Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias Físico Matemáticas
Licenciatura en Matemáticas

Los teoremas de incompletitud de Gödel

Tesis

que para obtener el grado de
licenciado en matemáticas

Presenta
Edwin Gabriel Lozano Galindo

Director de tesis
Dr. Iván Martínez Ruíz

Septiembre 2025

Para los que no me sueltan pese
a que soy un terco,
gracias por su paciencia

Agradecimientos

En primer lugar me gustaría agradecer a mi familia, por todo ese apoyo y paciencia incondicionales; a mis padres que me han sostenido y guiado toda mi vida; a mi hermano Yael que ha sido mi compañero y cómplice en todo momento; a Martha que ilumina como un sol mi vida todos los días y es mi motivación para seguir adelante.
A todos mis amigos; soy muy afortunado de tenerlos, gracias por todas las horas de estudio, por las horas de plática, por las horas de juego, por tantos años acompañándome, por nunca dejarme solo. Me ocuparían otras 90 páginas en agradecer a cada uno de ustedes lo que han hecho por mí.
Al profesor Félix Aquino y a la profesora Gina Helga, pues gracias a ellos me decidí a estudiar matemáticas con el objetivo de poder ser como ellos.
Al profesor Manuel Ibarra, porque cuando llegué a la facultad no estaba seguro de lograrlo, pero desde el primer día en que lo conocí, me contagió de la pasión por aprender y enseñar mates, y como por arte de magia perdí ese miedo que me inundaba.
Al profesor Iván Martínez, que me impulsó el amor a la lógica, gracias por esa paciencia, soy una persona muy terca cuando me pongo a escribir, y usted en ningún momento me negó nada, gracias por tantas horas de apoyo y trabajo.
A la familia de Martha; que desde el primer día en que los conocí me hicieron sentir muy querido.
A mis tíos Chevere y Asminda; que me acompañaron en una época complicada para todos.
A mis tíos Manuel y Yuri; porque toda mi vida estaré agradecidos con ellos y su familia.
A mis sinodales, que se tomarán el tiempo de revisar y hacer todas las correcciones necesarias.
En fin, gracias a todos por acompañarme y aguantarme. Los quiero muchísimo y gracias por todo.

Introducción

Kurt Gödel ha sido uno de los matemáticos más prolíficos en el ámbito de la Lógica. Es ampliamente reconocido por su trabajo en la completez de las Teorías de Primer Orden, por la consistencia del axioma de elección y la hipótesis del continuo. Además, revolucionó por completo el estudio y concepción que se tenían de las matemáticas en el siglo XX con sus famosos Teoremas de incompletitud.
Durante los años 30, un gran número de matemáticos trabajaba en un programa que buscaba formalizar todo el razonamiento matemático existente, cuyo principal impulsor fue David Hilbert. En el programa de Hilbert, se plantearon 2 preguntas importantes:

1. ¿Las matemáticas son completas?, es decir, ¿acaso cualquier afirmación en las matemáticas era demostrable?

2. ¿Las matemáticas son consistentes?, es decir, ¿la matemática está libre de contradicciones?

Muchos matemáticos de la época, incluido Hilbert, deseaban y estaban convencidos de que la respuesta a estas preguntas era sí, pero, ¿cómo las responderían? Fue así como muchos matemáticos como Hilbert, Bertrand Russell, Wilhelm Ackermann y John von Neumann trabajaron por responderlas.
Entre ellos, se encontraba Gödel, que intentó en repetidas ocasiones contribuir al programa tratando de responder las preguntas, intentó demostrar la consistencia del análisis clásico asumiendo que la aritmética era consistente. Pero, entre más trabajaba, empezaba a intuir que seria imposible lograrlo.
Fue así, que un 7 de septiembre de 1930, en una reunión del programa celebrada en Königsberg, Gödel anunció que tenía un trabajo en el que demostraba que los sistemas matemáticos tenían limites. Dicho trabajo titulado *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme* (Sobre sentencias formalmente indecidibles de Principia Mathematica y Sistemas afines) fue publicado en 1931 y en él se encuentran lo que hoy conocemos como los teoremas de incompletitud de Gödel.

Este trabajo tiene como objetivo hacer un análisis exhaustivo de dichos teoremas que revolucionaron la matemática, construyendo todo lo necesario para poder demostrarlos de la manera más precisa posible.

En el Capítulo 1 comenzaremos dando los conceptos básicos necesarios acerca de las Teorías de Primer Orden. Posteriormente, en el Capítulo 2 procederemos a estudiar ciertas Teorías de Primer Orden, las teorías con igualdad. Estudiaremos su definición, analizaremos caracterizaciones de éstas y propiedades que nos ayudarán a comprender el concepto. Luego, en el Capítulo 3, axiomatizaremos de manera formal una teoría muy estudiada, la Aritmética de Peano. El objetivo aquí es formalizar los conceptos básicos que conocemos acerca de los números naturales, tales como la relación de desigualdad, teoremas conocidos como el algoritmo de la división o la inducción fuerte. Esta teoría, será fundamental para el estudio de los teoremas de incompletitud. En el capítulo 4 introduciremos el concepto de funciones y relaciones número-teóricas, estas funciones están definidas dentro de la metateoría, es decir, son funciones cuya imagen está contenida en $\mathbb{N}$, así que será necesario estudiar los conceptos de representabilidad y expresabilidad, que nos ayudan a estudiar estas funciones y relaciones dentro de la teoría antes mencionada. Después estudiaremos cierto tipo de funciones y relaciones número-teóricas, las funciones recursivas. Analizaremos propiedades de estas que serán fundamentales en el estudio de los teoremas de incompletitud. Por último, en el Capítulo 5 ya tenemos todo lo necesario para empezar a estudiar los teoremas de incompletitud. Se comenzará introduciendo los números de Gödel, que fue la manera en que Gödel codificó toda la aritmética de Peano, después se analizarán proposiciones fundamentales para poder probar los teoremas de incompletitud y concluiremos con el análisis de los dos teoremas.

Índice general

Capítulo 1

Cálculo Predicativo Clásico

Este capítulo es un breve resumen de definiciones y resultados que se abarcan en un curso introductorio de Lógica. Es necesario que las tengamos presentes porque son la base del trabajo que desarrollaremos. Para consultar las pruebas de las proposiciones dadas, podemos consultar [1] en las páginas 45-82.

Definición 1.1. Se define el lenguaje $\mathscr{L}$ del Cálculo Predicativo Clásico como el conjunto

$$\mathscr{L} = \mathrm{VAR} \cup C \cup R \cup F \cup A \cup S \cup N$$

donde:

i) $VAR = \{x_n | n \in \mathbb{N}\}$, llamado el conjunto de variables.

ii) $C = \{a_n | n \in \mathbb{N}\}$, llamado el conjunto de constantes.

iii) $R = \{A_k^n | k, n \in \mathbb{N}\}$, llamado el conjunto de símbolos relacionales o predicativos y para $A_k^n \in R$, se denomina a $n \in \mathbb{N}$ la aridad del símbolo predicativo.

iv) $F = \{f_k^n | k, n \in \mathbb{N}\}$, llamado el conjunto de símbolos funcionales, en este caso, si $f_k^n \in F$, decimos que f_k^n es un símbolo funcional de aridad $n \in \mathbb{N}$.

v) $A = \{(,)\}$ es el conjunto de signos de agrupación.

vi) $S = \{\rightarrow, \neg\}$ es el conjunto de conectivos primitivos.

vii) $S = \{\forall\}$ es el conjunto de cuantificadores, donde $\forall$ es llamado el cuantificador universal.

Al Cálculo Predicativo también se le llama Lenguaje de Primer Orden.
En general, es posible obtener distintos Lenguajes de Primer Orden; todo depende de las variables, constantes, símbolos relacionales y símbolos funcionales que contengan al ser definidos. El Cálculo Predicativo Clásico es la manera general en la que definimos los lenguajes de Primer Orden.

Definición 1.2. Se define el conjunto $\mathcal{TERM}$ de términos como el menor conjunto X que cumple:

1. Si $x_i \in VAR$, entonces $x_i \in X$.
2. Si a_i es constante, entonces $a_i \in X$.
3. Si f_k^n es un símbolo funcional de aridad n y $t_1, t_2, \ldots, t_n \in X$, entonces $f_k^n(t_1, t_2, \ldots, t_n) \in X$.

Definición 1.3. Se define el conjunto $\mathcal{FORM}$ de fórmulas bien formadas como el menor conjunto X que cumple:

1. Si A_k^n es un símbolo predicativo de aridad n y $t_1, t_2, \ldots, t_n \in \mathcal{TERM}$, entonces $A_k^n(t_1, t_2, \ldots, t_n) \in X$.

2. Si $\varphi, \psi \in X$, entonces $(\varphi \to \psi) \in X$ y $\neg(\varphi) \in X$.

3. Si $\varphi \in X$ y $x_i \in VAR$, entonces $((\forall x_i)\varphi) \in X$.

Cuando no se generen confusiones podemos escribir $\varphi \to \psi$, $\neg\varphi$ y $(\forall x_i)\varphi$ en lugar de $(\varphi \to \psi)$, $\neg(\varphi)$ y $((\forall x_i)\varphi)$.
Usualmente, a las fórmulas del tipo $A_k^n(t_1, t_2, \ldots, t_n)$ las llamamos fórmulas atómicas.

Definición 1.4. Para $\varphi, \psi \in \mathcal{FORM}$ definimos las siguientes fórmulas de la siguiente manera:

i. $\neg(\varphi \to \neg\psi) := \varphi \ \wedge \ \psi$. A la fórmula $\varphi \ \wedge \ \psi$ la llamamos conjunción.

ii. $\neg\varphi \to \psi := \varphi \ \vee \ \psi$ A la fórmula $\varphi \ \vee \ \psi$ la llamamos disyunción.

iii. $\neg((\forall x)\neg\varphi) := (\exists x)\varphi$. A $(\exists x)$ lo llamamos el cuantificador existencial.

Definición 1.5. Definimos a la fórmula $(\exists_1 x)\varphi(x)$ como sigue:

$$(\exists_1 x)\varphi(x) := (\exists x)\varphi(x) \ \wedge \ (\forall x)(\forall y)(\varphi(x) \ \wedge \ \varphi(y) \to x = y)$$

Definición 1.6. Sean $\varphi \in \mathcal{FORM}$ y $x_i \in$ VAR:

1. Decimos que la variable x_i es libre en la fórmula φ si x_i no está al alcance de un cuantificador de la forma $(\forall x_i)$. Cuando ocurre lo contrario, decimos que x_i está acotada por el cuantificador $(\forall x_i)$.

