x)\} = X \in u,$$

por lo que

$$[c_n]_\sim < [c_m]_\sim.$$

De aquí, que ι es isomorfismo de orden y esto termina el teorema. □

Si se revisa cuidadosamente la demostración de 3.21, veremos que para cualquier ultrafiltro podemos asegurar que ι es monomorfismo para estas estructuras (de los naturales al ultraproducto). Más aún, el teorema anterior *es* un *si, y sólo si*, en el sentido de que si tenemos una estructura de ultraproducto isomorfa a los números naturales, entonces el ultraproducto se define con un ultrafiltro principal; o equivalentemente, si u no es ultrafiltro principal, entonces su estructura de ultraproducto no es isomorfa a los números naturales. Esto se sigue del siguiente teorema.

3.22 Teorema. *Sea u un ultrafiltro no principal sobre ω, entonces existe $h \in \prod_{n\in\omega} \omega$ tal que*

$$(\forall n \in \omega)([c_n]_\sim < [h]_\sim).$$

Demostración. Recordemos que:

$$\prod {}^{\omega}\!/_{u} = \{[f]_\sim | f : \omega \longrightarrow \omega\},$$

por lo que $\mathrm{id}_\omega \in \prod {}^{\omega}\!/_{u}$. Así, observemos que si existiera $n \in \omega$ tal que $[\mathrm{id}_\omega]_\sim < [c_n]_\sim$, entonces

$$K = \{k \in \omega | k < n\} = \{k \in \omega | \mathrm{id}(k) < c_n(k)\} \in u,$$

Pero K es un conjunto finito y por el teorema 1.63, u es principal, lo cuál es una contradicción. Luego, basta tomar $h = \mathrm{id}_\omega$ □

Así, si el ultreproducto definido por un ultrafiltro no principal fuera isomorfo a los números naturales, entonces existiría un elemento en los naturales que sería mayor a todos los naturales, lo cuál es absurdo. Así mismo, quizá sea bueno recordar que el teorema 1.67 garantiza la existencia de los ultrafiltros no principales.

Cabe recalcar lo siguiente: las clases o categorias Δ_0 son absolutas entre modelos y submodelos, es decir: si $N \subseteq M$ son modelos de PA, entonces

$$N \vDash \psi(x, y) \Longleftrightarrow M \vDash \psi(x, y),$$

para cualquier fórmula ψ. Este resultado es clásico en teorías de modelos, aunque requiere un desarrollo un poco más extenso, por lo que simplemente lo citamos. [8]

3.23 Teorema. *Para modelos de PA M y N tales que $M \subseteq N$, tenemos que:*

$$M \vDash \varphi \Longleftrightarrow N \vDash \varphi,$$

para φ del tipo Σ_1.

Demostración. Para el caso en que $\varphi \in \Delta_0$, es inmediato por la absolutez de Δ_0. Así, consideraremos expresiones de la forma $\exists y \psi(x, y)$.
Para la necesidad: supongamos

$$M \vDash \exists y \psi(a, y),$$

por lo que existe un b en M tal que:

$$M \vDash \psi(a, b).$$

Luego, por la absolutez de Δ_0,

$$N \vDash \psi(a, b),$$

por lo tanto,

$$N \vDash \exists y \psi(a, y).$$

Ahora, para la suficiencia: supongamos

$$N \vDash \exists y \psi(a, y),$$

entonces existe b en N al que

$$N \vDash \psi(a, b).$$

Como todos los cuantificadores están acotados en ψ, existe un testigo finito en el modelo, luego este es accesible por M; por lo tanto

$$M \vDash \psi(a, b), \text{ para algún } b \in M;$$

así pues:

$$M \vDash \exists y \psi(a, y).$$

□

Antes de terminar esta sección, mencionaremos un teorema de importancia capital en la teoría de los modelos no estandar.

3.24 Teorema. *(Principio de derramamiento) (overspill principle)*
Sea $\varphi(x)$ una fórmula (quizá con más parametros) en un modelo M no estandar. Si $\varphi(n)$ se satisface para cada n estandar de M, entonces existe $a \in M$ no estandar tal que $\varphi(a)$ se satisface en M.

Demostración. Supongamos que $\varphi(n)$ se satisface para cada n estandar, pero $\varphi(a)$ no se satisface para ningún a no estandar. Entonces, tenemos que

$$\omega = \{b \mid \varphi(b)\}.$$

Ento implica que, para cada $x \in X$,

$$(\omega, +, \cdot, S, <, 1) \vDash \omega = \left\{ f \in \prod_{x \in X} \omega \mid \varphi(f(x)) \right\},$$

es decir,

$$X = \left\{ x \in X \mid (\omega, +, \cdot, S, <, 1) \vDash \omega = \left\{ f \in \prod_{x \in X} \omega \mid \varphi(f(x)) \right\} \right\} \in u;$$

por lo que, por el teorema 3.20 tenemos que:

$$\left(\prod {}^{\omega}/_{u}, +_{\sim}, \cdot_{\sim}, S_{\sim}, <_{\sim}, [c_1]_{\sim} \right) \vDash M = \left\{ [f]_{\sim} \in \prod_{x \in X} \omega \mid \varphi([f]_{\sim}) \right\},$$

y como M no es estandar, tenemos que existe al menos una a no estandar en M, por lo que a satisfacería φ, lo cuál es una contradicción. □

El teorema anterior tiene una consecuencia muy curiosa como parte de su demostración.

3.25 Corolario. *El conjunto de los naturales es indefinible (en el sentido de 1.126) bajo los axiomas de Peano PA.*

Demostración. No existe una φ que pueda definir a los números naturales, como se vio en la demostración de 3.24, pues eso contradice el teorema 3.20. □

3.3. Conjuntos $\alpha-$grandes

En el siguiente capítulo desarrollaremos la teoria de conjuntos $\alpha-$grande; una poderosa teoría que será exageradamente útil en lo que resta del presente trabajo.

3.26 Definición. Definimos la operación $F : \varepsilon_0 \times \omega \longrightarrow \varepsilon_0$ como sigue:

$$F(\alpha, n) = \begin{cases} 0 & \text{si } \alpha = 0 \\ \beta & \text{si } \alpha = \beta + 1 \\ \omega^{\gamma+1} \cdot \beta + \omega^{\gamma} \cdot n & \text{si } \alpha = \omega^{\gamma+1} \cdot (\beta + 1) \\ \omega^{\delta}\beta + \omega^{F(\delta,n)} & \text{si } \alpha = \omega^{\delta} \cdot (\beta + 1) \wedge \delta \in \text{LIM} \end{cases}$$

Vale la pena observar que $F(\alpha, n) < \alpha$, para cualquier ordinal α. Más aún, F es inyectiva con respecto a su primer entrada; es decir:

$$F(\alpha, n) = F(\beta, n) \Longrightarrow \alpha = \beta.$$

3.27 Definición. Definiremos el concepto de $\alpha-$grande por inducción sobre $\alpha \in \varepsilon_0 \backslash \{0\}$ como sigue: Sea $X \subseteq \omega$, finito. Enumeramos los elementos de X en orden ascendente en la forma $x_0, x_1, \ldots, x_{|X|-1}$. Así,

- X es $1-$grande si $2 \leqslant |X|$;
- X es $\alpha-$grande si $X \backslash \{x_0\}$ es $F(\alpha, x_1)-$grande.

3.28 Observación. *Por como se definio el concepto de $\alpha-$grande y la función F, tenemos:*

- *Para X un conjunto y $n \in \omega$,*

$$X \text{ es } n-\text{grande} \iff |X| \geqslant n+1.$$

- *Para cualquier $n \in \omega$,*

$$F(\omega, n) = n.$$

3.29 Proposición. *Si X es $\alpha-$grande y X es segmento inicial de Y, entonces Y también es $\alpha-$grande.*

Demostración. Procedemos por inducción sobre α:
Como caso base; supongamos X tal que es $1-$grande. Entonces X tiene al menos dos elementos. Luego, cualquier conjunto Y que tenga a X como segmento inicial tiene al menos dos elementos, luego Y es $1-$grande. Ahora; consideremos $X = \{x_1, \ldots, x_k\}$ tal que es $\alpha-$grande y $Y = \{x_1, \ldots, x_k, y_{k+1}, \ldots, y_m\}$. Entonces, $\{x_2, \ldots, x_k\}$ es $F(\alpha, x_2)-$grande. Como $F(\alpha, x_2) < \alpha$, tenemos que, por hipótesis de inducción que

$$\{x_2, \ldots, x_k, y_{k+1}, \ldots, y_m\} \text{ es } F(\alpha, x_2) - \text{grande.}$$

Luego, $\{x_2, \ldots, x_k, y_{k+1}, \ldots, y_m\}$ es $F(\alpha, x_2)-$grande. Entonces,

$$Y \text{ es } \alpha - \text{grande.}$$

□

3.30 Proposición. *Dados $\alpha \in \varepsilon_0$ y $X \subseteq \omega$, existe Y, con X un segmento inicial de Y, tal que Y es $\alpha-$grande.*

Demostración. Procedemos por inducción sobre α:
Como caso base, dado cualquier conjunto X, si añadimos dos elementos y_1, y_2 tendremos que

$$|X \cup \{y_1, y_2\}| \geqslant 2,$$

por lo que $Y = X \cup \{y_1, y_2\}$ es $1-$grande. Por otro lado; consideremos $X = \{x_1, \ldots, x_k\}$. Por hipótesis de inducción, existen $y_1, \ldots, y_m$ tales que

$$\{x_2, \ldots, x_k, y_1, \ldots, y_m\} \text{ es } F(\alpha, x_2) - \text{grande,}$$

luego, $Y = \{x_1, \ldots, x_k, y_1, \ldots, y_m\}$ es $\alpha-$grande. □

3.31 Corolario.

$$(\forall n \in \omega)(\exists b_n \in \omega)([1, b_n] \text{ es } \alpha - \text{grande}).$$

Demostración. Se sigue de la proposición 3.30 considerando $X = \{1\}$. □

3.32 Lema. *Para cada $n, l \in \omega$, y para cada ordinal sucesor β, existe un ordinal α tal que*

$$F\left(\underbrace{\omega^{\cdot^{\cdot^{\omega^{\beta}}}}}_{\omega, n \text{ veces}}, l\right) = \underbrace{\omega^{\cdot^{\cdot^{\omega^{\alpha}}}}}_{\omega, n-1 \text{ veces}}.$$

donde la primer torre de exponentes (la que aparece en la función F) tiene n apariciones de ω, y la segunda tiene $n-1$ apariciones de ω.

Demostración. Procedemos por inducción sobre n:
Para el caso $n = 1$, tenemos que:

$$F(\omega^\beta, l) = \omega^{\beta-1} \cdot l.$$

Tomando a $\alpha = \omega^{\beta-1} \cdot l$, se cumple la propiedad. Ahora, asumimos que se cumple:

$$F\left(\underbrace{\omega^{\cdot^{\cdot^{\omega^\beta}}}}_{\omega,n \text{ veces}}, l\right) = \underbrace{\omega^{\cdot^{\cdot^{\omega^\alpha}}}}_{\omega,n-1 \text{ veces}},$$

y demostramos para el caso $n + 1$:

$$F\left(\underbrace{\omega^{\cdot^{\cdot^{\omega^\beta}}}}_{\omega,n+1 \text{ veces}}, l\right) = \omega^{\left(\underbrace{\omega^{\cdot^{\cdot^{\omega^\beta}}}}_{\omega,n \text{ veces}}, l\right)} = \omega^{\left(\underbrace{\omega^{\cdot^{\cdot^{\omega^\alpha}}}}_{\omega,n-1 \text{ veces}}\right)} = \underbrace{\omega^{\cdot^{\cdot^{\omega^\alpha}}}}_{\omega,n \text{ veces}}.$$

Esto completa la prueba. □

3.33 Lema. *Si* $X = \{x_1, \ldots, x_k\}$ *es* $\underbrace{\omega^{\cdot^{\cdot^{\omega^\beta}}}}_{\omega,n \text{ veces}}$ *−grande (con* $\beta > 0$*), entonces* $k \geqslant n$.

Demostración. Procedemos por inducción sobre n:
Considerando $n = 0$, tenemos que X es $\beta-$grande, entonces $k = |X| \geqslant 2 > 0$. Asumamos que se cumple el caso $n-$ésimo, entonces tenemos que

$$X = \{x_1, \ldots, x_k\} \text{ es } \underbrace{\omega^{\cdot^{\cdot^{\omega^\beta}}}}_{\omega,n+1 \text{ veces}} -\text{grande},$$

así pues,

$$\{x_2, \ldots, x_k\} \text{ es } F\left(\underbrace{\omega^{\cdot^{\cdot^{\omega^\beta}}}}_{\omega,n+1 \text{ veces}}, x_2\right) - \text{grande},$$

por lo que, gracias al lema 3.32, existe un ordinal α tal que:

$$\{x_2, \ldots, x_k\} \text{ es } \underbrace{\omega^{\cdot^{\cdot^{\omega^\alpha}}}}_{\omega,n \text{ veces}} -\text{grande},$$

luego, por hipótesis de inducción:

$$|\{x_2, \ldots, x_k\}| = k - 1 \geqslant n,$$

es decir:

$$k \geqslant n + 1.$$

□

3.34 Teorema. *Si* X *es* ω_n-*grande, entonces* $|X| \geqslant n + 1$.

Demostración. Sea $X = \{x_1, \ldots, x_k\}$ tal que es ω_n-grande. Entonces, por definición:

$$\{x_2, \ldots, x_k\} \text{ es } F(\omega_n, x_2) - \text{grande},$$

o lo que es lo mismo:

$$\{x_2, \ldots, x_k\} \text{ es } F\left(\underbrace{\omega^{\cdot^{\cdot^{\cdot^{\omega^1}}}}}_{\omega, n+1 \text{ veces}}, x_2\right) - \text{grande},$$

luego, por el lema 3.32, existe α tal que:

$$\{x_2, \ldots, x_k\} \text{ es } \underbrace{\omega^{\cdot^{\cdot^{\cdot^{\omega^\alpha}}}}}_{\omega, n \text{ veces}} -\text{grande}.$$

Ahora bien, por el lema 3.33 tenemos que

$$|X| - 1 = |\{x_2, \ldots, x_k\}| \geqslant n;$$

es decir,

$$|X| \geqslant n + 1.$$

□

3.35 Corolario. *Si* $[a, b]$ *es* ω_c-*grande, entonces* $b \geqslant c + a$.

Demostración. Por el teorema 3.34, tenemos que

$$b - a + 1 \geqslant c + 1$$

luego,

$$b \geqslant c + a.$$

□

3.36 Corolario. *Si* $[1, b]$ *es* ω_c-*grande, entonces* $c < b$.

Demostración. Por el teorema 3.34, tenemos que $b - 1 \geqslant c + 1$. Entonces,

$$b > c + 1,$$

y por lo tanto

$$b > c.$$

□

3.37 Proposición.

$$\forall n \in \omega \ \ (\alpha < \beta \implies F(\alpha, n) < F(\beta, n)).$$

Demostración. Procedemos por inducción sobre β:

- $\beta = 2$: si $\beta = 2$, entonces α es igual a 1 o a 0. De cualquier forma; $F(\beta, n) = 1$ y $F(\alpha, n) = 0$. Así, se cumple el enunciado.

- $\beta = \alpha + 1$: como $\alpha < \beta$, tenemos que $\alpha \leqslant \gamma < \beta$. Si $\alpha < \gamma$, entonces por hipótesis de inducción $F(\alpha, n) < F(\gamma, n)$. Si $\alpha = \gamma$, entonces $F(\alpha, n) = F(\gamma, n)$. Así pues,

$$F(\alpha, n) \leqslant F(\gamma, n) < \gamma = F(\gamma + 1, n) = F(\beta, n),$$

lo cuál es justo lo que queríamos.

- $\beta = \omega^\gamma(\lambda + 1)$: consideremos y igual a $\omega^{F(\gamma,n)}$ o a $\omega^{\gamma-1} \cdot n$, dependiendo si γ es límite o sucesor, respectivamente. Por propiedades del producto y la potencia ordinal, tenemos que como $\alpha < \beta$, entonces α es un sucesor, o $\alpha = \omega^{\gamma_1}(\lambda_1 + 1)$, con $\gamma_1 < \gamma$ o $\lambda_1 < \lambda$. Ahora, el caso de α sucesor se divide en dos casos. Si α es finito, la conclusión es inmediata, pues $F(\alpha, n)$ también sería finito, mientras que $F(\beta, n) = F(\omega^\gamma(\lambda + 1), n) = \omega^\gamma\lambda + \omega^{F(\gamma,n)} \cdot n$, el cuál es un ordinal infinito (de hecho, límite). Si α es infinito, entonces es de la forma $\omega^{\gamma_2}(\lambda_2 + 1) + m$, con $m \in \omega \setminus \{0\}$, $\gamma_2 < \gamma$ o $\lambda_2 < \lambda$ (lo cuál implica que $\lambda_2 + 1 \leqslant \lambda$); en ambos casos:

$$\begin{aligned} F(\alpha, n) &= F(\omega^{\gamma_2}(\lambda_2 + 1) + m, n) \\ &= \omega^{\gamma_2}(\lambda_2 + 1) + m - 1 \\ &\leqslant \omega^\gamma\lambda + m - 1 \\ &< \omega^\gamma\lambda + y \\ &= F(\beta, n); \end{aligned}$$

lo cuál es lo que queríamos, independientemente de si γ es sucesor o límite. Finalmente, si tenemos el caso donde $\alpha = \omega^{\gamma_1}(\lambda_1 + 1)$, tenemos:

$$F(\alpha, n) = \omega^{\gamma_1}\lambda_1 + y < \omega^\gamma\lambda + y = F(\beta, n),$$

independientemente de si γ es sucesor o límite.

□

3.38 Lema. *Sean X un conjunto y α y β dos ordinales. Si X es $\alpha-$grande y $\beta < \alpha$, entonces X es $\beta-$grande.*

Demostración. Procedemos por inducción sobre α:

- Si X es $2-$grande, entonces tiene al menos tres elementos, entonces tiene al menos dos elementos, entonces es $1-$grande.

- Ahora, supongamos que $X = \{x_1, \ldots, x_n\}$. Si X es $\alpha-$grande, entonces $\{x_2, \ldots, x_n\}$ es $F(\alpha, x_2)-$grande. Por la proposición 3.37 tenemos que $F(\beta, x_2) < F(\alpha, x_2)$, y por hipótesis de inducción, $\{x_2, \ldots, x_n\}$ es $F(\beta, x_2)-$grande. Luego, por definición, X es $\beta-$grande.

□

3.39 Lema. *Sean X un conjunto y α un ordinal. Si X es $\alpha-$grande y Y es un conjunto tal que*

$$(\forall y \in Y)(\forall x \in X)(y \leqslant x),$$

entonces $X \cup Y$ es $\alpha-$grande.

Demostración. Sin perdida de generalidad, suponemos Y no vacío. Procedemos por inducción sobre α:

- Si $\alpha = 1$, entonces al ser X $\alpha-$grande, X tiene al menos dos elementos; luego para cualquier conjunto Y como en el enunciado, $X \cup Y$ tiene al menos dos elementos, luego $X \cup Y$ es $\alpha-$grande.
- Supongamos que el enunciado se cumple para todo ordinal menor a α; y supongamos $Y = \{y_1, \ldots, y_n\}$, con $n \geqslant 2$. Ahora, por el lema 3.38 que X sea $\alpha-$grande implica que X es $F(\alpha, y_2)-$grande. Ahora, por hipótesis de inducción, $(Y \setminus \{y_1\}) \cup X$ es $F(\alpha, y_2)-$grande. Así, por definición, $Y \cup X$ es $\alpha-$grande. En el caso de que Y sea un conjunto de un sólo elemento, si $X \cap Y = \varnothing$ podemos considerar el conjunto $Y' = Y \cup \min X$ y el paso inductivo se cumple igual para este nuevo conjunto; en otro caso, no hay nada que probar, pues $Y \subseteq X$.

□

Capítulo 4

La indemostrabilidad del teorema de Goodstein

4.1. Los teoremas de Ketonen-Solovay

En la siguiente sección desarrollaremos unas cuantas herramientas muy especificas: los teoremas de Ketonen-Solovar. Así mismo, presentaremos en medida de lo posible todo aquello que sea útil para demostrar dichos teoremas. A continuación se definirán los indicadores y se escribiran explicitamente definiciones y resultados que permitirán el desarrollo de ideas en el último capítulo.[6]

Vale la pena aclarar que cuando hablamos de elementos o números *no estandar* nos referiremos a elementos de la forma como en el teorema 3.22.

4.1 Definición. Sea $M \vDash PA$ un modelo no estandar de PA y sea Q una propiedad de segmentos iniciales I de M. Una función $Y : M^2 \longrightarrow M$ es un indicador de Q en M si para cada $a, b \in M$,

$$Y(a,b) \text{ es no estandar de } PA \iff (\exists I \subseteq M)(a \in I \wedge b \notin I \wedge I \text{ satisface } Q).$$

Observemos que Q puede ser $I \vDash PA$. Este es un caso particular de la definición, pero que nos será útil, por lo que daremos una definición remplanzdo explicitamente Q.

4.2 Definición. Sea $M \vDash PA$ un modelo no estandar de PA. Una función $Y : M^2 \longrightarrow M$ es un indicador para modelos de PA si para cada $a, b \in M$,

$$Y(a,b) \text{ es no estandar de } PA \iff (\exists I \subseteq M)(a \in I \wedge b \notin I \wedge I \vDash PA);$$

con I un segmento inicial de M.

4.3 Teorema. *[8]*
Sea $f : \omega^k \longrightarrow \omega$. Entonces, son equivalentes las siguientes proposiciones:

- *f es demostrablemente computable en PA,*
- *la relación $f(x) = y$ es equivalente a una fórmula Σ_1 tal que:*

$$PA \vdash \forall x \exists y \varphi(x,y).$$

Demostración. Necesidad: supongamos que f es demostrablemente computable. Entonces, existe una máquina de Turing M tal que PA demuestra:

$$\forall x \exists t \ \ (M(x) \text{ se detiene en } t \text{ pasos}).$$

Ahora, se define:

$$\text{Comp}_M(x, y, t),$$

que se puede entender como t *codifica una computación válida de* M *sobre* x *con salida* y. Esta fórmula es Δ_0, pues la verificación finita es un cálculo aritmetico y acotado. Ahora, definimos:

$$\varphi(x, y) = \exists t \text{Comp}_M(x, y, t);$$

donde φ es Σ_1. Por otro lado, PA demuestra que M termina, por lo que:

$$\forall x \exists y \varphi(x, y);$$

más aún, como la máquina es determinista, tenemos que:

$$\forall x \forall y_1, y_2 \ \ (\varphi(x, y_1) \wedge \varphi(x, y_2) \implies y_1 = y_2);$$

por lo que la gráfica de f está definida por una fórmula Σ_1, que es lo que buscabamos. Suficiencia: supongamos que existe una fórmula Σ_1 de la forma:

$$\varphi(x, y) = \exists t \psi(x, y, t),$$

con ψ del tipo Δ_0, tal que PA demuestra:

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

Ahora, definimos el siguiente algoritmo:

```
for y=0,1,2,...
    for t = 0,1,2,...
        if \psi(x,y,t)
            return y
```

Este algoritmo es efectivo, pues ψ es Δ_0, luego es decidible, además de que la busqueda es computable. Ahora bien, PA demuestra que:

$$\forall x \exists y \exists t \psi(x, y, t);$$

esto significa que la busqueda siempre encuentra un testigo, por lo tanto PA demuestra que el algoritmo termina y que devuelve un único y. Así, con dicho algoritmo se contruye una máquina de Turing M_φ tal que busca testigos de forma efectiva, siempre termina y devuelve las salidas de f; y PA demuestra que la máquina termina. □

Este resultado se utilizará libremente a lo largo de esta sección, pues una caracterización importante de la funciones demostrablemente computables.