2. Decimos que φ es una sentencia si todas las variables que ocurren en φ están acotadas.

Proposición 1.7. *Sea $A(t)$ una propiedad de términos. Si $A(x_i)$ se cumple para cada variable x_i, $A(a_i)$ se cumple para cada constante a_i y si $A(t_1), \ldots, A(t_n)$ se cumplen para cada $t_1, \ldots, t_n \in \mathcal{TERM}$ y f_k^n es un símbolo de aridad n implica que $f_k^n(A(t_1), \ldots, A(t_n))$ es válido, entonces $A(t)$ es válido para toda $t \in \mathcal{TERM}$.*

Proposición 1.8. *Sea $A(\varphi)$ una propiedad de fórmulas. Si:*

1. *$A(\varphi)$ se cumple para cada fórmula atómica φ,*

2. *Si $A(\varphi)$ y $A(\psi)$, entonces $A(\varphi \to \psi)$,*

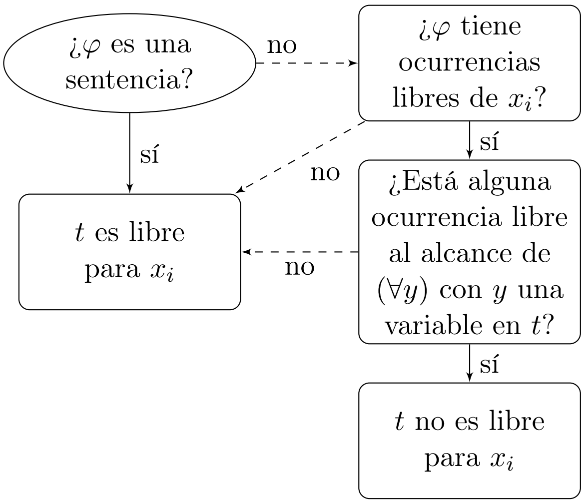
3. *Si $A(\varphi)$, entonces $A(\neg\varphi)$,*

4. *Si $A(\varphi)$ y $x_i \in VAR$, entonces $A((\forall x_i)\varphi)$,*

entonces $A(\varphi)$ para toda $\varphi \in \mathcal{FORM}$.

Definición 1.9. Sean $\varphi \in \mathcal{FORM}$, $t \in \mathcal{TERM}$ y $x_i \in VAR$. Diremos que t es libre para x_i en φ si ninguna ocurrencia libre de x_i en φ está al alcance de un cuantificador de la forma $(\forall)y$ donde $y \in VAR$ aparece en el término t.

En muchos resultados de lógica matemática, es recurrente preguntarse si un término t es libre para alguna variable x_i en una fórmula φ. El siguiente diagrama nos ayuda a responder esta pregunta de manera más sencilla.



Definición 1.10. Sea $\mathscr{L}$ un lenguaje de primer orden. Una interpretación $\mathfrak{M}$ de $\mathscr{L}$ consiste de los siguientes elementos:

1. Un conjunto no vacío D, llamado dominio de la interpretación.
2. Para cada símbolo predicativo de aridad n A_j^n, una relación $(A_j^n)^{\mathfrak{M}} \subseteq D^n$ de aridad n en D.
3. Para cada letra funcional f_j^n de aridad n, una función $(f_j^n)^{\mathfrak{M}} : D^n \to D$.
4. Para cada símbolo constante c de $\mathfrak{L}$, un elemento $(c)^{\mathfrak{M}} \in D$.

Definición 1.11. Sean $V : VAR \to D$ una función arbitraria que llamaremos valuación, y $\mathfrak{M}$ una interpretación de $\mathscr{L}$. Se define de manera recursiva $V' : \mathcal{TERM} \to D$ como sigue:

1. $V'(x_i) = V(x_i)$ para $x_i \in VAR$.
2. $V'(c) = c^{\mathfrak{M}}$ si c es constante.
3. $V'(f_j^n(t_1, \ldots, t_n)) = (f_j^n)^{\mathfrak{M}}(V'(t_1), \ldots, V'(t_n))$

A $V'(t)$ es llamada la valuación del término t.

Definición 1.12. Sean $\mathfrak{M}$ una interpretación, $V : VAR \to D$ una valuación y $V' : \mathcal{TERM} \to D$ la valuación de los términos. Se define $V^* : \mathcal{FORM} \to \{0, 1\}$ de manera recursiva como sigue:

1. Si $\varphi = A_i^n(t_1, \ldots, t_n)$, entonces

$$V^*(\varphi) = \begin{cases} 1 \quad \text{si} \quad (V'(t_1), \ldots, V'(t_n)) \in (A_i^n)^{\mathfrak{M}} \\ \\ 0 \qquad\qquad \text{en otro caso} \end{cases}$$

2. Si $\varphi = \neg\psi$, entonces

$$V^*(\varphi) = 1 - V^*(\psi) \qquad [V^*(\neg\psi) = 1 \text{ si y solo si } V^*(\psi) = 0]$$

3. Si $\varphi = \psi \to \gamma$, entonces

$$V^*(\varphi) = \begin{cases} 1 \quad \text{si} \quad V^*(\psi) \leq V^*(\gamma) \\ \\ 0 \qquad \text{en otro caso} \end{cases}$$

4. Si $\varphi = (\forall x_i)\psi$, entonces
   $V^*(\varphi) = 1$ si y solo si $V_0^*(\psi) = 1$ para cualquier $V_0 : VAR \longrightarrow D$ con $V_0 \restriction_{VAR\setminus\{x_i\}} = V$.

A $V^*(\varphi)$ lo llamamos la valuación de la fórmula φ.

Definición 1.13. Una fórmula φ es lógicamente válida si para cada estructura $\mathfrak{M}$ con dominio D y valuación $V : VAR \longrightarrow D$ se cumple que $V^*(\varphi) = 1$. Lo escribimos $\vDash_{\mathfrak{M}} \varphi$

Definición 1.14. Sea $\mathfrak{L}$ el lenguaje y $\mathcal{FORM}$ el conjunto de fórmulas bien formadas. Una teoría formal basada en $\mathfrak{L}$ consiste de los siguientes elementos:

1. Un conjunto de fórmulas, denominado conjunto de axiomas (cada fórmula se llamará un axioma de la teoría $\mathcal{T}$).
2. Un conjunto finito $\{R_i | i \in \{1, \ldots, n\}\}$ de relaciones, donde para cada $i \in \{1, \ldots, n\}$ se cumple que R_i es una relacion de aridad k_i en $\mathcal{FORM}$, es decir, $R_i \subseteq (\mathcal{FORM})^{k_i}$. Cada una de estas relaciones se denomina reglas de inferencia.

Observación 1.1. Llamamos a una teoría $\mathcal{T}$ una Teoría de Primer Orden siempre que esté basada en un lenguaje de primer orden y que su conjunto de axiomas incluya los axiomas del Cálculo Predicativo Clásico.

Definición 1.15. Sea $\mathfrak{M}$ una interpretación con dominio D y $V : VAR \longrightarrow D$ una valuación y $\varphi \in \mathcal{FORM}$.

i) Diremos que φ es verdadera para $\mathfrak{M}$ respecto de V si $V^*(\varphi) = 1$. En otro caso diremos que φ es falso respecto de V.

ii) Diremos que φ es verdadera para la interpretación $\mathfrak{M}$ si $V_0^*(\varphi) = 1$ para toda valuación $V_0 : VAR \longrightarrow D$.

iii) Diremos que φ es satisfacible en $\mathfrak{M}$ si existe $V_0 : VAR \longrightarrow D$ tal que $V_0^*(\varphi) = 1$.

iv) Diremos que φ es falsa para $\mathfrak{M}$ si no existe $V_0 : VAR \longrightarrow D$ tal que $V_0^*(\varphi) = 1$ ($V_0^*(\varphi) = 0$ para cada $V_0 : VAR \longrightarrow D$).

v) Si $\Gamma \subseteq \mathcal{FORM}$ es un conjunto de fórmulas, diremos que $\mathfrak{M}$ es un modelo para Γ si cada $\varphi \in \Gamma$ es verdadera para $\mathfrak{M}$.

Definición 1.16. Sea K una teoría de primer orden en el lenguaje $\mathfrak{L}$ y $\mathfrak{M}$ una interpretación de $\mathfrak{L}$. Decimos que $\mathfrak{M}$ es un modelo para K si los axiomas de K son verdaderas para $\mathfrak{M}$.

Definición 1.17. Sea K una teoría de primer orden en el lenguaje $\mathfrak{L}$, Decimos que una teoría K' es una extensión de K si todo teorema de K es teorema de K'

En la Teoría del Calculo Predicativo Clásico (y en general en cualquier teoría de primer orden) tenemos cinco esquemas de axiomas.

(A1) $\varphi \to (\psi \to \varphi)$.

(A2) $(\varphi \to (\psi \to \gamma)) \to ((\varphi \to \psi) \to (\varphi \to \gamma))$.

(A3) $(\neg\varphi \to \neg\psi) \to ((\neg\varphi \to \psi) \to \varphi)$.

(A4) $(\forall x_i)\varphi(x_i) \to \varphi(t)$ donde $\varphi(x_i)$ es una fórmula, t es un término que es libre para x_i en $\varphi(x_i)$ y $\varphi(t)$ se obtiene de sustituir las ocurrencias de x_i por t.

(A5) $(\forall x_i)(\varphi \to \psi) \to (\varphi \to (\forall x_i)\psi)$ si φ no admite ocurrencias libres de x_i.

Se tienen dos reglas de inferencia:

1. Modus Ponens (MP):
$$\frac{\begin{matrix}\varphi \to \psi \\ \varphi\end{matrix}}{\psi}$$
o de la misma manera
$$\frac{\begin{matrix}\varphi \\ \varphi \to \psi\end{matrix}}{\psi}$$

2. Generalización (Gen):
$$\frac{\varphi}{(\forall x_i)\varphi}$$

Definición 1.18. En una teoría de Primer Orden llamamos axiomas lógicos a los axiomas (A1)-(A5) y llamamos axiomas propios de la teoría a todos aquellos que se incluyan al definir la teoria.

Definición 1.19. Definimos la clausura de φ como la fórmula que surge de cuantificar todas la variables libres que tenga φ a traves de Gen

Definición 1.20. Sean $\Gamma \subseteq \mathcal{FORM}$ y $\varphi \in \mathcal{FORM}$. Diremos que existe una prueba formal para φ a partir del conjunto de hipótesis Γ, si existe una sucesión finita $\varphi_1, \varphi_2, \ldots, \varphi_n$ de fórmulas que cumple:

1. $\varphi_n = \varphi$

2. Para $1 \leq i \leq n$ se cumple alguna de las siguientes:

   - φ_i es un axioma o
   - $\varphi_i \in \Gamma$ o
   - Existen $j, k < i$ tales que $\varphi_k = \varphi_j \to \varphi_i$ y φ_i se obtiene de φ_j, φ_k aplicando MP.
   - $\varphi_i = (\forall x_k)\varphi_k$ con $k < i$ y φ_i se obtiene de φ_k aplicando Gen.

En este caso escribimos $\Gamma \vdash \varphi$.
Decimos que una fórmula φ es un teorema de la teoría cuando $\emptyset \vdash \varphi$ y escribimos únicamente $\vdash \varphi$.

Definición 1.21. Una teoría $\mathcal{T}$ es consistente si no existe una fórmula φ tal que $\vdash_{\mathcal{T}} \varphi$ y $\vdash_{\mathcal{T}} \neg\varphi$

Definición 1.22. Una teoría $\mathcal{T}$ se denomina completa si para cada fórmula φ, $\vdash_{\mathcal{T}} \varphi$ o $\vdash_{\mathcal{T}} \neg\varphi$

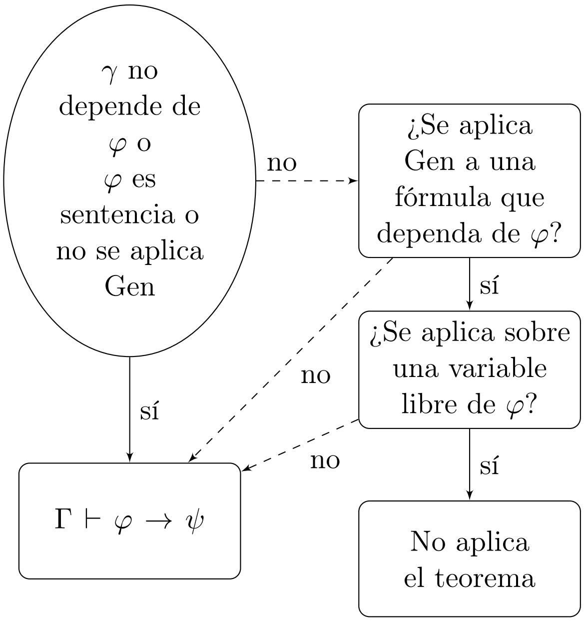
Definición 1.23. Sea φ una fórmula que pertenece a un conjunto $\Gamma \subseteq \mathcal{FORM}$ y suponga que $\gamma_1, \ldots, \gamma_n$ es una prueba formal de $\gamma = \gamma_n$ basada en Γ (es decir $\Gamma \vdash \gamma$. Para cada $1 \leq i \leq n$ diremos que γ_i depende de φ en la prueba si y solo si:

i) $\gamma_i = \varphi$ y la justificación en la prueba es que $\gamma_i \in \Gamma$.

ii) γ_i es consecuencia directa, por MP o Gen, de alguna fórmula (o fórmulas) donde alguna de ellas depende de φ en la prueba.

Teorema 1.24 (Teorema de la deducción)**.** *Si en alguna deducción que muestra que $\Gamma, \varphi \vdash \psi$, ninguna ocurrencia de Gen que se aplicó a alguna fórmula que depende de φ en la prueba, se aplicó introduciendo como variable cuantificada a una variable libre de φ, entonces se puede concluir que $\Gamma \vdash \varphi \to \psi$.*

El Teorema de la deducción (Teorema 1.24) es muy utilizado en numerosas pruebas que involucran a Teorías de primer orden. Es muy importante ser muy cuidadosos siempre que deseamos utilizarlo, el siguiente diagrama nos ayuda a responder de manera más sencilla cuando es posible aplicar el Teorema.



Metateoremas y reglas de deducción.

- Regla de particularización de (A4).
  Si t es libre para x en $\varphi(x)$ entonces

$$(\forall x)\varphi(x) \vdash \varphi(t).$$

- Regla existencial (E4).
  Sea t un término que es libre para x en la fórmula $\varphi(x)$ y sea $\varphi(t)$ la fórmula que se obtiene de sustituir todas las ocurrencias de x por t. entonces

$$\varphi(t) \vdash (\exists x)\varphi(x).$$

- Regla C.
  Al argumentar la validez de una propiedad o proposición en matemáticas, que incluye una fórmula del tipo $(\exists x)\varphi(x)$, es común utilizar una regla o argumento de la forma "Sea b tal que $\varphi(b)$". Continuamos con la demostración, empleando cuando sea necesario el hecho de que $\varphi(b)$ ocurre.
  Esta idea de elegir "un testigo" que satisface la propiedad la denominamos la Regla C.

Definición 1.25. Sean $\Gamma \subseteq \mathcal{FORM}$ y $\varphi \in \mathcal{FORM}$. Una deducción de φ mediante regla C, denotada por $\Gamma \vdash_C \varphi$, es una sucesión finita $\varphi_1, \ldots, \varphi_n$ de fórmulas tales que $\varphi_n = \varphi$ y se cumple lo siguiente:

1. Para cada $1 \leq i \leq n$:

   i. φ_i es un axioma ó
   ii. $\varphi_i \in \Gamma$ ó
   iii. φ_i se obtiene por MP o Gen aplicado a algunas fórmulas anteriores en la deducción ó
   iv. Existe $j < i$ talque $\varphi_j = (\exists x)\gamma(x)$ y $\varphi_i = \gamma(d)$ donde d es un nuevo símbolo constante.

2. Después de introducir el símbolo constante d, podemos emplearlo en lo sucesivo mediante las reglas del paso 1.

3. Ninguna aplicación de Gen se realiza usando alguna variable que es libre en alguna fórmula $(\exists x)\varphi(x)$ donde se aplicó la Regla C previamente.

4. φ no tiene alguna de las constantes introducidas en alguna aplicación de la Regla C.

Proposición 1.26. *Sean* $\Gamma \subseteq \mathcal{FORM}$ *y* $\varphi \in \mathcal{FORM}$. *Si* $\Gamma \vdash_C \varphi$ *entonces* $\Gamma \vdash \varphi$

Definición 1.27. Sean $x_i, x_j \in VAR$ tales que $x_i \neq x_j$ y sea $\varphi(x_i) \in \mathcal{FORM}$. Si $\varphi(x_j)$ se obtiene de $\varphi(x_i)$ sustituyendo todas las ocurrencias libres de x_i en $\varphi(x_i)$ por x_j, diremos que $\varphi(x_i)$ y $\varphi(x_j)$ son similares si x_j es libre para x_i en $\varphi(x_i)$ y $\varphi(x_i)$ no tiene ocurrencias libres de x_j

Proposición 1.28. *Si* $\varphi(x_i)$ *y* $\varphi(x_j)$ *son similares entonces*

$$\vdash (\forall x_i)\varphi(x_i) \leftrightarrow (\forall x_j)\varphi(x_j)$$

Proposición 1.29. *Sean* $\varphi, \beta(x), \beta(y) \in \mathcal{FORM}$. *Si* $\beta(x)$ *es similar a* $\beta(y)$, $(\forall x)\beta(x)$ *es subfórmula de* φ *y* φ' *resulta de reemplazar una o más ocurrencias de* $(\forall x)\beta(x)$ *en* φ *por* $(\forall y)\beta(y)$ *entonces*

$$\vdash \varphi \leftrightarrow \varphi'$$

Observación 1.2. Las Proposiciones 1.28 y 1.29 nos permiten hacer cambios de variables en fórmulas eligiendo variables a nuestra conveniencia, esto resultará útil en el desarrollo del trabajo, sobre todo cuando tengamos necesidad de utilizar el axioma (A4) en nuestras pruebas y necesitemos tener términos libres para variables, así, cuando tengamos una variable en las que no exista la certeza de que un término es libre para ella, ocupando estas proposiciones podemos elegir variables que lo sean.

Teorema 1.30. *Una teoría* K *es consistente si y solo si admite un modelo numerable.*

Teorema 1.31 (Teorema de Completitud de Gödel)**.** *Sea* $\varphi \in \mathcal{FORM}$ *entonces* $\vdash \varphi$ *si y solo si* $\vDash \varphi$.

Para los siguientes capítulos, todo lo que desarrollemos tomará como base lo descrito en este capítulo.

Capítulo 2

Teorías de Primer Orden con igualdad

Muchas veces cuando trabajamos con Teorías de Primer Orden, introducimos la relación " = " al lenguaje. De manera formal, se tiene que introducir un nuevo símbolo predicativo y nuevos axiomas que garanticen que este nuevo símbolo funcione de la manera correcta, es decir, que cuando lo interpretemos en algún modelo, la interpretación se comporte como la relación de igualdad del dominio. A estas teorías, las llamaremos Teorías de Primer Orden con Igualdad.

Definición 2.1. Sea K una teoría de Primer Orden que tiene como uno de sus símbolos predicativos a $A_1^2(t,s)$ que abreviaremos de aquí en adelante como $t = s$. Decimos que K es una teoría de primer orden con igualdad si las siguientes dos fórmulas son teoremas de K

(A6) $(\forall x_1)A_1^2(x_1, x_1)$ $[(\forall x_1)x_1 = x_1]$ **[Reflexividad de la igualdad]**

(A7) $A_1^2(x,y) \to (\beta(x,x) \to \beta(x,y))$ $[x = y \to (\beta(x,x) \to \beta(x,y))]$ **[Sustitución de la igualdad]**.
Donde $x, y \in VAR, \beta(x,x) \in \mathcal{FORM}$ y $\beta(x,y)$ surge de reemplazar en $\beta(x,x)$, algunas pero no necesariamente todas las ocurrencias libres de x por y, con la suposición de que y es libre para x en $\beta(x,x)$. Así $\beta(x,y)$ puede o no tener ocurrencias libres de x.

Veamos un ejemplo de cómo usaremos (A7) en el desarrollo del trabajo:

Supongamos que tenemos una teoría con igualdad K en la que las siguientes fórmulas son válidas

$$\varphi(x,x) := (w = yz + x), x = y.$$

Es decir, $\vdash_K \varphi(x,x)$ y $\vdash_K x = y$. Supongamos que nos gustaría demostrar que en la teoría K se cumple que $\vdash_K w = yz + y$. Para probar esto podemos emplear (A7).
Primero, construimos la fórmula

$$\varphi(x,y) := (w = yz + y)$$

Podemos notar que $\varphi(x,y)$ surge de sustituir en $\varphi(x,x)$ una ocurrencia libre de $x \in VAR$ por $y \in VAR$. Además y es libre para x en $\varphi(x,x)$ pues x no está al alcance de ningún cuantificador. Así que por (A7) se cumple que

$$\vdash_K x = y \to (\varphi(x,x) \to \varphi(x,y))$$

Pero como $\vdash_K x = y$, entonces aplicando MP tenemos que

$$\vdash_K \varphi(x,x) \to \varphi(x,y)$$

Pero como $\vdash_K \varphi(x,x)$, entonces aplicando MP concluimos que

$$\vdash_K \varphi(x,y)$$

Es decir $\vdash_K w = yz + y$ que es lo que queríamos probar. Así es como en lo sucesivo utilizaremos (A7) cuando trabajemos con teorías con igualdad.

Proposición 2.2. *Para una teoría con igualdad K se cumple que para $r, t \in \mathcal{TERM}$ y $\varphi(x,x) \in \mathcal{FORM}$:*

$$\vdash_K t = r \to (\varphi(t,t) \to \varphi(t,r))$$

donde $\varphi(t,r)$ surge de sustituir algunas, pero no necesariamente todas las ocurrencias de t por r.

Demostración. Como K es una teoría con igualdad, entonces se cumple que $\vdash_K x = y \to (\varphi(x,x) \to \varphi(x,y))$ donde $\varphi(x,y)$ surge de sustituir algunas, pero no necesariamente todas, las ocurrencias libres de x por y, donde y es libre para x en $\varphi(x,x)$. Ahora por Gen se cumple que $\vdash_K (\forall x)(x = y \to (\varphi(x,x) \to \varphi(x,y)))$. Sea $\gamma(x) := x = y \to (\varphi(x,x) \to \varphi(x,y))$

1. Si t es libre para x en $\gamma(x)$, entonces,por la regla de particularización (A4) se cumple que

$$(\forall x)\gamma(x) \vdash_K \gamma(t)$$

   y como sabemos que $\vdash_K (\forall x)\gamma(x)$, entonces

$$\vdash_K t = y \to (\varphi(t,t) \to \varphi(t,y))$$

2. Si t no es libre para x en $\gamma(x)$, entonces se tiene que alguna ocurrencia libre de x esta al alcance de un cuantificador $(\forall z)$ con z una variable que ocurre en el termino t. Ahora, consideremos $z_0 \in VAR$ que no ocurre en t y que z_0 no ocurra en $\gamma(x)$. Sea $\gamma(x, z_0)$ la fórmula que surge de sustituir todas las ocurrencias libres de z por z_0. Se cumple que $\gamma(x)$ y $\gamma(x, z_0)$ son similares pues:

   a. $\gamma(x)$ no tiene ocurrencias libres de z_0 pues z_0 no ocurre en $\gamma(x)$.

   b. z_0 es libre para z en $\gamma(x)$ pues al no ocurrir z_0 en $\gamma(x)$, entonces z no estará al alcance de $(\forall z_0)$.