4.4 Definición. Un indicador $Y(x, y)$ se dice que es un indicador bien comportado para Q en PA si

1. $Y(x, y) = z$ es una Σ_1 $\mathcal{L}_A$−formula con únicamente las variables libres x, y y z;

2. $PA \vdash \forall x, y \exists! z Y(x,y) = z$;

3. $PA \vdash \forall x, y Y(x,y) \leqslant y$;

4. $PA \vdash x, y, x', y'(x' \leqslant x \wedge y \leqslant y' \Longrightarrow Y(x,y) \leqslant Y(x',y'))$;

5. para cada módelo no estandar $M \vDash PA$ y para cada $a, b \in M$, $Y(a,b)$ es no estandar si, y sólo si existe $I \subseteq_i M$ con $a \in I$ e I tiene la propiedad Q.

4.5 Teorema. *Sea M un modelo no estandar de PA. La función $Y : M^2 \longrightarrow \omega$ dada por*

$$Y(a,b) = \textit{máx}\{c | [a,b] \textit{ es } \omega_c - \textit{grande}\},$$

es un indicador bien comportado para modelos de PA.

Demostración.
1. Observemos lo siguiente:

$$\begin{aligned} Y(a,b) = d &\Longleftrightarrow \text{máx}\,\{c \mid [a,b] \text{ es } \omega_c - \text{grande}\} = d \\ &\Longleftrightarrow \exists c \ \ ([a,b] \text{ es } \omega_c - \text{grande} \wedge [a,b] \text{ no es } \omega_{c+1} - \text{grande}). \end{aligned}$$

3. Procedemos por contradicción: si tenemos que $y < Y(x,y)$, entonces tenemos que $y + 1 \leqslant Y(x,y)$. Así pues, por la proposición 3.38, tenemos que $[x,y]$ es $\omega_{y+1}-$grande. Luego, por el teorema 3.34 tenemos:

$$y - x + 1 \geqslant (y+1) + 1,$$

$$-x \geqslant 1;$$

y dado que x es un mayor o igual a 0, tenemos una contradicción.
2. Tenemos dos casos: si $\{c \mid [a,b] \text{ es } \omega_c - \text{grande}\}$ es vacío, basta considerar que

$$\text{máx}\,\varnothing = 0,$$

lo cuál basta para dar un elemento máximal único. Por otro lado, si el conjunto es no vacío, dado que es un conjunto acotado (por el punto 3), tenemos que posee un elemento máximal, el cuál es único.
4. Sean x, y, x', y' tales que $x' \leqslant x$ y $y \leqslant y'$. Nombremos los siguientes conjuntos:

$$A = \{c | [x,y] \text{ es } \omega_c - \text{grande}\},$$

$$B = \{c | [x,y'] \text{ es } \omega_c - \text{grande}\},$$

$$C = \{c | [x',y'] \text{ es } \omega_c - \text{grande}\}.$$

Claramente, por definición, $Y(x,y) = \text{máx}\,A$, $Y(x,y') = \text{máx}\,B$ y $Y(x',y') = \text{máx}\,C$. Así pues, por la proposición 3.29, como $[x,y]$ es $Y(x,y)-$grande, entonces $[x,y']$ es $Y(x,y)-$grande; así, $Y(x,y) \in B$, y por lo tanto

$$Y(x,y) \leqslant Y(x,y').$$

Ahora bien, $[x,y']$ es $Y(x,y')-$grande, así, por el lema 3.39, $[x',y']$ es $Y(x,y')-$grande. Así, tenemos que $Y(x,y') \in C$, y por lo tanto,

$$Y(x,y') \leqslant Y(x',y').$$

De estas dos desigualdades, tenemos que $Y(x,y) \leqslant Y(x',y')$.
5. Para la suficiencia, consideremos $I \subseteq_i M$ tal que $I \vDash PA$, $a \in I$y $b \notin I$. Dado k estandar, por la proposición 3.30 existe $d_k > a$ tal que $d_k \in I$ (por el teorema 3.20) y $[a, d_k]$ es ω_k-grande, luego como $b > d_k$ y por la proposición 3.29 y el teorema 3.20, $[a,b]$ es ω_k-grande. Como k es arbitraria (sólo pidiendole que sea estándar), para cada k estándar tenemos que:

$$[a,b] \text{ es } \omega_k - \text{grande.}$$

Por el principio 3.24, existe una c no estándar tal que

$$[a,b] \text{ es } \omega_c - \text{grande,}$$

y como la función Y se define como un máximo, $Y(a,b)$ es no estandar.
Para la necesidad basta observar lo siguiente: los segmentos iniciales de un modelo de PA son cerrados bajo funciones demostrablemente computables, esto es porque si $f(x) = y$ es equivalente a una expresión Σ_1 en M, entonces también lo es en I, para I segmento inicial. Luego, por el punto 1, tenemos que Y es una función demostrablemente computable. Así pues, tenemos que:

$$(a \in I \wedge b \in I) \implies Y(a,b) \in I;$$

o lo que es lo mismo:

$$Y(a,b) \notin I \implies (a \notin I \vee b \notin I).$$

Ahora bien, todo modelo de PA tiene segmentos iniciales que satisfacen PA (al menos, la sección isomorfa al módelo estandar). Sea $I \subseteq_i M$ tal que $a \in I$ y $I \vDash PA$. Si $Y(a,b)$ es no estandar (es decir, no está en I), entonces

$$b \notin I.$$

□

4.6 Lema. *(Primer Teorema de Ketonen-Solovay)*
Sea M un modelo no estandar de PA. La función $Y : M^2 \longrightarrow \omega$ dada por

$$Y(a,b) = \textit{máx}\{c | [a,b] \textit{ es } \omega_c - \textit{grande}\},$$

es un indicador para modelos de PA.

Demostración. Se sigue del teorema 4.5. □

4.7 Lema. *Sea $Y(x,y)$ un indicador bien comportado para la propiedad $I \vDash PA$ de segmentos iniciales I, y $Q_n : A_n \longrightarrow \omega$ dada por*

$$Q_n(x) = \text{mín}\{y \geqslant x | Y(x,y) \geqslant n\},$$

con $n \in \omega$ y $A_n \in \mathcal{P}(\omega)$. Si $a \in I \vDash PA$ para algún segmento inicial $I \subseteq_i \omega$, entonces

$$\forall n \in \omega \quad \mathcal{N} \vDash \exists c\, Q_n(a) = c.$$

Además, $PA \vdash \forall x \exists! y\, Q_n(x) = y$, y también cada $Q_n(x)$ es demostrablemente computable en PA.

Demostración. Si $a \in I$ y $b \in \prod^{\omega}/_{u} \backslash I$, con $I \vDash PA$, entonces $\mathcal{N} \vDash Y(a,b) = d$ para algún d no estandar, pues Y indica segmentos iniciales que satisfacen PA. Luego, $M \vDash \exists x(Y(a,b) \geqslant n)$ y el menor $x \geqslant a$ es $Q_n(a)$. Entonces para cada $a \in \mathcal{N}$ y cada $b \in \prod^{\omega}/_{u} \backslash \mathcal{N}$ tenemos que $Y(a,b)$ es no estandar, ya que $\mathcal{N}$ satisface PA. Por lo tanto, $\prod^{\omega}/_{u} \vDash \exists x(Y(a,x) \geqslant n)$, es decir, $\mathcal{N} \vDash \exists x(Y(a,x) \geqslant n)$ como $\mathcal{N} \prec \prod^{\omega}/_{u}$, y de nuevo el mínimo x es $Q_n(a)$. Finalmente, para verificar que cada $Q_n(a)$ es demostrablemente computable en PA deberíamos simplemente verificar que la fórmula $Q_n(x) = y$ es equivalente a una Σ_1 fórmula. Pero $Q_n(x) = y$ es

$$Y(x,y) \geqslant n \wedge \forall z < y \exists w(Y(x,y) = w \wedge w < n)$$

la cuál es $\Sigma_1(PA)$ ya que $Y(x,y) = z$ es Σ_1 y $\Sigma_1(PA)$ es cerrador bajo cuantificaciones acotadas. □

4.8 Observación. *Una cosa importante a resaltar es que:*

$$\text{mín}\{y \geqslant x \mid \text{máx}\{c \mid [x,y] \text{ es } \omega_c - \textit{grande}\} \geqslant n\} = \text{mín}\{y \geqslant x \mid [x,y] \text{ es } \omega_n - \textit{grande}\}.$$

Este hecho se sigue de lo siguiente:
Sea $y' = \text{mín}\{y \geqslant x \mid \text{máx}\{c \mid [x,y] \text{ es } \omega_c - \textit{grande}\}\}$. *Es decir, el mayor* c *tal que* $[x,y']$ *es* ω_c-*grande, es mayor a* n*; entonces, como* $c \geqslant n$ *y por el lema 3.38,* $[x,y']$ *es* ω_n-*grande. Luego*

$$y' \in \{y \geqslant x \mid [x,y] \text{ es } \omega_n - \textit{grande}\}.$$

Por otro lado, si $y'' = \text{mín}\{\{y \geqslant x \mid [x,y] \text{ es } \omega_n - \textit{grande}\}\}$, *entonces el mayor* c *tal que* $[x,y'']$ *es* ω_c-*grande es mayor o igual a* n*, luego*

$$y'' \in \{y \geqslant x \mid \text{máx}\{c \mid [x,y] \text{ es } \omega_c - \textit{grande}\}\}.$$

Luego, se sigue la igualdad.

4.9 Definición. *(Jerarquia de Hardy)*
Definimos la función $h_\alpha : \omega \longrightarrow \omega$ de la siguiente forma:

$$h_0(n) = n,$$
$$h_\alpha(n) = h_{F(\alpha,n)}(n+1).$$

4.10 Definición. Para cada $i \in \omega$, definimos las funciones $q_i : \omega \longrightarrow \omega$

$$q_i(x) = \text{mín}\{y \geqslant x | [x,y] \text{ es } \omega_i - \text{grande}\}.$$

4.11 Lema. *Sea* n *un número natural. Entonces, para cada* x*:*

$$q_n(x+1) = q_{n+1}(x).$$

Demostración. Por el corolario 3.35, tenemos las siguientes implicaciones:

$$[x,y] \text{ es } \omega_{n+1}-\text{grande} \implies y - x + 1 \geqslant (n+1) + 1;$$
$$[x+1,y] \text{ es } \omega_n-\text{grande} \implies y - (x+1) + 1 \geqslant n + 1.$$

Así, tomando los mínimos valores que puede tomar y en cada caso, tenemos lo siguiente:

$$q_{n+1}(x) - x + 1 = (n+1) + 1 \wedge q_n(x) - (x+1) + 1 = n + 1.$$

Haciendo algebra sobre las expresiones anteriores, tenemos que:

$$q_{n+1}(x) = n + 1 + x \wedge q_n(x) = n + 1 + x,$$

por lo que tenemos de inmediato que

$$q_{n+1}(x) = q_n(x).$$

□

4.12 Lema. *Para cada α, se tiene que para toda x suficientemente grande*

$$h_\alpha(x) < q_N(x),$$

con $N = \text{mín}\{n \in \omega \mid \alpha < \omega_n\}$ *o* $N = \text{mín}\{n \in \omega \mid \alpha < \omega_n\} + 1$.

Demostración. Procedemos por inducción sobre α:
Observemos que $x < q_0(x)$, pues $[x, q_0(x)]$ es $\omega-$grande si y sólo si $[x+1, q_0(x)]$ es $F(\omega_0, x+1)-$grande, pero $F(\omega_0, x+1) = x+1$, además que

$$X \text{ es } n - \text{grande} \Longleftrightarrow |X| \geqslant n + 1,$$

por lo que tenemos, por la mínimalidad de $q_0(x)$, que $q_0(x) - (x+1) + 1 = (x+1) + 1$, es decir:

$$q_0(x) = 2(x+1) > x.$$

Como h_0 es simplemente la identidad, para cada x, $h_0(x) < q_0(x)$, además

$$0 = \text{mín}\{n \in \omega \mid 0 < \omega_n\}.$$

Ahora, supongamos que el lema se cumple para cada $\xi < \alpha$. Tenemos dos casos: $\alpha = \omega_{N'}$, para alguna N', o para cada n se tiene que $\alpha \neq \omega_n$.

- Si $\alpha = \omega_{N'}$, para cada η tal que $\omega_{N'-1} \leqslant \eta < \alpha$,

  $$N' = \text{mín}\{n \in \omega \mid \eta < \omega_n\};$$

  luego, dado que $(F(\alpha, n))_{n\in\omega}$ forma una sucesión creciente de ordinales que converge a α, a partir de un cierto indice m, se tiene que

  $$F(\alpha, m) \geqslant \omega_{N'-1};$$

  por lo que, por el lema 4.11 y por hipótesis de inducción, existe un número l tal que para toda x mayor o igual que $\text{máx}\{m, l\}$,

  $$h_\alpha(x) = h_{F(\alpha,x)}(x+1) < q_{N'}(x+1) = q_{N'+1}(x).$$

  Ahora, tomando $N = N' + 1$, tenemos que en efecto

  $$N = \text{mín}\{n \in \omega \mid \alpha < \omega_N\}.$$

- Si $\alpha \neq \omega_n$ para cualquier n, nuevamente considerando que $(F(\alpha, n))_{n\in\omega}$ forma una sucesión creciente de ordinales que converge a α y que cada termino de la sucesión es menor estricto que α, tenemos que a partir de cierto indice m

$$\omega_{N-1} \leqslant F(\alpha, m) < \alpha < \omega_N;$$

para $N = \min\{n \in \omega \mid \alpha < \omega_n\}$. Entonces, por el lema 4.11 y por la hipótesis de inducción, existe un l tal que para toda x mayor o igual que $\max\{m, l\}$,

$$h_\alpha(x) = h_{F(\alpha,x)}(x+1) < q_N(x+1) = q_{N+1}(x).$$

Esto termina la prueba. □

4.13 Lema. *[9]*
Para una función $f : \omega^k \longrightarrow \omega$, las siguientes proposiciones son equivalentes:

- *f es demostrablemente computable en T;*
- *existe una fórmula $\psi(x, y, t) \in \Delta_0$ tal que*

$$T \vdash \forall x \exists! y \exists t \psi(x, y, t),$$

y $f(x) = y$ es el único y que satisface esto.

Demostración. Comencemos por la necesidad:
Si f es demostrablemente computable, existe una máquina de Turing M tal que:

$$T \vdash \forall x \exists t \mathrm{Halt}_M(x, t),$$

donde $\mathrm{Halt}_M(x, t)$ se interpreta como *M se detiene sobre x en t pasos.* Ahora bien, la relación

$$\mathrm{Comp}_M(x, y, t),$$

la cuál se interpreta como *t codifica un cálculo válido de M sobre x que termina con salida y* es tal que toda verificación es finita y se recorren los t pasos; es decir, es Δ_0. Ahora, definimos el algoritmo:

```
for y = 0,1,2,...
    for t = 0,1,2,...
        if Comp_M(x,y,t)
            return y
```

Este algoritmo es computable y *PA* demuestra que existe algún t en donde termina el algoritmo y que el y encontrado es único. Cabe recalcar que esta busqueda es exhaustiva.
Para la suficiencia:
Supongamos que existe $\psi(x, y, t) \in \Delta_0$ tal que

$$T \vdash \forall x \exists! y \exists t \psi(x, y, t).$$

Definimos el algoritmo:

```
for y = 0,1,2,...
    for t = 0,1,2,...
        if Comp_M(x,y,t)
            return y
```

Este algoritmo es efectivo porque Δ_0 es decidible y la busqueda es computable. *PA* también demuestra que:

$$\forall x \forall y_1 \forall y_2 (\exists t_1 \psi(x, y_1, t_1) \wedge \exists t_2 \psi(x, y_2, t_2) \implies y_1 = y_2),$$

lo cuál implica que la salida y es la correcta y única. Ahora, como el algoritmo define una máquina de Turing que siempre termina y que *PA* demuestra esto último, entonces f es demostrablemente computable. □

4.14 Observación. *El anterior lema se puede entender como lo siguiente: una función es demostrablemente computable si, y sólo si puede obtenerse por una busqueda exhaustiva efectiva cuya terminación puede demostrarse en la teoría.*

4.15 Proposición. *Dado $\alpha \in \varepsilon_0$, h_α es una función estrictamente creciente.*

Demostración. Supongamos que no, es decir, existe un número natural x tal que:

$$h_\alpha(x+1) \leqslant h_\alpha(x).$$

Ya sabemos que no existen decrecimientos infinitos en los ordinales, por lo que si aplicamos la función F a α, como en la definición de las funciones h_α, en una cantidad finita de pasos, digamos ξ pasos, tenemos que:

$$h_0(x+1+\chi) \leqslant h_0(x+\chi);$$

pero esto es:

$$x+1+\chi \leqslant x+\chi,$$

lo que implica

$$1 \leqslant 0,$$

lo cuál es una contradicción. □

4.16 Proposición. *Sean α y β dos ordinales. Entonces, para x suficientemente grande, tenemos que:*

$$\alpha < \beta \implies h_\alpha(x) < h_\beta(x).$$

Demostración. Procedemos por inducción sobre β:
Para el caso $\beta = 1$, α no tiene de otra que ser 0, por lo que:

$$h_\alpha(x) = x < x+1 = h_0(x+1) = h_1(x) = h_\beta(x);$$

por lo que se cumple para todo x. Para el caso $\beta = \gamma + 1$, $\alpha \leqslant \gamma$, por lo que:

$$h_\alpha(x) \leqslant h_\gamma(x) = h_\beta(x-1) < h_\beta(x);$$

por lo que se cumple para cada x. Finalmente, si β es límite,

$$h_\beta(x) = h_{F(\beta,x)}(x+1).$$

Tomando x suficientemente grande para que

$$F(\beta, x) > \alpha,$$

entonces, por hipótesis de inducción,

$$h_\alpha(x+1) < h_{F(\beta,x)}(x+1);$$

luego

$$h_\alpha(x) < h_\alpha(x+1) < h_{F(\beta,x)}(x+1) = F_\beta(x).$$

□

4.17 Lema. *Dado $x \in \omega$, existe un $\alpha \in \varepsilon_0$ tal que:*

$$\forall n \in \omega \;\; n \leqslant h_\alpha(x).$$

Demostración. Procedemos por inducción sobre los naturales:
Para el caso $n = 0$: basta tomar $\alpha = 0$, pues

$$\forall m \in \omega \;\; (0 \leqslant m);$$

luego

$$0 \leqslant h_\alpha(x).$$

Ahora, si ya se cumple que $n \leqslant h_\alpha(x)$, para algún α, tenemos que:

$$n + 1 \leqslant h_\alpha(x) + 1 \leqslant h_{\alpha+1}(x).$$

□

4.18 Lema. *Para cualquier función f demostrablemente computable, existe un $\alpha \in \varepsilon_0$ tal que, para x suficientemente grande,*

$$f(x) < h_\alpha(x).$$

Demostración. Supongamos que existe f una función tal que, para todo $\alpha \in \varepsilon_0$, se cumple que:

$$\forall y \exists x > y \;\; (h_\alpha(x) \leqslant f(x));$$

demostraremos que f no es demostrablemente computable. Observemos que si x es tal que

$$\forall \alpha \in \varepsilon_0 \;\; (h_\alpha(x) \leqslant f(x)),$$

entonces, para cada $n \in \omega$ y para cada α, tenemos que:

$$n \leqslant h_\alpha(x) \leqslant f(x);$$

más aún, como es para cada α, y por la proposición 4.16, la primer desigualdad es estricta, pues podemos tomar α suficientemente grande para ello (consideramos α_n como el ordinal que mayora a cada n bajo h_{α_n} y tomamos el supremo de todos esos α_n como α). Entonces;

$$n < h_\alpha(x) \leqslant f(x).$$

Como n es arbitrario, $f(x)$ es un número no estandar. Luego, por el lema 4.13, f no puede ser demostrablemente computable bajo PA, dado que un algoritmo de busqueda exhaustiva jamás podría dar con $f(x)$ es una cantidad finita de pasos. □

Otro argumento útil para el final del lema anterior (4.18) es porque los modelos de *PA* son cerrados bajo funciones demostrablemente computables, como vimos en la demostración del teorema 4.5.

4.19 Corolario. *(Tercer Teorema de Ketonen-Solovay)*
Las funciones

$$q_n : \omega \longrightarrow \omega$$
$$x \mapsto \text{mín}\,\{y \geqslant x | [x, y] \text{ es } \omega_n - \text{grande}\}$$

son total computables (demostrable en PA), y para dacada función total demostrablemente computable f, existe $n \in \omega$ tal que $f(x) < q_n(x)$ para toda $x \in \omega$ suficientemente grande.

Demostración. La primera parte se sigue del teorema 4.7., tomando $Y(x, y)$ como el indicador del teorema 4.6 y $Q_n = q_n$. Lo segundo se sigue directamente de 4.18. □

4.2. Antes de la indemostrabilidad

En la siguiente sección daremos herramientas y resultados útiles para dar con el objetivo de este trabajo: demostrar la Indemostrabilidad del teorema de Goodstein bajo los axiomas de Peano.

4.20 Observación. *En lo siguiente, designaremos al conjunto de todas las tuplas finitas con entradas de números naturales por T.*

4.21 Definición. Definimos la función $v : T \longrightarrow \omega$ dada para cada $(x_1, x_2, \ldots, x_n) \in T$ como,

$$v(x_1, x_2, \ldots, x_n) = p_1^{x_1} \cdot p_2^{x_2} \cdots p_n^{x_n+1},$$

con p_i el $i-$ésimo número primo.

4.22 Definición. Definimos la función $u : \varepsilon_0 \longrightarrow T$, dada por $\forall \alpha \in \varepsilon_0$,

$$u(\alpha) = \begin{cases} (\alpha, 0) & \text{si } \alpha \in \omega \\ (\delta_0, v(u(\gamma_0)), \ldots, \delta_n, v(u(\gamma_n))) & \text{si } \alpha = \omega^{\gamma_0} \cdot \delta_0 + \cdots + \omega^{\gamma_n} \cdot \delta_n \end{cases},$$

donde, en el segundo caso, la suma $\omega^{\gamma_0} \cdot \delta_0 + \cdots + \omega^{\gamma_n} \cdot \delta_n$ es la forma normal de α.

4.23 Definición. Nombramos la función $\eta : \varepsilon_0 \longrightarrow \omega$, la cuál está dada por

$$\eta = v \circ u.$$

4.24 Observación. *Observemos que la función η, quitando de su dominio el ordinal 0, es inyectiva.*

Las anteriores funciones simplemente se ponen de manifiesto para recalcar que todos los resultados sobre ordinales e hidras son traducibles al lenguaje de la aritmetica de Peano y, por lo tanto, todo es demostrable bajo *PA*.