   Así, por la Proposición 1.28 se cumple que

$$\vdash_K (\forall z)\gamma(x) \leftrightarrow (\forall z_0)\gamma(x, z_0) \tag{2.1}$$

   Sabemos que $\vdash_K \gamma(x)$, entonces, por Gen se cumple que $\vdash_K (\forall z)\gamma(x)$. Entonces por MP y por (2.1), se cumple que

$$\vdash_K (\forall z_0)\gamma(x, z_0)$$

   Como z_0 es libre para z_0 en la fórmula $\gamma(x, z_0)$ entonces por la regla de particularización (A4) se cumple que $\vdash_K \gamma(x, z_0)$,y por Gen, $\vdash_K (\forall x)\gamma(x, z_0)$
   Ahora, $\gamma(x, z_0)$ surge de sustituir todas las ocurrencias libres de z por z_0 en $\gamma(x)$ y como z_0 no ocurre en t se cumple que t es libre para x en la formula $\gamma(x, z_0)$, Así por la regla de particularización (A4) $\vdash_K \gamma(t, z_0)$, es decir

$$\vdash_K t = y \to (\varphi(t,t) \to \varphi(t,y))$$

De 1. y 2. concluimos entonces que $\vdash_K t = y \to (\varphi(t,t) \to \varphi(t,y))$.
Ahora, sea $\beta(y) := t = y \to (\varphi(t,t) \to \varphi(t,y))$, por Gen se tiene que $\vdash_K (\forall y)\beta(y)$, De manera análoga a 1. y 2. podemos analizar los casos en que r es libre para y en $\beta(y)$, y cuando no lo es; y así, usando regla de particularización (A4) podemos concluir que

$$\vdash_K t = r \to (\varphi(t,t) \to \varphi(t,r)$$

∎

Notación 2.1. En lo sucesivo, llamaremos (A7′) a la Proposición 2.2. siempre que sea utilizada.

Proposición 2.3. *En cualquier teoría con igualdad K se cumple que para $r, s, t \in \mathcal{TERM}$:*

a. $\vdash_K t = t$

b. $\vdash_K t = s \to s = t$

c. $\vdash_K t = s \to (s = r \to t = r)$

Demostración. Consideremos una teoría con igualdad y sean $t, r, s \in \mathcal{TERM}$.
a. Por (A6) se cumple que

$$\vdash_K (\forall x_1)x_1 = x_1$$

Ahora, t es libre para x_1 en $\varphi(x_1) := (x_1 = x_1)$ pues x_1 no está al alcance de ningún cuantificador universal, por lo que en particular no estará al alcance de los cuantificadores $(\forall z)$ donde $z \in VAR$ es una variable que aparece en el término t. Así que, por la regla de particularización (A4) se cumple que

$$(\forall x_1)\varphi(x_1) \vdash_K \varphi(t)$$

Y como $\vdash_K (\forall x_1)x_1 = x_1$, entonces concluimos que $\vdash_K \varphi(t)$, es decir

$$\vdash_K t = t$$

b. Sean $x, y \in VAR$ que no ocurren en t o s. Sea $\varphi(x, x) := (x = x)$ y $\varphi(x, y) := (y = x)$. Se cumple que y es libre para x en $\varphi(x, x)$ pues x no está al alcance de ningún cuantificador universal, así que por (A7) se cumple que $\vdash_K x = y \to (\varphi(x, x) \to \varphi(x, y))$, es decir
$\vdash_K x = y \to (x = x \to y = x)$. Notemos que:

1.	$x = y \to (x = x \to y = x)$	[(A7)]
2.	$(x = y \to (x = x \to y = x)) \to (x = x \to (x = y \to y = x))$ $[\vdash (\varphi \to (\psi \to \gamma)) \to (\psi \to (\varphi \to \gamma))]$	
3.	$x = x \to (x = y \to y = x)$	MP(1,2)
4.	$x = x$ [Como $x \in \mathcal{TERM}$, aplicamos *a.*]	
5.	$x = y \to y = x$	MP(3,4)
6.	$(\forall y)(x = y \to y = x)$	[Gen (5)]
7.	$(\forall x)(\forall y)(x = y \to y = x)$	[Gen (6)]

Ahora, si $\gamma(x) := (\forall y)(x = y \to y = x)$, se cumple que t es libre para x en $\gamma(x)$ pues x esta al alcance de $(\forall y)$ pero en t no ocurre la variable y. Así que, ocupando la regla (A4) tenemos que:

$$\vdash_K (\forall y)t = y \to y = t$$

Ahora, si $\gamma(y) := (t = y \to y = t)$, se cumple que s es libre para y en $\gamma(y)$ pues y no está al alcance de ningún cuantificador, entonces, ocupando la regla (A4) tenemos que:

$$\vdash_K t = s \to s = t$$

c. Sean $x, y, z \in VAR$ que no ocurren en t, s o r. Sea $\varphi(y, y) := (y = z)$ y $\varphi(y, x) := (x = z)$. Se cumple que x es libre para y en $\varphi(y, y)$ pues y no esta al alcance de ningún cuantificador universal, así que por (A7) se cumple que $\vdash_K y = x \to (\varphi(y, y) \to \varphi(y, x))$, es decir
$\vdash y = x \to (y = z \to x = z)$. Entonces:

1. $y = x \to (y = z \to x = z)$ [(A7)]
2. $x = y \to y = x$
   [Como $x, y \in \mathcal{TERM}$, aplicamos b.]
3. $(x = y \to y = x) \to ((y = x \to (y = z \to x = z)) \to (x = y \to (y = z \to x = z)))$
   $[\vdash (\varphi \to \psi) \to ((\psi \to \gamma) \to (\varphi \to \gamma))]$
4. $(y = x \to (y = z \to x = z)) \to (x = y \to (y = z \to x = z))$ MP(2,3)
5. $x = y \to (y = z \to x = z)$ MP(1,4)
6. $(\forall z)x = y \to (y = z \to x = z)$ [Gen (5)]
7. $(\forall y)(\forall z)x = y \to (y = z \to x = z)$ [Gen (6)]
8. $(\forall x)(\forall y)(\forall z)x = y \to (y = z \to x = z)$ [Gen (7)]

Ahora, si $\gamma(x) := (\forall y)(\forall z)x = y \to (y = z \to x = z)$, se cumple que t es libre para x en $\gamma(x)$ pues x esta al alcance de $(\forall y)$ y $(\forall z)$ pero en t no ocurre las variables y ni z. Así que, ocupando la regla (A4) tenemos que:

$$\vdash_K (\forall y)(\forall z)t = y \to (y = z \to t = z)$$

Ahora, si $\gamma(y) := (\forall z)t = y \to (y = z \to t = z)$, se cumple que s es libre para y en $\gamma(y)$ pues y esta al alcance de $(\forall z)$ pero en s no ocurre la variable x. Así que, ocupando la regla (A4) tenemos que:

$$\vdash_K (\forall z)t = s \to (s = z \to t = z)$$

Por último, si $\gamma(z) := (t = y \to (y = z \to t = z))$, se cumple que r es libre para z en $\gamma(z)$ pues z está al alcance de ningún cuantificador. Así que, ocupando la regla (A4) tenemos que:

$$\vdash_K t = s \to (s = r \to t = r)$$

■

Los siguientes dos resultados nos ayudan a simplificar el uso del esquema (A7) cuando trabajamos con teorías con igualdad.

Proposición 2.4. *Si K una teoría de primer orden en la que se cumple (A6) y que también se cumple (A7) para $\varphi(x, x)$ tal que $\varphi(x, x)$ es una fórmula atómica y no tiene constantes, entonces K es una teoría con igualdad, es decir, (A7) se satisface para toda $\varphi(x, x) \in \mathcal{FORM}$.*

Demostración. Veamos que (A7) se cumple para cualquier fórmula $\varphi(x, x)$.
Por hipótesis (A7) se cumple para las fórmulas atómicas que no tienen constantes. Notemos que en esta prueba podemos usar los resultados de la proposición anterior, pues siempre que ocupamos (A7) en la prueba, fue sobre fórmulas atómicas que no tenían constantes.
Hagamos la prueba por inducción sobre el número de cuantificadores y conectivos de la fórmula $\varphi(x, x)$.

1. Supongamos que $\varphi(x, x)$ tiene 0 conectivos y cuantificadores, entonces $\varphi(x, x)$ es una fórmula atómica.

   i) Si $\varphi(x, x)$ no tiene constantes, entonces por hipótesis se satisface (A7).

   ii) Si $\varphi(x, x)$ tiene constantes:
   Sin pérdida de generalidad supongamos que $\varphi(x, x)$ solo tiene una constante, digamos a_1 que será reemplazada por la variable z_1, así, $\varphi^*(x, x)$ surge de reemplazar las ocurrencias de a_1 en $\varphi(x, x)$ por z_1. Como $\varphi^*(x, x)$ es una fórmula sin constantes por hipótesis satisface (A7), así que:
   1. $x = y \to (\varphi^*(x, x) \to \varphi^*(x, y))$ [(A7)]
   2. $(\forall z_1)x = y \to (\varphi^*(x, x) \to \varphi^*(x, y))$ [Gen(1)]

Ahora si $\varphi(z_1) := (x = y \to (\varphi^*(x,x) \to \varphi^*(x,y)))$ se cumple que a_1 es libre para z_1 en $\varphi(z_1)$, entonces por la regla (A4)

$$(\forall z_1)\varphi(z_1) \vdash_K \varphi(a_1).$$

Es decir, se cumple la formula $\varphi(a_1)$ que surge de sustituir las ocurrencias de z_1 por a_1.
Pero $\varphi(a_1) := (x = y \to (\varphi(x,x) \to \varphi(x,y)))$, pues como
$\varphi(z_1) := (x = y \to (\varphi^*(x,x) \to \varphi^*(x,y)))$ las ocurrencias de z_1 son en
$\varphi^*(x,x)$ y $\varphi^*(x,y)$. Así, concluimos que

$$\vdash_K x = y \to (\varphi(x,x) \to \varphi(x,y)).$$

Por lo tanto, (A7) se cumple para cualquier fórmula atómica. Si $\varphi(x,x)$ tiene más de una constante, realizamos el mismo proceso al que hicimos con una sola constante.