4.25 Proposición. *Existe una estrategía computable τ tal que*

$$G_\tau(\alpha, n) = F(\alpha, n + 1).$$

Demostración. Definamos τ como la siguiente estrategía:
Comenzando desde la raíz, subimos por el árbol de tal forma que, habiendo llegado a un nodo, viajamos al nodo inmediatamente por encima de él que tiene el ordinal asignado más bajo entre todos los nodos inmediatamente por encima. (Si más de uno de ellos tiene el ordinal mínimo, elegimos, digamos, el de más a la izquierda.) Eventualmente, llegamos a un nodo superior y la cabeza a la que está unido es la que hay que cortar.
Dado que tenemos un algoritmo para τ, es una estrategía computable. Sólo basta demostrar que $G_\tau(\alpha, n) = F(\alpha, n+1)$. Sea n un número natural; procedemos por inducción sobre α:
Si α es ordinal sucesor, entonces

$$G_\tau(\alpha, n) = \alpha - 1 = F(\alpha, n+1).$$

Así nuestro caso base es $\alpha = 1$. Si, para cada ordinal menor a α se satisface la igualdad; consideremos

$$\alpha = \omega^{\beta_1} + \cdots + \omega^{\beta_m},$$

con $\beta_1 \geqslant \cdots \geqslant \beta_m$; la cuál es la forma usual de un ordinal asociado a una hidra que no es sucesor. Entonces, la cabeza qué se cortará está asociada al ordinal ω^{β_m}. Consideraremos $\omega^{\beta_m} \neq 0$ para evitar el caso sucesor.

- Si β_m es un sucesor, entonces $\omega^{\beta_m} = \omega^{\gamma+1}$ y $G(\alpha, n) = \omega^{\beta_1} + \cdots + \omega^{\gamma} \cdot (n+1) = F(\alpha, n+1)$;

- si β_n es límite, entonces, dado que $\beta_n < \alpha$, tenemos:

$$G_\tau(\alpha, n) = \omega^{\beta_1} + \cdots + \omega^{G_\tau(\beta_m, n)} = \omega^{\beta_1} + \cdots + \omega^{F(\beta_m, n+1)} = F(\alpha, n+1).$$

Esto completa la prueba. □

4.26 Definición. Se define la operación $H : \varepsilon_0 \times \omega \longrightarrow \varepsilon_0$ como sigue:

$$H(\alpha, n) = \begin{cases} 0, & \text{si } \alpha = 0, \\ \beta, & \text{si } \alpha = \beta + 1, \\ \omega^{\delta} \cdot \beta + \omega^{H(\delta,n)} \cdot n + H(\omega^{H(\delta,n)}, n), & \alpha = \omega^{\delta}(\beta + 1). \end{cases}$$

4.27 Definición. (operador cambio de base)
Se define el operador de cambio de base como sigue: dados $m, n \in \omega$, donde

$$m = n^k \cdot a_k + n^{k-1} \cdot a_{k-1} + \cdots + n \cdot a_1 + a_0;$$

definimos $f^{m,n} : \omega + 1 \longrightarrow \varepsilon_0$ como:

$$f^{m,n}(x) = \sum_{i=0}^{k} a_i \cdot x^{f^{i,n}(x)};$$

donde el caso base es

$$f^{0,n}(x) = 0.$$

4.28 Observación. *Dado $m > 0$, tenemos:*

$$g_n(m) = f^{m,n}(n+1) - 1,$$

y

$$f_n(m) = f^{m,n}(\omega);$$

donde g_n y f_n son como en las definiciones 2.5 y 2.3, respectivamente.

4.29 Lema. *Para $m \geqslant 0$, $n > 1$, si $\alpha = f_{n+1}(m)$, entonces $f_{n+1}(m-1) = H(\alpha, n)$.*

Demostración. Consideremos la representación en base $n+1$ de m: sea

$$m = a_p(n+1)^{f^{p,n+1}(n+1)} + a_{p-1}(n+1)^{f^{p-1,n+1}(n+1)} + \cdots + a_0(n+1)^{f^{0,n+1}(n+1)},$$

con $0 \leqslant a_i \leqslant n$, y (dado que $m \neq 0$) sea j el número más pequeño tal que $a_j \neq 0$. El resultado es claro si $j = 0$, por lo que asumimos $j > 0$ y que el resultado es valido para cada $m' \in [[0, m]] \setminus \{0, m\}$. Entonces,

$$f_{n+1}(m-1) = \left(\sum_{i=j+1}^{p} \omega^{f^{i,n+1}(\omega)} \cdot a_i \right) + \omega^{f^{j,n+1}(\omega)}(a_j - 1) +$$

$$+ f_{n+1}(n \cdot (n+1)^{f^{j,n+1}(n+1)-1}) + f_{n+1}((n+1)^{f^{j,n+1}(n+1)-1} - 1),$$

mientras que

$$H(\alpha, n) = \left(\sum_{i=j+1}^{p} \omega^{f^{i,n+1}(\omega)} \cdot a_i \right) + \omega^{f^{j,n+1}(\omega)}(a_j - 1) + \omega^{H(f^{j,n+1}(\omega),n)} n + H(\omega^{H(f^{j,n+1}(\omega),n)}, n).$$

Usando la hipótesis de inducción es fácil ver que estas dos son iguales. □

4.30 Lema. *Para $n > 1$,*

$$H(f_n(m), n) = f_{n+1}(g_n(m)).$$

Demostración. Sea

$$m = \sum_{i=j}^{p} b_i n^{f^{i,n}(n)}$$

donde $0 \leqslant b_i < n$ y $b_j \neq 0$. Si $j = 0$, entonces es claro que

$$H(f_n(m), n) = f_{n+1}(g_n(m)),$$

así que asumiremos $j > 0$. Así,

$$H(f_n(m), n) = \left(\sum_{i=j+1}^{p} \omega^{f^{i,n}(\omega)} b_i \right) + \omega^{f^{j,n}(\omega)}(b_j - 1) + \omega^{H(f^{j,n}(\omega),n)} n + H(\omega^{H(f^{j,n}(\omega),n)}, n)$$

y

$$f_{n+1}(g_n(m)) = \left(\sum_{i=j+1}^{p} \omega^{f^{i,n}(\omega)} b_i \right) + f_{n+1}((n+1)^{f^{j,n}(n+1)} b_j - 1)$$

$$= \left(\sum_{i=j+1}^{p} \omega^{f^{i,n}(\omega)} b_i \right) + \omega^{f^{j,n}(\omega)}(b_j - 1) + f_{n+1}((n+1)^{f^{j,n}(n+1)-1} n)$$

$$+f_{n+1}((n+1)^{f^{j,n}(n+1)-1}-1).$$

Luego, por 4.29

$$f_{n+1}((n+1)^{f^{j,n}(n+1)-1}n)=\omega^{H(f^{j,n}(\omega),n)}n,$$

y

$$f_{n+1}((n+1)^{f^{j,n}(n+1)-1}-1)=H(\omega^{H(f^{j,n}(\omega),n)},n);$$

lo cuál nos da lo requerido para concluir lo deseado. □

4.31 Observación. *Para alguna operación $P(\alpha,n)$, denotamos:*

$$P(\beta,(n_1,\ldots,n_k)):=P(P(\beta,n_1),(n_2,\ldots,n_k));$$

es decir, iterando la operación P, $k-$veces, de forma que el primer parametro en cada ocación es, o bien el ordinal β, o bien la iteración anterior; y el segundo parametro uno de los elementos del conjunto $\{n_1,\ldots,n_k\}$. De manera análoga, si contamos con un conjunto $X=\{x_1,\ldots,x_n\}$, con sus elementos ordenados de forma ascendente, tenemos:

$$P(\beta,X)=P(\beta,(x_1,\ldots,x_k)).$$

4.32 Lema. *Dado un conjunto finito $X=\{x_1,\ldots,x_k\}$, con al menos dos elementos,*

$$X \text{ es } \alpha-\text{grande} \iff F(\alpha,X)=0.$$

Demostración. Procedemos por inducción sobre α:
Si X es $1-$grande, tenemos que X tiene al menos dos elementos; luego,

$$F(1,x_1)=0,$$

es decir:

$$F(1,X)=F(F(1,x_1),(x_2,\ldots,x_k))=0.$$

Por otro lado, si X es tal que

$$F(1,X)=0,$$

entonces,

$$F(F(1,x_1),(x_2,\ldots,x_k))=0;$$

luego, como $\{x_2,\ldots,x_k\}\neq\varnothing$, tenemos que X es $1-$grande. Así pues, si tenemos

$$X \text{ es } \alpha-\text{grande},$$

de inmediato tenemos que

$$\{x_2,\ldots,x_k\} \text{ es } F(\alpha,x_1)-\text{grande}.$$

Así, considerando que $F(\alpha,x_1)<\alpha$, por hipótesis de inducción tenemos:

$$F(F(\alpha,x_1),(x_2,\ldots,x_k))=F(\alpha,X)=0.$$

Reciprocamente, si tenemos $F(\alpha,X)=0$, tenemos que

$$F(F(\alpha,x_1),(x_2,\ldots,x_k))=0,$$

lo cuál, por hipótesis de inducción nos arroja que

$$\{x_2,\ldots,x_k\} \text{ es } F(\alpha,x_1)-\text{grande};$$

es decir

$$X \text{ es } \alpha-\text{grande},$$

justo lo que buscabamos. □

4.33 Definición. Escribimos

$$\beta \underset{n}{\to} \alpha$$

si para algunos $j_1, \ldots, j_k \leqslant n$,

$$\alpha = F(\beta, (j_1, \ldots, j_k)),$$

o si $\alpha = \beta$. También escribimos:

$$\beta \underset{n}{\Rightarrow} \alpha$$

si sucede los mismo con $j_1 = \cdots = j_k = n$, o también se cumple la igualdad.

4.34 Observación. *La relación* $\underset{n}{\Rightarrow}$ *es transitiva, pues si tenemos* $\alpha \underset{n}{\Rightarrow} \beta$ *y* $\beta \underset{n}{\Rightarrow} \gamma$,

$$\beta = F(\alpha, \underbrace{(n, \ldots, n)}_{k-veces}) \wedge \gamma = F(\beta, \underbrace{(n, \ldots, n)}_{k'-veces});$$

por lo que:

$$\gamma = F(F(\alpha, \underbrace{(n, \ldots, n)}_{k-veces}), \underbrace{(n, \ldots, n)}_{k'-veces}) = F(\alpha, \underbrace{(n, \ldots, n)}_{(k+k')-veces}),$$

es decir,

$$\alpha \underset{n}{\Rightarrow} \gamma.$$

De manera equivalente con $\underset{n}{\to}$.

4.35 Lema. *Sea* $n > 0$ *y sea* $l \in \omega$ *tal que*

$$F(\omega^\delta \cdot n, \underbrace{(n, \ldots, n)}_{l-veces}) \geqslant \omega^\delta(n-1)$$

entonces, existen $\xi_1, \ldots, \xi_l$ *ordinales tales que:*

- $k < l \Longrightarrow F(\omega^\delta \cdot n, \underbrace{(n, \ldots, n)}_{k-veces}) = \omega^\delta(n-1) + \xi_k$;
- $\omega^\delta > \xi_1 > \cdots > \xi_l$.

Demostración. Procedemos por inducción finita sobre k: si $k = 1$:

- Si $\delta \in$ SUCC:

  $$F(\omega^\delta \cdot n, n) = \omega^\delta(n-1) + \omega^{\delta-1} \cdot n = \omega^{\delta-1}(\omega(n-1) + n),$$

  así, $\xi_1 = \omega^{\delta-1} \cdot n$.

- Si $\delta \in$ LIM:

  $$F(\omega^\delta \cdot n, n) = \omega^\delta(n-1) + \omega^{F(\delta,n)} = \omega^{F(\delta,n)}(\omega^{\delta - F(\delta,n)}(n-1) + 1),$$

  así, $\xi_1 = \omega^{F(\delta,n)}$. Observemos que si bien, no tiene sentido hablar de $\delta - F(\delta, n)$, ya que delta es límite, podemos entenderlo como para algún ordinal entre $F(\delta, n)$ y δ, y al tomar el límite (el supremo) esto coincide con lo que buscamos.

Ahora, supongamos que ya están dado los $\xi_1, \ldots, \xi_k$, con $k \in [1, l-1]$, entonces

$$F(\omega^\delta \cdot n, \underbrace{(n, \ldots, n)}_{(k+1)-\text{veces}}) = F(F(\omega^\delta \cdot n, \underbrace{(n, \ldots, n)}_{k-\text{veces}}), n) = F(\omega^\delta(n-1) + \xi_k, n).$$

Observemos que $\xi_k \neq 0$, pues por hipótesis:

$$F(\omega^\delta \cdot n, \underbrace{(n, \ldots, n)}_{l-\text{veces}}) \geqslant \omega^\delta(n-1);$$

entonces, si $\xi_k = 0$, por lo que:

$$F(\omega^\delta \cdot n, \underbrace{(n, \ldots, n)}_{k-\text{veces}}) = \omega^\delta(n-1);$$

luego,

$$F(\omega^\delta \cdot n, \underbrace{(n, \ldots, n)}_{(k+1)-\text{veces}}) < \omega^\delta(n-1);$$

por lo que,

$$F(\omega^\delta \cdot n, \underbrace{(n, \ldots, n)}_{l-\text{veces}}) < \omega^\delta(n-1),$$

lo cuál es una contradicción.

- Si $\xi_k = \gamma + 1$, para algún ordinal γ, entonces

  $$F(\omega^\delta \cdot n, \underbrace{(n, \ldots, n)}_{k-\times veces}) = \omega^\delta(n-1) + \gamma + 1,$$

  el cuál es sucesor. Por lo tanto,

  $$F(\omega^\delta \cdot n, \underbrace{(n, \ldots, n)}_{(k+1)-\times veces}) = \omega^\delta(n-1) + \gamma,$$

  por lo tanto, $\xi_{k+1} = \gamma < \gamma + 1 = \xi_k$.

- Si ξ_k es límite, tenemos dos posibles casos:

  $$\xi_k = \omega^\alpha(\beta + 1) \wedge (\alpha \in \text{SUCC} \wedge \alpha \in \text{LIM}).$$

  Además, como $\xi_k < \omega^\delta$,

  $$\omega^\alpha \leqslant \omega^\alpha(\beta + 1) < \omega^\delta,$$

  luego

  $$\alpha < \delta.$$

  Señalemos que

  $$F(\omega^\delta \cdot n, \underbrace{(n, \ldots, n)}_{k-\text{veces}}) = \omega^\delta(n-1) + \omega^\alpha(\beta+1) = \omega^\alpha(\omega^{\delta-\alpha}(n-1) + \beta + 1),$$

  y

  $$F(\omega^\delta \cdot n, \underbrace{(n, \ldots, n)}_{(k+1)-\text{veces}}) = F(\omega^\alpha(\omega^{\delta-\alpha}(n-1) + \beta + 1), n).$$

1. Caso 1: $\alpha \in \mathrm{SUCC}$:

$$F(\omega^\delta \cdot n, \underbrace{(n, \ldots, n)}_{(k+1)-\text{veces}}) = \omega^\alpha(\omega^{\delta-\alpha}(n-1)+\beta) + \omega^{\alpha-1}\cdot n$$

$$= \omega^\delta(n-1) + \omega^\alpha \cdot \beta + \omega^{\alpha-1}\cdot n.$$

Además,

$$F(\omega^\alpha(\beta+1), n) = \omega^\alpha \cdot \beta + \omega^{\alpha-1}\cdot n,$$

por lo que, por el caracter decreciente de la función F,

$$\omega^\alpha \cdot \beta + \omega^{\alpha-1}\cdot n < \omega^\alpha(\beta+1).$$

Así, tomamos $\xi_{k+1} = \omega^\alpha \cdot \beta + \omega^{\alpha-1}\cdot n$, y claro que

$$\xi_{k+1} < \xi_k.$$

2. Caso 2: $\alpha \in \mathrm{LIM}$:

$$F(\omega^\delta \cdot n, \underbrace{(n, \ldots, n)}_{(k+1)-\text{veces}}) = \omega^\alpha(\omega^{\delta-\alpha}(n-1)+\beta) + \omega^{F(\alpha,n)}$$

$$= \omega^\delta(n-1) + \omega^\alpha \cdot \beta + \omega^{F(\alpha,n)}.$$

Y como

$$F(\omega^\alpha(\beta+1), n) = \omega^\alpha \cdot \beta + \omega^{F(\alpha,n)},$$

por el caracter decreciente de la función F,

$$\omega^\alpha \cdot \beta + \omega^{F(\alpha,n)} < \omega^\alpha(\beta+1).$$

Así, tomamos $\xi_{k+1} = \omega^\alpha \cdot \beta + \omega^{F(\alpha,n)}$, y claro que:

$$\xi_{k+1} < \xi_k.$$

Esto concluye la prueba. □

4.36 Observación. *Vale la pena señalar que los ξ_k en el lema 4.35 son únicos, dado que F es una función, por lo que estos no varían con la elección de l.*

4.37 Lema. *Se cumplen los siguientes enunciados:*

1. $(\beta \underset{n}{\Rightarrow} \alpha \wedge n > 0) \Longrightarrow \omega^\beta \underset{n}{\Rightarrow} \omega^\alpha$.
2. $0 < i < j \leqslant n \Longrightarrow F(\beta, j) \underset{n}{\Rightarrow} F(\beta, i)$.
3. $\beta \underset{n}{\Rightarrow} \alpha \Longleftrightarrow \beta \underset{n}{\to} \alpha$.
4. *Supongase* $\beta = \omega^{\beta_1} + \cdots + \omega^{\beta_k}$, $\gamma = \omega^{\gamma_1} + \cdots + \omega^{\gamma_m}$, *con*

$$\beta_1 \geqslant \cdots \geqslant \beta_k \geqslant \gamma_1 \geqslant \cdots \geqslant \gamma_m.$$

Entonces,

$$\gamma \underset{n}{\to} \delta \Longrightarrow \beta + \gamma \underset{n}{\to} \beta + \delta.$$

En particular $\beta + \gamma \underset{n}{\to} \beta$.

Demostración.

1. Procedemos por inducción sobre β: si $\beta = 0$ y $\beta \underset{n}{\Rightarrow} \alpha$, entonces:

$$\alpha = F(\beta, \underbrace{(n, \ldots, n)}_{k-\text{veces}}) = F(0, \underbrace{(n, \ldots, n)}_{k-\text{veces}}) = 0.$$

Por lo tanto $\alpha = \beta$ y $\omega^\alpha = \omega^\beta$, lo cual es suficiente. Consideremos que se cumple para cada $\lambda < \beta$. El caso $\beta = \alpha$ es inmediato, por lo que consideraremos $\alpha \neq \beta$.

- Si $\beta \in$ LIM, existe $k > 0$ tal que:

$$\beta \underset{n}{\Rightarrow} \alpha \iff \alpha = F(\beta, \underbrace{(n, \ldots, n)}_{k-\text{veces}}) = F(F(\beta, n), \underbrace{(n, \ldots, n)}_{(k-1)-\text{veces}}) \iff F(\beta, n) \underset{n}{\Rightarrow} \alpha.$$

Como $F(\beta, n) < \beta$, por hipótesis de inducción:

$$\omega^{F(\beta,n)} \underset{n}{\Rightarrow} \omega^\alpha;$$

es decir, existe j tal que:

$$\omega^\alpha = F(\omega^{F(\beta,n)}, \underbrace{(n, \ldots, n)}_{j-\text{veces}})$$

Ahora, observemos que:

$$F(\omega^\beta, n) = \omega^{F(\beta,n)},$$

por lo que:

$$\omega^\alpha = F(F(\omega^\beta, n), \underbrace{(n, \ldots, n)}_{j-\text{veces}}) = F(\omega^\beta, \underbrace{(n, \ldots, n)}_{(j+1)-\text{veces}});$$

es decir,

$$\omega^\beta \underset{n}{\Rightarrow} \omega^\alpha.$$

- Si $\beta \in$ SUCC, existe un ordinal límite γ, y un ordinal finito no nulo k tal que $\beta = \gamma + k$. Primero, observemos que:

$$\beta = \gamma + k \underset{n}{\Rightarrow} \gamma + k - 1 \underset{n}{\Rightarrow} \cdots \underset{n}{\Rightarrow} \gamma.$$

Ahora, afirmamos que para cada $n > 0$,

$$\omega^{\gamma+k} \underset{n}{\Rightarrow} \omega^{\gamma+k-1}.$$

En efecto, tenemos que:

$$F(\omega^{\gamma+k}, n) = \omega^{\gamma+k-1} \cdot n,$$

es decir,

$$\omega^{\gamma+k} \underset{n}{\Rightarrow} \omega^{\gamma+k-1} \cdot n.$$

Ahora, consideremos el conjunto

$$C = \left\{ i \in \omega \setminus \{0\} \mid F(\omega^{\gamma+k-1} \cdot n, \underbrace{(n, \ldots, n)}_{i-\text{veces}}) \geqslant \omega^{\gamma+k-1} \cdot (n-1) \right\}.$$

Este conjunto claro que no es vacio, pues al menos $1 \in C$ por definción. Observemos que C debe tener elemento máximo, pues en caso contrario tendríamos un decrecimiento infinito dado por los ξ_i del lema 4.35, lo cuál es imposible. Más aún, como estos ξ_i determinan una sucesión decreciente,

$$\xi_{\max C} = 0;$$

es decir:

$$F(\omega^{\gamma+k-1} \cdot n, \underbrace{(n, \ldots, n)}_{\max C-\text{veces}}) = \omega^{\gamma+k-1} \cdot (n-1),$$

es decir,

$$\omega^{\gamma+k-1} \cdot n \underset{n}{\Rightarrow} \omega^{\gamma+k-1} \cdot (n-1);$$

y como n es arbitraria, tenemos que:

$$\omega^{\gamma+k-1} \cdot n \underset{n}{\Rightarrow} \omega^{\gamma+k-1} \cdot (n-1) \underset{n}{\Rightarrow} \cdots \underset{n}{\Rightarrow} \omega^{\gamma+k-1}.$$

Así pues, tenemos lo que afirmabamos. Ahora, como k es fijo (y sólo depende de la elección de β), tenemos que:

$$\omega^{\gamma+k} \underset{n}{\Rightarrow} \omega^{\gamma+k-1} \underset{n}{\Rightarrow} \cdots \underset{n}{\Rightarrow} \omega^{\gamma}.$$

Finalmente, tenemos tres casos:

- $\alpha = \gamma + k'$, con $0 < k' < k$. Entonces, por lo señalado anteriormente:

$$\omega^{\gamma+k} \underset{n}{\Rightarrow} \omega^{\gamma+k'} = \omega^{\alpha}.$$

- $\alpha = \gamma$. Entonces, nuevamente por lo anterior:

$$\omega^{\gamma+k} \underset{n}{\Rightarrow} \omega^{\gamma} = \omega^{\alpha}.$$

- $\alpha < \gamma$. Entonces, como $\beta \underset{n}{\Rightarrow} \alpha$, entonces existe m tal que:

$$F(\beta, \underbrace{(n, \ldots, n)}_{m-\text{veces}}) = \alpha.$$

  Además, $F(\beta, \underbrace{(n, \ldots, n)}_{k-\text{veces}}) = \gamma$, or lo que $k < m$ y $\gamma \underset{n}{\Rightarrow} \alpha$. Así, como ya tenemos que

$$\omega^{\gamma+k} \underset{n}{\Rightarrow} \omega^{\gamma},$$

  y por el caso límite, ya sabemos que:

$$\omega^{\gamma} \underset{n}{\Rightarrow} \omega^{\alpha}.$$

  Así, tenemos que:

$$\omega^{\gamma+k} \underset{n}{\Rightarrow} \omega^{\alpha}.$$

Esto concluye este inciso.