2. Supongamos que (A7) se cumple para las fórmulas con $k < n$ conectivos y cuantificadores. Sea $\varphi(x,x) \in \mathcal{FORM}$ con n conectivos y cuantificadores. Vamos a demostrar que (A7) es válido para $\varphi(x,x)$.

   i) $\varphi(x,x) := \neg\alpha(x,x)$ con $\alpha(x,x) \in \mathcal{FORM}$
   $\alpha(x,x)$ tiene $n-1$ cuantificadores y conectivos. Si $\alpha(x,y)$ es la fórmula que surge de sustituir las ocurrencias libres de x por $y \in VAR$, $\alpha(x,y)$ tiene $n-1$ conectivos y cuantificadores. También x es libre para y en $\alpha(x,y)$ pues y no está al alcance de $(\forall x)$ pues siempre que sustituimos x por y era en ocurrencias libres de x.
   Como $n-1 < n$ entonces por hipótesis inductiva se cumple que:

   $$\vdash_K y = z \to (\alpha(x,y) \to \alpha(x,z)),$$

   donde $\alpha(x,z)$ es cualquier fórmula que cumple que z es libre para y en $\alpha(x,y)$ y se sustituyeron algunas pero no necesariamente todas las ocurrencias libre de y por z.
   Ya tenemos que x es libre para y en $\alpha(x,y)$ y que $\alpha(x,x)$ surge de sustituir todas las ocurrencias de y (que son libres) por x, así que:

   $$\vdash_K y = x \to (\alpha(x,y) \to \alpha(x,x)).$$

   Ahora:
   1. $y = x \to (\alpha(x,y) \to \alpha(x,x))$
   2. $(\alpha(x,y) \to \alpha(x,x)) \to (\neg\alpha(x,x) \to \neg\alpha(x,y))$
      [pues $\vdash_K (\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$]
   3. $[y = x \to (\alpha(x,y) \to \alpha(x,x))] \to [((\alpha(x,y) \to \alpha(x,x)) \to (\neg\alpha(x,x) \to \neg\alpha(x,y)))$
      $\to (y = x \to (\neg\alpha(x,x) \to \neg\alpha(x,y)))]$
      [pues $\vdash_K (\varphi \to \psi) \to ((\psi \to \gamma) \to (\varphi \to \gamma))$]
   4. $[((\alpha(x,y) \to \alpha(x,x)) \to (\neg\alpha(x,x) \to \neg\alpha(x,y)))$
      $\to (y = x \to (\neg\alpha(x,x) \to \neg\alpha(x,y)))]$
      [MP(1,3)]
   5. $y = x \to (\neg\alpha(x,x) \to \neg\alpha(x,y))$
      [MP(2,4)]
   6. $x = y \to y = x$
      [pues $\vdash_K t = r \to r = s$]
   7. $(x = y \to y = x)$
      $\to ((y = x \to (\neg\alpha(x,x) \to \neg\alpha(x,y))) \to (x = y \to (\neg\alpha(x,x) \to \neg\alpha(x,y))))$
      [pues $\vdash_K (\varphi \to \psi) \to ((\psi \to \gamma) \to (\varphi \to \gamma))$]
   8. $(y = x \to (\neg\alpha(x,x) \to \neg\alpha(x,y))) \to (x = y \to (\neg\alpha(x,x) \to \neg\alpha(x,y)))$
      [MP(6,7)]
   9. $x = y \to (\neg\alpha(x,x) \to \neg\alpha(x,y))$
      [MP(5,8)]

Por lo tanto

$$\vdash_K x = y \to (\varphi(x,x) \to \varphi(x,y))$$

ii) $\varphi(x,x) := \alpha(x,x) \to \gamma(x,x)$, donde $\alpha(x,x), \gamma(x,x) \in \mathcal{FORM}$.
$\alpha(x,x)$ tiene l conectivos y cuantificadores donde $l < n$ y $\gamma(x,x)$ tiene m conectivos y cuantificadores donde $m < n$, así que satisfacen la hipótesis inductiva.
Análogo al caso anterior ya vimos que si construimos $\alpha(x,y)$ y $\gamma(x,y)$ comprobamos que $\vdash_K y = x \to (\alpha(x,y) \to \alpha(x,x))$ y también $\vdash_K y = x \to (\gamma(x,y) \to \gamma(x,x))$ y como $\vdash_K x = y \to y = x$, tenemos que

$$\vdash_K x = y \to (\alpha(x,y) \to \alpha(x,x)) \text{ y } \vdash_K x = y \to (\gamma(x,y) \to \gamma(x,x))$$

Denotemos $\varphi := (x = y), \psi := \alpha(x,x), \psi_1 := \alpha(x,y), \sigma := \gamma(x,y), \sigma_1 := \gamma(x,x)$, entonces:

1. $\varphi \to (\psi_1 \to \psi)$
2. $\varphi \to (\sigma \to \sigma_1)$
3. $(\varphi \to (\psi_1 \to \psi)) \to [(\varphi \to (\sigma \to \sigma_1)) \to (\varphi \to ((\psi \to \sigma) \to (\psi_1 \to \sigma_1)))]$
   [Es una tautologia del cálculo predicativo]
4. $(\varphi \to (\sigma \to \sigma_1)) \to (\varphi \to ((\psi \to \sigma) \to (\psi_1 \to \sigma_1)))$ MP(1,3)
5. $\varphi \to ((\psi \to \sigma) \to (\psi_1 \to \sigma_1))$ MP(2,4)

Sustituyendo la notación tenemos que

$$\vdash_K x = y \to ((\alpha(x,x) \to \gamma(x,x)) \to (\alpha(x,y) \to \gamma(x,y))).$$

Es decir:

$$\vdash_K x = y \to (\varphi(x,x) \to \varphi(x,y))$$

iii) $\varphi(x,x) := (\forall z)\alpha(x,x,z)$ con $\alpha(x,x,z) \in \mathcal{FORM}$.
$\alpha(x,x,z)$ tiene $n-1$ conectivos y cuantificadores, así que por hipótesis de inducción se cumple que $\vdash_K x = y \to (\alpha(x,x,z) \to \alpha(x,y,z))$ donde $\alpha(x,y,z)$ surge de sustituir en $\alpha(x,x,z)$ algunas pero no necesariamente todas las ocurrencias libres de x por y, además y es libre para x en $\alpha(x,x,z)$. Aplicando Gen tenemos que
$\vdash_K (\forall z)(x = y \to (\alpha(x,x,z) \to \alpha(x,y,z)))$. Pero notemos que $\gamma := (x = y)$ no admite ocurrencias libres de z, entonces por (A5) se tiene que

$$\vdash_K (\forall z)(x = y \to (\alpha(x,x,z) \to \alpha(x,y,z))) \to (x = y \to (\forall z)(\alpha(x,x,z) \to \alpha(x,y,z)))$$

Aplicando MP

$$\vdash_K x = y \to (\forall z)(\alpha(x,x,z) \to \alpha(x,y,z))$$

Denotemos $\beta := (x = y), \psi := (\forall z)(\alpha(x,x,z) \to \alpha(x,y,z))$ y
$\gamma := ((\forall z)\alpha(x,x,z) \to (\forall z)\alpha(x,y,z))$, entonces:

1. $\beta \to \psi$
2. $\psi \to \gamma$ $[\vdash_K (\forall w)(\sigma \to \sigma_1) \to ((\forall w)\sigma \to (\forall w)\sigma_1)]$
3. $(\beta \to \psi) \to ((\psi \to \gamma) \to (\beta \to \gamma))$ [tautología del Cálculo Predicativo]
4. $(\psi \to \gamma) \to (\beta \to \gamma)$ [MP(1,3)]
5. $\beta \to \gamma$ [MP(2,4)]

Sustituyendo la notación tenemos que

$$\vdash_K x = y \to ((\forall z)\alpha(x,x,z) \to (\forall z)\alpha(x,y,z)).$$

Es decir:

$$\vdash_K x = y \to (\varphi(x,x) \to \varphi(x,y)).$$

Así podemos concluir que (A7) se satisface para $\varphi(x,x) \in \mathcal{FORM}$, por lo que K es una teoría con igualdad. ∎

La siguiente proposición es otra caracterización de las teorías con igualdad. Puede consultarse la prueba en la página 95 de [1].

Proposición 2.5. *Sea K una teoría de primer orden en la que se cumple (A6) y que los siguientes enunciados son verdaderos:*

a. *El esquema (A7) se cumple para cualquier fórmula atómica $\varphi(x,x)$ que no tiene constantes o letras funcionales y $\varphi(x,y)$ surge de reemplazar una ocurrencia de x por y.*

b. $\vdash_K x_k = y \to f_j^n(x_1,\dots,x_k,\dots,x_n) = f_j^n(x_1,\dots,y,\dots,x_n)$, *donde f_j^n es una letra funcional de K, $x_1,\dots,x_n,y \in VAR$ y $f_j^n(x_1,\dots,y,\dots,x_n)$ surge de reemplazar en $f_j^n(x_1,\dots,x_k,\dots,x_n)$ al menos una ocurrencia de x por y.*

Entonces K es una teoría con igualdad.

Ejemplo 1 (Teoría elemental de grupos G). Consideremos la letra predicativa $A_1^2(t,s)$ que abreviamos con $t = s$, la constante a_1 que abreviaremos como 0 y la letra funcional $f_1^2(t,s)$ que abreviaremos con $t+s$ y los conjuntos $\mathcal{FORM}$ y $\mathcal{TERM}$ los mismos que en el cálculo predicativo.
Los axiomas de la teoría de grupos son:

a. $x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$

b. $x_1 + 0 = x_1$

c. $(\forall x_1)(\exists x_2)x_1 + x_2 = 0$

d. $x_1 = x_1$

e. $x_1 = x_2 \to x_2 = x_1$

f. $x_1 = x_2 \to (x_2 = x_3 \to x_1 = x_3)$

g. $x_1 = x_2 \to (x_1 + x_3 = x_2 + x_3 \wedge x_3 + x_1 = x_3 + x_2)$

G es una teoría con igualdad pues:

i) $\vdash_G (\forall x_1)x_1 = x_1$
   1. $x_1 = x_1$ [axioma d]
   2. $(\forall x_1)x_1 = x_1$ [Gen (1)]

ii) Sea $\varphi(x,x) \in \mathcal{FORM}$ atómica sin constantes o letras funcionales y sea $\varphi(x,y)$ la fórmula que surge de sustituir una ocurrencia por y donde y es libre para x en $\varphi(x,x)$.
Como $\varphi(x,x)$ es atómica, entonces $\varphi(x,x) := A_1^2(x,z)$ con $x,z \in VAR$ pues $\varphi(x,x)$ no tiene constantes o letras funcionales.
Como $\varphi(x,x) := (x = z)$, entonces $\varphi(x,y) := (y,z)$. Queremos probar que $\vdash_G x = y \to (x = z \to y = z)$.
   1. $y = x \to (x = z \to y = z)$ [f.]
   2. $x = y \to y = x$ [e.]
   3. $(x = y \to y = x) \to ((y = x \to (x = z \to y = z)) \to (x = y \to (x = z \to y = z)))$ [$\vdash_G (\varphi \to \psi) \to ((\psi \to \gamma) \to (\varphi \to \gamma))$]
   4. $(y = x \to (x = z \to y = z)) \to (x = y \to (x = z \to y = z))$ [MP(2,3)]
   5. $x = y \to (x = z \to y = z)$ [MP(1,4)]

Por lo tanto (A7) se cumple para cualquier fórmula atómica sin constantes o letras funcionales donde $\varphi(x,y)$ surge de reemplazar una ocurrencia de x por y.

iii) Veamos que $\vdash_G x = y \to f_1^2(x, x_2) = f_1^2(y, x_2)$ donde $x, y, x_2 \in VAR$ y $f_1^2(y, x_2)$ surge de reemplazar una ocurrencia de x por y.
Queremos ver que $\vdash_G x = y \to x + x_2 = y + x_2$
1. $x = y \to (x + x_2 = y + x_2 \wedge x_2 + x = x_2 + y)$ [g.]
2. $(x + x_2 = y + x_2 \wedge x_2 + x = x_2 + y) \to (x + x_2 = y + x_2)$
[Pues $\vdash_G (\varphi \wedge \psi) \to \varphi$]
3. $(x = y \to (x + x_2 = y + x_2 \wedge x_2 + x = x_2 + y))$
$\to (((x + x_2 = y + x_2 \wedge x_2 + x = x_2 + y) \to (x + x_2 = y + x_2))$
$\to (x = y \to (x + x_2 = y + x_2)))$
[Pues $\vdash_G (\varphi \to \psi) \to ((\psi \to \gamma) \to (\varphi \to \gamma))$]
4. $((x + x_2 = y + x_2 \wedge x_2 + x = x_2 + y) \to (x + x_2 = y + x_2))$
$\to (x = y \to (x + x_2 = y + x_2))$
[MP(1,3)]
5. $x = y \to (x + x_2 = y + x_2)$ [MP(2,4)]

De i), ii) y iii), ocupando la proposición anterior podemos concluir que G es una teoría con igualdad.
Si a los axiomas de la teoría de grupos le agregamos el axioma h. $x_1 + x_2 = x_2 + x_1$, la nueva teoría que se forma es llamada la teoría de grupos abelianos.