2. Procedemos por inducción sobre β:
El caso $\beta = 0$ es inmediato, pues $F(0, x) = 0$, para cada x. Ahora, supongamos que para cada ordinal menor a β, se satisface el enunciado.

   - $\beta = \gamma + 1$: tenemos que para cada $m \in \omega$,

     $$F(\beta, m) = F(\gamma + 1, m) = \gamma;$$

     por lo tanto,

     $$F(\beta, i) = F(\beta, j).$$

   - $\beta = \omega^{\theta+1}(\gamma + 1)$: observemos lo siguiente:

     $$F(\beta, j) = \omega^{\theta+1} \cdot \gamma + \omega^{\theta} \cdot j = \omega^{\theta}(\omega \cdot \gamma + j).$$

     Ahora, por el lema 4.35, y usandolo como en el primer inciso de este lema, tenemos la siguiente secuencia:

     $$F(\beta, j) = \omega^{\theta}(\omega \cdot \gamma + j) \underset{n}{\Rightarrow} \omega^{\theta}(\omega \cdot \gamma + j - 1) \underset{n}{\Rightarrow} \cdots \underset{n}{\Rightarrow} \omega^{\theta}(\omega \cdot \gamma + i) = F(\beta, i).$$

   - $\beta = \omega^{\delta}(\gamma + 1)$: tenemos que, como los ordinales que estamos considerando son menores que ε_0, $\delta < \beta$, por lo que:

     $$F(\delta, j) \underset{n}{\Rightarrow} F(\delta, i).$$

     Luego, por el primer inciso, tenemos que:

     $$\omega^{F(\delta,j)} \underset{n}{\Rightarrow} \omega^{F(\delta,i)},$$

     por lo tanto,

     $$\omega^{\delta} \cdot \gamma + \omega^{F(\delta,j)} \underset{n}{\Rightarrow} \omega^{\delta} \cdot \gamma + \omega^{F(\delta,i)},$$

     es decir,

     $$F(\beta, j) \underset{n}{\Rightarrow} F(\beta, i).$$

   Esto termina el inciso.

3. La necesidad es inmediata por definición. Para la suficiencia procedemos por contrapositiva: supongamos que $\beta \underset{n}{\not\Rightarrow} \alpha$, es decir, para cada número natural k tenemos,

   $$\alpha \neq F(\beta, \underbrace{(n, \ldots, n)}_{k-\text{veces}}).$$

   Ahora, supongamos que existen $j_1, \ldots, j_m$ tales que:

   $$(\forall i \in [1, m])(j_i < n) \wedge F(\beta, (j_1, \ldots, j_m)) = \alpha.$$

   Por el inciso anterior, tenemos que:

   $$F(\beta, n) \underset{n}{\Rightarrow} F(\beta, j_1),$$

es decir, existe m_{j_1} tal que:

$$F(\beta, j_1) = F(F(\beta, n), \underbrace{(n, \ldots, n)}_{m_{j_1}-\text{veces}}) = F(\beta, \underbrace{(n, \ldots, n)}_{m_{j_1}+1-\text{veces}}).$$

Aplicando el mismo proceso a $F(\beta, n)$ y a las expresiones resultantes con cada j_i, tenemos que:

$$F(\beta, (j_1, \ldots, j_m)) = F(\beta, \underbrace{(n, \ldots, n)}_{m_{j_1}+\cdots+m_{j_m}+1-\text{veces}}).$$

Por lo tanto, tomando $k = m_{j_1} + \cdots + m_{j_m} + 1$, tenemos:

$$\alpha = F(\beta, \underbrace{(n, \ldots, n)}_{k-\text{veces}}).$$

Esto es una contradicción, y por lo tanto, tenemos que:

$$\beta \underset{n}{\nrightarrow} \alpha.$$

Esto termina el inciso.

4. Procedemos por inducción sobre β: el caso base es $\beta = 1$. En este caso, a γ no le queda otra que ser 1. Luego, si tenemos que $\gamma \underset{n}{\to} \delta$, entonces:

$$\gamma = 1 \Longrightarrow (\delta = 1 \vee \delta = 0).$$

En cualquier caso, $\beta + \gamma = 2$, y tenemos que:

$$2 \underset{n}{\to} 1 \underset{n}{\to} 0;$$

además que $\beta + \delta$ queda justo en esa secuencia, siempre menor o igual que $\beta + \gamma$, por lo que se cumple el caso base. Supongamos que la proposición se cumple para cada $\lambda < \beta$.

- $\beta = \alpha + 1$: por la forma que suponemos que tienen β y γ, al ser β un sucesor, debe ser de la forma:
$$\beta = \omega^{\beta_1} + \cdots + \omega^{\beta_k} + \omega^0;$$
y γ, por el orden en los exponente, no tiene otra que ser 1, por lo que $\beta + \gamma = \beta + 1$. Así pues, si tenemos que $\gamma \underset{n}{\to} \delta$, nuevamente δ tiene que ser 1 o 0, por lo que $\beta + \delta = \beta + 1$ o $\beta + \delta = \beta$; en el primer caso tendríamos la igualdad y terminamos, mientras que en el segundo caso se cumple por como se define la función F para sucesores.
- $\beta = \omega^\alpha(l+1)$: se tiene entonces que en la descomposición por suma de potencias de ω, el menor exponente es α; por lo que γ tiene como exponente más grande, a lo sumo, a α. Observemos que:
$$\omega^\alpha \cdot l < \beta;$$
por lo que, por hipótesis de inducción:
$$\omega^\alpha \cdot l + \gamma \underset{n}{\to} \omega^\alpha \cdot l + \delta.$$

Ahora, observemos que el exponente más grande que tiene $\omega^\alpha \cdot l + \gamma$ es α. Además, $\omega^\alpha < \beta$, por lo que nuevamente, por hipótesis de inducción,

$$\omega^\alpha + \omega^\alpha \cdot l + \gamma \underset{n}{\to} \omega^\alpha + \omega^\alpha \cdot l + \delta;$$

es decir,

$$\beta + \gamma \underset{n}{\to} \beta + \delta.$$

Esto concluye el inciso.

Esto concluye el lema. □

4.38 Lema. *Supongase que* $\beta \underset{n}{\to} \alpha$ *y* $0 < n \leqslant n_1 < n_2 < \cdots < n_k$. *Entonces,*

$$F(\beta, \{n_1, \ldots, n_k\}) \geqslant F(\alpha, \{n_1, \ldots, n_k\}).$$

Demostración. Procedemos por inducción sobre β:
El caso $\beta = 0$ es trivial, pues dado que $\beta \underset{n}{\to} \alpha$, entonces existen $j_1, \ldots, j_n$ tales que:

$$\alpha = F(\beta, (j_1, \ldots, j_k));$$

luego, por el comportamiento de F decreciente, tenemos que $0 = \beta \geqslant \alpha$, por lo que $\alpha = 0$. Así, para cualesquiera elementos como en el enunciado, tenemos:

$$F(\beta, \{n_1, \ldots, n_k\}) = F(\alpha, \{n_1, \ldots, n_k\}) = 0.$$

Así, supongamos que el resultado se mantiene para elementos menores a β. Como $n \leqslant n_1$, tenemos:

$$\beta \underset{n_1}{\to} \alpha \underset{n_1}{\to} F(\alpha, n_1),$$

es decir, tenemos elementos $j_1, \ldots, j_r < n \leqslant n_1$ tales que:

$$F(\beta, (j_1, \ldots, j_r)) = \alpha$$

luego,

$$F(F(\beta, (j_1, \ldots, j_r)), n_1) = F(\alpha, n_1),$$

y como $F(F(\beta, (j_1, \ldots, j_r)), n_1) = F(\beta, (j_1, \ldots, j_r, n_1))$, tenemos que:

$$\beta \underset{n_1}{\to} F(\alpha, n_1).$$

Por el inciso 3 del lema 4.37, afirmamos que:

$$F(\beta, n_1) \underset{n_1}{\to} F(\alpha, n_1);$$

en efecto: como $\beta \underset{n_1}{\to} F(\alpha, n_1)$, tenemos en particular que:

$$\beta \underset{n_1}{\Rightarrow} F(\alpha, n_1).$$

Si $F(\beta, n_1) = F(\alpha, n_1)$, entonces $\beta = \alpha$ y se tiene lo deseado. Por otro lado, si

$$F(\beta, \underbrace{(n_1, \ldots, n_1)}_{\text{al menos dos}}) = F(\alpha, n_1),$$

entonces,

$$F(F(\beta, n_1), \underbrace{(n_1, \ldots, n_1)}_{\text{al menos uno}}) = F(\alpha, n_1),$$

y se tiene lo deseado. Luego, como $F(\beta, n_1) < \beta$ y por hipótesis de inducción:

$$F(F(\beta, n_1), \{n_2, \ldots, n_k\}) \geqslant F(F(\alpha, n_1), \{n_2, \ldots, n_k\})$$

es decir,

$$F(\beta, \{n_1, \ldots, n_k\}) \geqslant F(\alpha, \{n_1, \ldots, n_k\}).$$

□

4.39 Proposición. *Para cada $\alpha \in \varepsilon_0$ y $j \in \omega$,*

$$H(\alpha, j) \underset{j}{\to} F(\alpha, j).$$

Demostración. Procedemos por inducción sobre α:
Si $\alpha = 0$, es trivial, pues

$$F(H(0, j), n_1) = F(0, n_1) = 0 = F(0, j).$$

En el caso de ordinales sucesores, tenemos:

$$H(\beta + 1, j) = F(\beta + 1, j),$$

y se tiene lo deseado. Así, considerando ordinales límites; si $\alpha = \omega^{\gamma+1}(\beta + 1)$, entonces por las definiciones 3.26 y 4.26, tenemos:

$$F(\alpha, j) = \omega^{\gamma+1}\beta + \omega^{\gamma} j \wedge H(\alpha, j) = F(\alpha, j) + H(\omega^{\gamma}, j).$$

Aplicando el inciso 4 del lema 4.37, tenemos:

$$H(\alpha, j) \underset{j}{\to} F(\alpha, j).$$

Si $\alpha = \omega^{\delta}(\beta + 1)$, con $\delta \in \mathrm{LIM}$, entonces por hipótesis de inducción:

$$H(\delta, j) \underset{j}{\to} F(\delta, j).$$

Por el inciso 1 del lema 4.37, tenemos

$$\omega^{H(\delta,j)} \underset{j}{\to} \omega^{F(\delta,j)}.$$

Entonces,

$$H(\alpha, j) = \omega^{\delta}\beta + \omega^{H(\delta,j)} + H(\omega^{H(\delta,j)}, j) \underset{j}{\to} \omega^{\delta}\beta + \omega^{H(\delta,j)}, \text{ inciso 4 del lema 4.37}$$

$$\underset{j}{\to} \omega^{\delta}\beta + \omega^{F(\delta,j)} = F(\alpha, j).$$

□

4.40 Teorema. *Sean $b_0, b_1, b_2, \ldots$ la sucesión de Goodstein de m en el $n-$ésimo paso y sea k el mínimo número tal que $b_k = 0$. Entonces, $[[n-1, n+k]]$ es $f_n(m)-$grande.*