Ejemplo 2 (Teoría elemental de campos F). Consideremos la letra predicativa $A_1^2(t, s)$ que abreviamos con $t = s$, las constantes a_1, a_2 que abreviaremos como 0 y 1 respectivamente, las letras funcionales $f_1^2(t, s)$ que abreviaremos con $t + s$ y $f_2^2(t, s)$ que abreviaremos con $t \cdot s$, y los conjuntos $\mathcal{FORM}$ y $\mathcal{TERM}$ los mismos que en el cálculo predicativo.
Como axiomas consideremos los incisos a.-h. del ejemplo anterior y agregamos los siguientes:

i. $x_1 = x_2 \to (x_1 \cdot x_3 = x_2 \cdot x_3 \wedge x_3 \cdot x_1 = x_3 \cdot x_2)$

j. $x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$

k $x_1 \cdot (x_2 + x_3) = (x_1 \cdot x_2) + (x_1 \cdot x_3)$

l. $x_1 \cdot x_2 = x_2 \cdot x_1$

m. $x_1 \cdot 1 = x_1$

n. $x_1 \neq 0 \to (\exists x_2) x_1 \cdot x_2 = 1$

o. $0 \neq 1$

F es una teoría con igualdad. En el ejemplo anterior usamos a.-g para demostrar que:

i) $(\forall x_1) x_1 = x_1$

ii) Si $\varphi(x, x) \in \mathcal{FORM}$ atómica sin constantes o letras funcionales y $\varphi(x, y)$ es la fórmula que surge de sustituir una ocurrencia por y donde y es libre para x en $\varphi(x, x)$, entonces se cumple que $x = y \to (\varphi(x, x) \to \varphi(x, y))$

iii) $x = y \to f_1^2(x, x_2) = f_1^2(y, x_2)$ donde $x, y, x_2 \in VAR$ y $f_1^2(y, x_2)$ surge de reemplazar una ocurrencia de x por y.

Solo nos falta demostrar que $\vdash_F x = y \to f_2^2(x, x_2) = f_2^2(y, x_2)$ donde $x, y, x_2 \in VAR$ y $f_2^2(y, x_2)$ surge de reemplazar una ocurrencia de x por y. Esta prueba es análoga al punto iii), así que concluimos que F es una teoría con igualdad.

Proposición 2.6. *Si K es una teoría con igualdad, entonces*

1. $\vdash_K t_k = u \to f_j^n(t_1, \ldots, t_k, \ldots, t_n) = f_j^n(t_1, \ldots, u, \ldots, t_n)$ *donde f_j^n es una letra funcional de K, $t_1, \ldots, t_n, u \in \mathcal{TERM}$ y $f_j^n(t_1, \ldots, u, \ldots, t_n)$ surge de reemplazar en $f_j^n(t_1, \ldots, t_k, \ldots, t_n)$ al menos una ocurrencia de t_k por u.*

2. $\vdash_K t_k = u \to (A_j^n(t_1, \ldots, t_k, \ldots, t_n) \to A_j^n(t_1, \ldots, u, \ldots, t_n))$ *donde A_j^n es símbolo predicativo de K, $t_1, \ldots, t_n, u \in \mathcal{TERM}$ y $A_j^n(t_1, \ldots, u, \ldots, t_n)$ surge de reemplazar en $A_j^n(t_1, \ldots, t_k, \ldots, t_n)$ al menos una ocurrencia de t_k por u.*

Demostración. 1. Sean $t_1, \ldots, t_n, u \in \mathcal{TERM}$. Como K es una teoría con igualdad, entonces por la Proposición 2.5 se cumple que $\vdash_K x_k = y \to f_j^n(x_1, \ldots, x_k, \ldots, x_n) = f_j^n(x_1, \ldots, y, \ldots, x_n)$ donde $x_1, \ldots, x_n, y \in VAR$. Por Gen se cumple que $\vdash_K (\forall x_k)(\forall y)(x_k = y \to f_j^n(x_1, \ldots, x_k, \ldots, x_n) = f_j^n(x_1, \ldots, y, \ldots, x_n))$. Denotemos como $\varphi(x_k, y) := (\forall y)(x_k = y \to f_j^n(x_1, \ldots, x_k, \ldots, x_n) = f_j^n(x_1, \ldots, y, \ldots, x_n))$. Sabemos que $\vdash_K (\forall x_k)\varphi(x_k, y)$. Sea $x'_k \in VAR$ que no ocurre en el término u y no es ninguna de las variables $x_1, \ldots, x_n$. Consideremos la fórmula $\varphi(x'_k, y) := (\forall y)(x'_k = y \to f_j^n(x_1, \ldots, x'_k, \ldots, x_n) = f_j^n(x_1, \ldots, y, \ldots, x_n))$. Es decir, $\varphi(x'_k, y)$ surge de sustituir todas las ocurrencias de x_k por x'_k en $\varphi(x_k, y)$. Notemos que $\varphi(x_k, y)$ y $\varphi(x'_k, y)$ son similares, pues:

i. $\varphi(x_k, y)$ no tiene ocurrencias libres de x'_k, pues x'_k no ocurre en $\varphi(x_k, y)$.

ii. x'_k es libre para x_k en $\varphi(x_k, y)$, pues x_k no está al alcance de $(\forall x'_k)$ en $\varphi(x_k, y)$.

Entonces, por la Proposición 1.28 se cumple que $\vdash_K (\forall x_k)\varphi(x_k, y) \leftrightarrow (\forall x'_k)\varphi(x'_k, y)$. Como sabíamos que $\vdash_K (\forall x_k)\varphi(x_k, y)$, entonces por MP tenemos que $\vdash_K (\forall x'_k)\varphi(x'_k, y)$, es decir,

$$\vdash_K (\forall x'_k)(\forall y)(x'_k = y \to f_j^n(x_1, \ldots, x'_k, \ldots, x_n) = f_j^n(x_1, \ldots, y, \ldots, x_n))$$

Entonces, se cumple que

$$\vdash_K (\forall y)(\forall x'_k)(x'_k = y \to f_j^n(x_1, \ldots, x'_k, \ldots, x_n) = f_j^n(x_1, \ldots, y, \ldots, x_n))$$

Denotemos como $\alpha(y) := (\forall x'_k)(x'_k = y \to f_j^n(x_1, \ldots, x'_k, \ldots, x_n) = f_j^n(x_1, \ldots, y, \ldots, x_n))$. Se tiene que u es libre para y en $\alpha(y)$ pues y está al alcance de $(\forall x'_k)$ pero x'_k no ocurre en u. Así, por la regla de particularización (A4) se cumple que $\vdash_K \alpha(u)$, es decir,

$$\vdash_K (\forall x'_k)(x'_k = u \to f_j^n(x_1, \ldots, x'_k, \ldots, x_n) = f_j^n(x_1, \ldots, u, \ldots, x_n))$$

Ahora, t_k es libre para x'_k en la fórmula $x'_k = u \to f_j^n(x_1, \ldots, x'_k, \ldots, x_n) = f_j^n(x_1, \ldots, u, \ldots, x_n)$, entonces por la regla de particularización (A4) se tiene que

$$\vdash_K t_k = u \to f_j^n(x_1, \ldots, t_k, \ldots, x_n) = f_j^n(x_1, \ldots, u, \ldots, x_n)$$

También, t_1 es libre para x_1 en la fórmula $t_k = u \to f_j^n(x_1, \ldots, t_k, \ldots, x_n) = f_j^n(x_1, \ldots, u, \ldots, x_n)$. Así, si aplicamos la regla de particularización (A4) tenemos que

$$\vdash_K t_k = u \to f_j^n(t_1, \ldots, t_k, \ldots, x_n) = f_j^n(t_1, \ldots, u, \ldots, x_n)$$

De la misma manera podemos aplicar la regla de particularización (A4) con las $n - 2$ variables restantes y podemos concluir que

$$\vdash_K t_k = u \to f_j^n(t_1, \ldots, t_k, \ldots, t_n) = f_j^n(t_1, \ldots, u, \ldots, t_n)$$

El inciso 2. se prueba de manera análoga al 1. ■

Observación 2.1. Algunos autores, véase [2] definen las teorías con igualdad como las teorías de primer orden que cumplen los siguientes axiomas:

(E6) $\vdash_K (\forall x)(x = x)$.

(E7) $\vdash_K t_k = u \to f_j^n(t_1, \dots, t_k, \dots, t_n) = f_j^n(t_1, \dots, u, \dots, t_n)$ donde f_j^n es una letra funcional de K, $t_1, \dots, t_n, u \in \mathcal{TERM}$ y $f_j^n(t_1, \dots, u, \dots, t_n)$ surge de reemplazar en $f_j^n(t_1, \dots, t_k, \dots, t_n)$ al menos una ocurrencia de t_k por u.

(E8) $\vdash_K t_k = u \to (A_j^n(t_1, \dots, t_k, \dots, t_n) \to A_j^n(t_1, \dots, u, \dots, t_n))$ donde A_j^n es símbolo predicativo de K, $t_1, \dots, t_n, u \in \mathcal{TERM}$ y $A_j^n(t_1, \dots, u, \dots, t_n)$ surge de reemplazar en $A_j^n(t_1, \dots, t_k, \dots, t_n)$ al menos una ocurrencia de t_k por u.

En este trabajo, basándonos en los axiomas (A6) y (A7) hemos demostrado la validez de (E7) y (E8). Así, cuando nos refiramos a teorías con igualdad, también podremos emplear en lo sucesivo dichos nuevos resultados para verificar que efectivamente estamos trabajando con una teoría con igualdad.

Definición 2.7. Sea K una teoría con igualdad y considere $\mathfrak{M}$ un modelo de K Sea $E = (A_1^2)^{\mathfrak{M}}$, donde $E \subseteq D^2$ y D es el dominio del modelo. Si en $\mathfrak{M}$ la relación E es la relación de igualdad del dominio D, entonces decimos que $\mathfrak{M}$ es un modelo normal de K.

Ejemplo 3. Consideremos la teoría elemental de grupos G y la siguiente interpretación de la teoría de grupos G:

I. El dominio sera el conjunto $\mathbb{Z}$

II. Para A_1^2 consideremos $(A_1^2)^{\mathfrak{M}} \subseteq \mathbb{Z}^2$ la relación de igualdad de los enteros.

III. Para f_1^2 y f_2^2 considere $(f_1^2)^{\mathfrak{M}} : \mathbb{Z}^2 \longrightarrow \mathbb{Z}$ tal que $(f_1^2)^{\mathfrak{M}}(n, m) = n + m$ y $(f_2^2)^{\mathfrak{M}} : \mathbb{Z}^2 \longrightarrow \mathbb{Z}$ tal que $(f_2^2)^{\mathfrak{M}}(n, m) = nm$

Si consideramos que los axiomas de esta teoría son verdaderos en esta interpretación, tenemos que $\mathfrak{M}$ es un modelo de la teoría. Como la interpretación de A_1^2 es la igualdad de los enteros, concluimos que $\mathfrak{M}$ es un modelo normal de G.

Lema 2.8. *Si K es una teoría con igualdad, entonces* $\vdash_K x_1 = y_1 \wedge x_2 = y_2 \to (\varphi(x_1, x_2) \to \varphi(y_1, y_2))$, *donde $\varphi(x_1, x_2) \in \mathcal{FORM}$ y $\varphi(y_1, y_2)$ surge de sustituir al menos una ocurrencia libre de x_1 y x_2 por y_1 e y_2 respectivamente, además y_1, y_2 son libres para x_1, x_2 respectivamente en $\varphi(x_1, x_2)$.*

Demostración. Sean $\varphi(x_1, x_2) \in \mathcal{FORM}$ y $\varphi(y_1, y_2)$ como se especifica en las hipótesis del lema. Probemos que $x_1 = y_1 \wedge x_2 = y_2 \vdash_K \varphi(x_1, x_2) \to \varphi(y_1, y_2)$.

1. $x_1 = y_1 \wedge x_2 = y_2$	[Hipótesis]
2. $x_1 = y_1 \wedge x_2 = y_2 \to x_1 = y_1$	[$\vdash_K \beta \wedge \gamma \to \beta$]
3. $x_1 = y_1$	[MP(1,2)]
4. $x_1 = y_1 \wedge x_2 = y_2 \to x_2 = y_2$	[$\vdash_K \beta \wedge \gamma \to \gamma$]
5. $x_2 = y_2$	[MP(1,4)]
6. $x_1 = y_1 \to (\varphi(x_1, x_2) \to \varphi(y_1, x_2))$	[(A7)]
7. $\varphi(x_1, x_2) \to \varphi(y_1, x_2)$	[MP(3,6)]

Notemos que $\varphi(y_1, x_2) \in \mathcal{FORM}$ y además surge de sustituir al menos una ocurrencia de x_1 por y_1 en $\varphi(x_1, x_2)$ y además se tiene que y_1 es libre para x_1 en $\varphi(x_1, x_2)$. Por hipótesis, y_2 es libre para x_2 en $\varphi(x_1, x_2)$ es decir, x_2 no está al alcance de $(\forall y_2)$ en $\varphi(x_1, x_2)$.Y como en $\varphi(y_1, x_2)$ solo sustituimos x_1 por y_1 entonces se sigue cumpliendo que x_2 no esta al alcance de $(\forall y_2)$ en $\varphi(y_1, x_2)$, es decir, y_2 es libre para x_2 en $\varphi(y_1, x_2)$. Así que, podemos utilizar (A7) en

$\varphi(y_1, x_2)$:

8. $x_2 = y_2 \to (\varphi(y_1, x_2) \to \varphi(y_1, y_2))$ [(A7)]
9. $\varphi(y_1, x_2) \to \varphi(y_1, y_2)$ [MP(5,8)]
10. $(\varphi(x_1, x_2) \to \varphi(y_1, x_2)) \to ((\varphi(y_1, x_2) \to \varphi(y_1, y_2)) \to (\varphi(x_1, x_2) \to \varphi(y_1, y_2)))$
pues $[\vdash_K (\beta \to \psi) \to ((\psi \to \gamma) \to (\beta \to \gamma))]$
11. $(\varphi(y_1, x_2) \to \varphi(y_1, y_2)) \to (\varphi(x_1, x_2) \to \varphi(y_1, y_2))$ [MP(7,10)]
12. $\varphi(x_1, x_2) \to \varphi(y_1, y_2)$ [MP(9,11)]

Donde $\varphi(y_1, y_2)$ surgió de sustituir al menos una ocurrencia libre de x_1 y x_2 por y_1 e y_2 respectivamente.Así:

$$x_1 = y_1 \wedge x_2 = y_2 \vdash_K \varphi(x_1, x_2) \to \varphi(y_1, y_2)$$

Como en la prueba nunca utilizamos (Gen), por el teorema de la deducción, concluimos que

$$\vdash_K x_1 = y_1 \wedge x_2 = y_2 \to (\varphi(x_1, x_2) \to \varphi(y_1, y_2))$$

■

Observación 2.2. Lo que hicimos en el Lema 2.8 fue extender el axioma (A7) a la sustitución de más de una variable; en este caso fue para sustituir dos, pero se puede replicar el mismo proceso para extender el axioma (A7) a un número n de variables, es decir

$$\vdash_K x_1 = y_1 \wedge x_2 = y_2 \wedge \ldots \wedge x_n = y_n \to (\varphi(x_1, x_2, \ldots, x_n) \to \varphi(y_1, y_2, \ldots, y_n))$$

Cuando hablamos de Teorías de Primer Orden con igualdad, usualmente pensamos que para un modelo $\mathfrak{M}$, la interpretación del símbolo predicativo $A_1^2(t, r)$ es la igualdad del dominio del modelo, pero no necesariamente es así; podemos tener teorías que al ser interpretadas, la relación $(A_1^2(t, r))^{\mathfrak{M}}$ sea algún otro tipo de relación. Veamos un ejemplo de esto.

Ejemplo 4. Sea K una teoría con igualdad con una letra funcional f_1^2, un símbolo predicativo A_1^2 y una constante a_1. Definamos la interpretación I de la siguiente manera:

i. El dominio de la interpretación es $\mathbb{Z}$.

ii. $(f_1^2)^I : \mathbb{Z}^2 \longrightarrow \mathbb{Z}$ tal que para $m, n \in \mathbb{Z}$, $(f_1^2)^I(m, n) = m + n \in \mathbb{Z}$.

iii. $(a_1)^I = 0 \in \mathbb{Z}$

iv. Para A_1^2 consideremos que $(A_1^2)^I \subseteq \mathbb{Z}^2$ es la relación de congruencia módulo 2, es decir, $(m, n) \in (A_1^2)^I \iff m \equiv n \text{ mód } 2$

Se cumple que I es un modelo para K. Verifiquemos que los axiomas descritos en la Observación 2.1 son verdaderos en la interpretación I. En efecto:

1. La interpretación de (A6) en I es $z \equiv z$ mód 2 y esta es verdadera para toda $z \in \mathbb{Z}$.

2. Verifiquemos que el esquema (E7) es verdadero en I. Como nuestra teoría solo tiene al símbolo funcional f_1^2, verificaremos que es verdadero (E7) para este. Tenemos que para $t_1, t_2, u \in \mathcal{TERM}$ y para $x, y, z \in \mathbb{Z}$:

   a. $\vdash_K t_1 = u \to f_1^2(t_1, t_2) = f_1^2(u, t_2)$ cuya interpretación en I es si $x \equiv y$ mód 2 entonces $x + z \equiv y + z$ mód 2 lo cual es verdad pues si $x \equiv y$ mód 2 entonces se cumple que $2|x - y$, necesitamos ver que $2|x + z - (y + z)$ lo cual es verdad pues $x + z - (y + z) = x - y$ y sabíamos que $2|x - y$.

   b. $\vdash_K t_2 = u \to f_1^2(t_1, t_2) = f_1^2(t_1, u)$ cuya interpretación en I es si $z \equiv y$ mód 2 entonces $x + z \equiv x + y$ mód 2 lo cual es verdadero pues si $z \equiv y$ mód 2 entonces $2|z - y$, y $2|x + z - (x + y)$ es verdadero pues $x + z - (x + y) = z - y$ y ya sabíamos que $2|z - y$.

Por tanto el esquema (E7) es verdadero para la interpretación I.

3. Verifiquemos que el esquema (E8) es verdadero en I. Como nuestra teoría solo tiene al símbolo predicativo A_1^2, verificaremos que es verdadero (E8) para este. Tenemos que para $t_1, t_2, u \in \mathcal{TERM}$ y para $x, y, z \in \mathbb{Z}$:

   A. $\vdash_K t_1 = u \to (t_1 = t_2 \to u = t_2)$ cuya interpretación en I es si $x \equiv y$ mód 2 entonces siempre que $x \equiv z$ mód 2 se cumple que $y \equiv z$ mód 2 lo cual es verdad pues como $x \equiv y$ mód 2 entonces existe $z_0 \in \mathbb{Z}$ tal que $2z_0 = x - y$, y como $x \equiv z$ mód 2 entonces existe $z_1 \in \mathbb{Z}$ tal que $2z_1 = x - z$, Así que $2z_1 - 2z_0 = x - z - x + y = y - z$, entonces $2(z_1 - z_0) = y - z$, por lo que existe $z_3 = (z_1 - z_0) \in \mathbb{Z}$ tal que $2z_3 = y - z$, es decir, $y \equiv z$ mód 2.

   B. $\vdash_K t_2 = u \to (t_1 = t_2 \to t_1 = u)$ cuya interpretación en I es si $z \equiv y$ mód 2 entonces siempre que $x \equiv z$ mód 2 se cumple que $x \equiv y$ mód 2 y de manera análoga a A., se tiene que es verdadera dicha interpretación.

   Por tanto el esquema (E8) es verdadero para la interpretación I.

Así, se cumple que I es un modelo de una teoría con igualdad K. Así, podemos notar que la interpretación del símbolo "$=$" en un modelo I no necesariamente es la igualdad del dominio del modelo, sino que puede ser otro tipo de relación que siga satisfaciendo los axiomas de las teorías con igualdad.

Ahora nos interesa responder la siguiente pregunta, ¿es posible obtener siempre un modelo normal para una teoría con igualdad? La respuesta es que sí bajo una condición, de hecho, si nosotros conocemos un modelo de una teoría, es posible construir a partir de ese modelo un modelo normal para la teoría. El siguiente resultado lo demuestra.

Proposición 2.9. *Si K es una teoría con igualdad, entonces todo modelo $\mathfrak{M}$ para K puede ser "contraído" a un modelo normal para K.*

Demostración. Sea $\mathfrak{M}$ un modelo de una teoría con igualdad K. Sea $E := (A_1^2)^{\mathfrak{M}}$ y D el dominio de $\mathfrak{M}$. Por la Proposición 2.3 se cumple que:

a. $\vdash t = t$ $[\vdash A_1^2(t, t)]$

b. $\vdash t = s \to s = t$ $[\vdash A_1^2(t, s) \to A_1^2(s, t)]$

c. $\vdash t = s \to (s = r \to t = r)$ $[\vdash A_1^2(t, s) \to (A_1^2(s, r) \to A_1^2(t, r))]$

Como $E \subseteq D^2$ es la interpretación del símbolo A_1^2 en $\mathfrak{M}$, entonces se nos garantiza que, para $x, y, z \in D$:

a. $(x, x) \in E$

b. $(x, y) \in E \to (y, x) \in E$

c. $(x, y) \in E \to ((y, z) \in E \to (x, z) \in E)$

Por lo que $E := (A_1^2)^{\mathfrak{M}}$ es una relación de equivalencia en el dominio D. Así que, podemos construir el conjunto de clases de equivalencia determinadas por E en el dominio D, lo denotaremos con $D^* := D/E$.
Vamos a construir una nueva interpretación de K, que llamaremos $\mathfrak{M}^*$.