Demostración. Consideremos $\alpha = f_n(b_0)$. Tomando en cuenta el lema 4.30, tenemos la siguiente sucesión de ordinales:

$$f_n(m) = f_n(b_0) = \alpha,$$

$$f_{n+1}(b_1) = H(\alpha, n),$$
$$f_{n+2}(b_2) = H(\alpha, \{n, n+1\}),$$
$$\vdots$$
$$f_{n+k}(b_k) = f_{n+k}(0) = 0 = H(\alpha, \{n, n+1, \ldots, n+k\}).$$

Por el lema 4.38 y el teorema 4.39,

$$F(\alpha, \{n, n+1, \ldots, n+k\}) \leqslant F(H(\alpha, n), \{n+1, \ldots, n+k\})$$
$$\leqslant F(H(\alpha, \{n, n+1\}), \{n+2, \ldots, n+k\})$$
$$\leqslant \cdots \leqslant H(\alpha, \{n, \ldots, n+k\}) = 0.$$

Luego, por el lema 4.32, $[[n-1, n+k]]$ es $\alpha-$grande. □

4.3. Indemostrabilidad

Un trabajo común en matemáticas es demostrar que una propiedad no se sigue de ciertos enunciados. Este tipo de demostraciones suelen llevarse a cabo exhibiendo un *algo* que satisface el enunciado en cuestión, pero que no satisface la propiedad. Por ejemplo, se puede demostrar fácilmente que la conmutatividad no se sigue de los axiomas de grupo, simplemente dando un grupo que no es conmutativo. La siguiente demostración consiste en eso: exhibir un modelo de *PA* que no satisface el teorema de Goodstein (asumiendo que sí lo hace y llegando a una contradicción); teniendo como consecuencia que el teorema de Goodstein no se puede seguir de los axiomas de Peano (ni de ningún conjunto de axiomas equivalente).[5]

4.41 Teorema. *El teorema de Goodstein no se puede demostrar bajo PA.*

Demostración. Supongamos que

$$PA \vdash (\forall m)(\exists k)(g_k(m) = 0); \tag{TG}$$

es decir, que el teorema de Goodstein es demostrable en *PA*. Del corolario 3.31, para cada n, número natural, existe b_n tal que $[[1, b_n]]$ es $\omega_{n+1}-$grande. Por el corolario 3.36 tenemos que $n+1 < b_n$. Luego, consideremos Y como en el teormea 4.6, por lo que

$$Y(1, b_n) = \text{máx}\left\{c | [[1, b_n]] \text{ es } \omega_c - \text{grande}\right\},$$

podemos afirmar que:

$$Y(1, b_n) \geqslant n+1 > n.$$

Luego, por el teorema 3.20 y tomando $b : \omega \longrightarrow \omega$ tal que $b(n) = b_n$, tenemos que:

$$[[[c_1]_\sim, [b]_\sim]] \text{ es } \omega_{[\text{id} + c_1]_\sim} - \text{grande}.$$

Más aún, denotando $i = [\mathrm{id}]_\sim$. Tenemos que

$$Y([c_1]_\sim, [b]_\sim) > i.$$

Por lo que tenemos que $Y([c_1]_\sim, [b]_\sim)$ es no estandar. Por lo tanto, existe un segmento inicial I de $\prod^\omega/_u$ tal que

$$I \vDash PA \wedge [b]_\sim \notin I.$$

Por lo tanto, el conjunto

$$\mathcal{C} = \left\{[t]_\sim | [[[c_1]_\sim, [t]_\sim]] \text{ es } \omega_{[\mathrm{id}+c_1]_\sim} - \text{grande} \wedge Y([c_1]_\sim, [t]_\sim) \text{ es no estandar}\right\} \neq \varnothing.$$

Pues $[b]_\sim \in \mathcal{C}$. Tomemos $[j]_\sim$ el mínimo elemento de este conjunto. Entonces,

$$[[[c_1]_\sim, [j]_\sim]] \text{ es } \omega_{[\mathrm{id}+c_1]_\sim} - \text{grande} \wedge Y([c_1]_\sim, [j]_\sim) \text{ es no estandar;}$$

luego existe M, segmento inicial de $\prod^\omega/_u$, tal que:

$$M \vDash PA \wedge [j]_\sim \notin M.$$

Luego, tenemos:

$$M \vDash (\neg\exists [j]_\sim)([[[c_1]_\sim, [t]_\sim]] \text{ es } \omega_{[\mathrm{id}+c_1]_\sim} - \text{grande}). \tag{NE}$$

Ahora, consideremos en M el número $d = 2^{2^{\cdot^{\cdot^{2}}}}$ con $[\mathrm{id}+c_1]_\sim$ exponenciaciones iteradas. Así, considerando f_n como en 2.3, tenemos que:

$$f_2(d) = \omega_{[\mathrm{id}+c_1]_\sim}.$$

Ahora, por TG, existe $[e]_\sim \in M$ suficientemente grande tal que

$$g_{[e]_\sim}(d) = 0.$$

Dado que la proposición 4.40 se puede probar bajo PA, tenemos en M:

$$[[[c_1]_\sim, [c_2 + e]_\sim]] \text{ es } \omega_{[\mathrm{id}+c_1]_\sim} - \text{grande,}$$

lo que contradice NE. Por lo tanto, en M no se satisface el teorema de Goodstein. Luego,

$$PA \nvdash (\forall m)(\exists k)(g_k(m) = 0).$$

□

Ahora, veamos el equivalente para hidras.

4.42 Teorema. *El enunciado toda estrategía computable es una estrategia ganadora no es demostrable bajo PA.*

Demostración. Sea τ una estrategía recursiva tal que

$$G_\tau(\alpha, n) = F(\alpha, n).$$

Cualquier prueba de que τ es ganadora es equivalente a demostrar lo mismo por inducción sobre $\alpha \in \varepsilon_0$; es decir, se puede demostrar por inducción que:

$$(\exists k)(F(\alpha, k) = 0).$$

Luego, esto significa que para cada $\alpha \in \varepsilon_0$, se puede calcular en una cantidad finita de pasos el ordinal $F(\alpha, n)$ (pues para $n < k$, se puede hacer como el algoritmo de τ indica, y para $k \geqslant n$ siempre vale 0), esto es que

$$F : \varepsilon_0 \times \omega \longrightarrow \varepsilon_0$$

es total computable. Nuevamente, como α se puede codificar bajo η como en 4.23, todo esto se podría hacer bajo PA. Así, consideremos la función:

$$\begin{array}{c} Q : \omega \times \omega \longrightarrow \omega \\ (n, x) \mapsto q_n(x) \end{array},$$

con q_n como en el corolario 4.19. Así pues, tenemos

```
input(n,x)
for(y=x+1; ;y++):
    if grande([x,y],omega_n)
        return y
```

Claramente este es el algoritmo qué calcula Q, más aún, como F es total computable, la parte del código

```
if grande([x,y],omega_n)
```

está bien definida y no es necesario usar que F es decreciente dejando fijo el primer argumento (no se podría usar esto, pues el primer argumento varia en ε_0). Esto prueba que Q es total computable. Sin embargo, observemos lo siguiente: definimos:

$$\begin{array}{c} q : \omega \longrightarrow \omega \\ x \mapsto \text{máx}\,\{q_j(i)\}\,[j, i \leqslant x] + 1 \end{array};$$

la cuál es una función computable, gracias a qué Q lo es. Luego, por el corolario 4.19, existe n tal que para cada x suficientemente grande

$$q(x) < q_n(x).$$

En particular, tomando $x > n$ y suficientemente grande, tenemos:

$$q_n(x) < q(x) < q_n(x),$$

lo cuál es absurdo. Así, tenemos qué no se puede demostrar que τ es ganadora. □

Capítulo 5

Anexo

A continuación se presentaran algunos elementos que se usaron o desarrollaron durante la realización de este trabajo, pero que no tendría sentido introducir en algún capítulo.

5.1. Axioma de elección y lema de Zorn

En la siguiente sección sólo se presentaran dos enunciados sumamente importantes en la teoría de conjuntos. Esto con el objetivo de no dejar por fuera dos enunciados que resultan cruciales en la matemática y su relación que ha dado tanto de qué hablar en la historia de la matemática.

5.1 Definición. En el sistema axiomatico Zermelo-Fränkel (ZF) podemos aceptar un axioma más: el axioma de elección, el cuál consiste de lo siguiente:

$$(\forall x)(((\forall y \in x)(y \neq \varnothing) \wedge (\forall y, z \in x)(y \cap z = \varnothing)) \Longrightarrow (\exists z)(\forall y \in x)(\exists! w)(w \in z \wedge w \in y))$$

Intuitivamente, si x es una familia de conjuntos no vacíos disjuntos dos a dos, entonces se puede escoger un elemento de cada miembro de x.

5.2 Definición. El siguiente enunciado es conocido como *el lema de Zorn*:
Todo conjunto parcialmente ordenado, no vacío, en el que toda cadena tiene una cota superior, contiene un elemento maximal.

5.3 Teorema. *(ZF)*
El axioma de elección es equivalente al lema de Zorn.

5.2. Código que cálcula sucesiones de Goodstein

A continuación presentaremos un código en *Python* que se desarrollo como primer acercamiento a las sucesiones de Goodstein, de forma en que se pueda visualizar la velocidad con la que crecen estas mismas:

```
import math as mt

def base_n(n,p):
    p1=p
    p_base=[]
    if p%n!=0:
        p_base.append(p%n)
        p1=p1-p%n
        if p1!=0:
            p_base.append("+")
        else:
            return p_base
    i=1
    while i!=0:
        con=0
        while mt.pow(n,con+1)<=p1:
            con=con+1
        kon=1
        while (kon+1)*mt.pow(n,con)<=p1:
            kon=kon+1
        if kon!=1:
            p_base=p_base+[kon,"*",n,"^",con]
        else:
            p_base=p_base+[n,"^",con]
        p1=p1-kon*mt.pow(n,con)
        if p1!=0:
            p_base.append("+")
        else:
            return p_base

def salto(p_base,n,p):
    p_aux=p_base
    if p_base==[]:
        return 0
    if len(p_base)==1:
        return p_base[0]
    if p_base[1]=="+":
        p_aux=p_aux[2:]
        return int(p_base[0]+salto(p_aux,n,p))
    if p_base[1]=="^":
        p_aux=p_aux[4:]
        return int(mt.pow((p_base[0]+1),
                salto(base_n(n,p_base[2]),n,p))+salto(p_aux,n,p))
    if p_base[1]=="*":
        p_aux=p_aux[6:]
        return int(p_base[0]*mt.pow((p_base[2]+1),
                salto(base_n(n,p_base[4]),n,p))+salto(p_aux,n,p))
```

```
def goodstein(p,i):
    if i==1:
        return p
    a=goodstein(p,i-1)
    if a>0:
        return salto(base_n(i,a),i,p)-1
    return 0

def sucesion_g(p,k):
    a=[]
    for i in range(k):
        a.append(goodstein(p,i+1))
    return a
```

Bibliografía

[1] Just W., Weese M., Discovery modern set theory, Vol. 1, American Mathematical Society, (1996).

[2] Fernández Bretón D. J., The American Mathematical Monthly, (2021), **129**, 116–131.

[3] Enderton H. B., A mathematical introduction to logic, Academic Press Inc., (1972).

[4] Weber R., Computability theory, American Mathematical Society, 1 edn., (1977).

[5] Kirby L., Paris J., Bulletin of the London Mathematical Society, (1982), **14**, 285–293.

[6] Kaye R., Models of Peano Arithmetic, Oxford University Press, 1 edn., (1991).

[7] Chang C. C., Keisler H. J., Model theory, Elsevier Science Publishers, 3 edn., (1990).

[8] Hájek P., Pudlák P., Metamathematics of first-order arithmetic, Cambridge University Press, 1 edn., (1998).

[9] Schwichtenberg H., Wainer S. S., Proofs and computations, Cambridge University Press, 1 edn., (2012).