i) El dominio de $\mathfrak{M}^*$ sera D^*

ii) Para cualquier letra predicativa A_j^n, $b_1, \ldots, b_n \in D$ y $[b_1], \ldots, [b_n] \in D^*$ diremos que $([b_1], \ldots, [b_n]) \in (A_j^n)^{\mathfrak{M}^*}$ si y solo si $(b_1, \ldots, b_n) \in (A_j^n)^{\mathfrak{M}}$.
Esta definición no depende de los representantes que elijamos en D pues si suponemos que para $i \in \{1, \ldots, n\}$ se cumple que $x_i = y_i$, entonces, como $A_j^n(x_1, \ldots, x_n) \in \mathcal{FORM}$, por la Observación 2.2 tenemos que

$$\vdash x_1 = y_1 \wedge \ldots \wedge x_n = y_n \to (A_j^n(x_1, \ldots, x_n) \to A_j^n(y_1, \ldots, y_n))$$

y también que

$$\vdash x_1 = y_1 \wedge \ldots \wedge x_n = y_n \to (A_j^n(y_1, \ldots, y_n) \to A_j^n(x_1, \ldots, x_n)),$$

entonces tenemos que

$$\vdash x_1 = y_1 \wedge \ldots \wedge x_n = y_n \to (A_j^n(x_1, \ldots, x_n) \to A_j^n(y_1, \ldots, y_n)) \wedge (A_j^n(y_1, \ldots, y_n) \to A_j^n(x_1, \ldots, x_n))$$

Pues sabemos que si $\alpha, \beta, \gamma \in \mathcal{FORM}$ y se cumple que $\vdash \alpha \to \beta$ y $\vdash \alpha \to \gamma$, entonces $\vdash \alpha \to \beta \wedge \gamma$.Así podemos concluir que

$$\vdash x_1 = y_1 \wedge \ldots \wedge x_n = y_n \to (A_j^n(x_1, \ldots, x_n) \leftrightarrow A_j^n(y_1, \ldots, y_n))$$

Es decir, la definición no depende de los representantes que elegimos.

iii) Para cualquier letra funcional f_j^n, $b_1, \ldots, b_n \in D$ y $[b_1], \ldots, [b_n] \in D^*$ sea $(f_j^n)^{\mathfrak{M}^*}([b_1], \ldots, [b_n]) = [(f_j^n)^{\mathfrak{M}}(b_1, \ldots, b_n)]$.
Veamos que esta definición no depende de los representantes que elijamos en D.
Denotemos por $\varphi(x_1, \ldots, x_n) := (f_j^n(x_1, \ldots, x_n) = f_j^n(x_1, \ldots, x_n))$.
Queremos ver que $\vdash x_1 = y_1 \wedge \ldots \wedge x_n = y_n \to f_j^n(x_1, \ldots, x_n) = f_j^n(y_1, \ldots, y_n)$, demostremos que $x_1 = y_1 \wedge \ldots \wedge x_n = y_n \vdash f_j^n(x_1, \ldots, x_n) = f_j^n(y_1, \ldots, y_n)$. Notemos que $\varphi(y_1, \ldots, y_n) := (f_j^n(x_1, \ldots, x_n) = f_j^n(y_1, \ldots, y_n))$ surge de sustituir algunas ocurrencias libres de x_i por y_i para $i \in \{1, \ldots, n\}$ en $\varphi(x_1, \ldots, x_n)$ entonces por la Observación 2.2 tenemos que

$$\vdash x_1 = y_1 \wedge \ldots \wedge x_n = y_n \to (\varphi(x_1, \ldots, x_n) \to \varphi(y_1, \ldots, y_n))$$

1. $x_1 = y_1 \wedge \ldots \wedge x_n = y_n \to (\varphi(x_1, \ldots, x_n) \to \varphi(y_1, \ldots, y_n))$
2. $x_1 = y_1 \wedge \ldots \wedge x_n = y_n$ [Hipótesis]
3. $\varphi(x_1, \ldots, x_n) \to \varphi(y_1, \ldots, y_n)$ [MP(1,2)]
4. $f_j^n(x_1, \ldots, x_n) = f_j^n(x_1, \ldots, x_n)$ [$\vdash t = t$]
5. $\varphi(x_1, \ldots, x_n)$ [Abreviación de 4]
6. $\varphi(y_1, \ldots, y_n)$ [MP(3,5)]

Es decir, tenemos que $x_1 = y_1 \wedge \ldots \wedge x_n = y_n \vdash f_j^n(x_1, \ldots, x_n) = f_j^n(y_1, \ldots, y_n)$, así por el teorema de la deducción, tenemos que

$$\vdash x_1 = y_1 \wedge \ldots \wedge x_n = y_n \to f_j^n(x_1, \ldots, x_n) = f_j^n(y_1, \ldots, y_n)$$

Es decir, la definición no depende de los representantes que elegimos.

iv) Para cada constante a_i, sea $(a_i)^{\mathfrak{M}^*} = [(a_i)^{\mathfrak{M}}]$

La relación $E^* := (A_1^2)^{\mathfrak{M}^*}$ es la relación de identidad de D^*. Solo nos resta ver que la interpretación $\mathfrak{M}^*$ es un modelo para K. El siguiente lema nos ayudara a resolver esta ultima parte.

Lema 2.10. *Sean* $(b_i)_{i \in \mathbb{N}} \subseteq D$ *y* $([b_i])_{i \in \mathbb{N}} \subseteq D^*$. *Sean* $S : VAR \longrightarrow D$ *cualquier valuación tal que* $S(x_i) = b_i$ *y sea* $S' : VAR \longrightarrow D^*$ *tal que* $S'(x_i) = [S(x_i)] = [b_i]$. *Entonces* $\varphi \in \mathcal{FORM}$ *se satisface en* $\mathfrak{M}$ *para cualquier* S *si y solo si* φ *se satisface en* $\mathfrak{M}^*$ *por* S'.

Demostración. Para $S : VAR \longrightarrow D$ por la Definición 1.11 podemos obtener de manera recursiva $S^* : \mathcal{TERM} \longrightarrow D$, la valuación de términos respecto de S. De la misma manera, para $S' : VAR \longrightarrow D^*$ obtenemos la valuación de términos respecto de S' $(S')^* : \mathcal{TERM} \longrightarrow D$.

Afirmamos que para $t \in \mathcal{TERM}$, $(S')^*(t) = [S^*(t)]$. Veamos que se cumple utilizando inducción sobre la complejidad del término t.

1. Si $t := x_i \in VAR$, entonces $(S')^*(x_i) = S'(x_i) = [b_i]$. Pero $S^*(x_i) = S(x_i) = b_i$, por lo que $(S')^*(x_i) = [S^*(x_i)]$.
2. Si $t := c$ una constante del lenguaje, entonces $(S')^*(c) = c^{\mathfrak{M}^*}$.
   Pero sabemos que $c^{\mathfrak{M}^*} = [c^{\mathfrak{M}}]$, ademas $S^*(c) = c^{\mathfrak{M}}$, por lo que $(S')^*(c) = [S^*(c)]$.
3. Si $t := f_i^n(t_1, \ldots, t_n)$ donde $t_1, \ldots, t_n \in \mathcal{TERM}$ y para $i \in \{1, \ldots, n\}$ $(S')^*(t_i) = [S^*(t_i)]$, entonces

$$\begin{aligned}
(S')^*(f_i^n(t_1, \ldots, t_n)) &= (f_i^n)^{\mathfrak{M}^*}((S')^*(t_1), \ldots, (S')^*(t_n)) \\
&= (f_i^n)^{\mathfrak{M}^*}([S^*(t_1)], \ldots, [S^*(t_n)]) && \text{[HI]} \\
&= [(f_i^n)^{\mathfrak{M}}(S^*(t_1), \ldots, S^*(t_n))] && \text{[definición de } (f_i^n)^{\mathfrak{M}^*}\text{]} \\
&= [S^*(f_i^n(t_1, \ldots, t_n))]
\end{aligned}$$

   Por lo que $(S')^*(f_i^n(t_1, \ldots, t_n)) = [S^*(f_i^n(t_1, \ldots, t_n))]$

De 1., 2. y 3. podemos concluir que para $t \in \mathcal{TERM}$, $(S')^*(t) = [S^*(t)]$.
Ahora, por la Definición 1.12 para S^* podemos obtener de manera recursiva
$V_{S^*} : \mathcal{FORM} \longrightarrow \{0, 1\}$, la valuación sobre las fórmulas respecto de S^*. De la misma manera, para $(S')^*$, de manera recursiva obtenemos $V_{(S')^*} : \mathcal{FORM} \longrightarrow \{0, 1\}$.
Probaremos el lema por inducción sobre la complejidad de la fórmula φ.

I. $\varphi := (A_i^n)(t_1, \ldots, t_n)$.
   Sea $S : VAR \longrightarrow D$. Supongamos que φ se satisface en $\mathfrak{M}$ por S.
   Demostremos que φ se satisface en $\mathfrak{M}^*$ por S', es decir, verifiquemos que $V_{(S')^*}(\varphi) = 1$.
   Como φ se satisface en $\mathfrak{M}$ por S, entonces, $V_{S^*}(\varphi) = 1$, entonces,
   $(S^*(t_1), \ldots, S^*(t_n)) \in (A_i^n)^{\mathfrak{M}}$, así que $([S^*(t_1)], \ldots, [S^*(t_n)]) \in (A_i^n)^{\mathfrak{M}^*}$ pues así fue como definimos $(A_i^n)^{\mathfrak{M}^*}$. Pero sabemos que $([S^*(t_1)], \ldots, [S^*(t_n)]) = ((S')^*(t_1), \ldots, (S')^*(t_n))$ pues para $i \in \{1, \ldots, n\}$ se tiene que $(S')^*(t_i) = [S^*(t_i)]$. Por lo que concluimos que $((S')^*(t_1), \ldots, (S')^*(t_n)) \in (A_i^n)^{\mathfrak{M}^*}$, es decir

$$V_{(S')^*}(\varphi) = 1$$

   De manera análoga si suponemos que φ se satisface en $\mathfrak{M}^*$ por S', se concluye que φ se satisface en $\mathfrak{M}$ por S.

II. $\varphi := \neg\psi$ y sea $S : VAR \longrightarrow D$.
   Supongamos que ψ se satisface en $\mathfrak{M}$ para cualquier $T : VAR \longrightarrow D$ si y solo si ψ se satisface en $\mathfrak{M}^*$ por T'.
   Demostremos que $\neg\psi$ se satisface en $\mathfrak{M}$ por S si y solo si $\neg\psi$ se satisface en $\mathfrak{M}^*$ por S'.
   Supongamos que $\neg\psi$ se satisface en $\mathfrak{M}$, entonces $V_{S^*}(\neg\psi) = 1$, entonces $V_{S^*}(\psi) = 0$, es decir, ψ no se satisface en $\mathfrak{M}$ por S, así que por hipótesis inductiva, tenemos que ψ no se satisface en $\mathfrak{M}^*$ por S', entonces $V_{(S')^*}(\psi) = 0$.
   Sabemos también que $V_{(S')^*}(\neg\psi) = 1 - V_{(S')^*}(\psi) = 1 - 0 = 1$, por lo que $V_{(S')^*}(\neg\psi) = 1$, es decir, $\neg\psi$ se satisface en $\mathfrak{M}^*$ por S'.
   De manera análoga, si suponemos que $\neg\psi$ se satisface en $\mathfrak{M}^*$ por S', concluimos que $\neg\psi$ se satisface en $\mathfrak{M}$ por S.

III. $\varphi := (\psi \rightarrow \gamma)$ y sea $S : VAR \longrightarrow D$.
Supongamos que ψ se satisface en $\mathfrak{M}$ para cualquier $T : VAR \longrightarrow D$ si y solo si ψ se satisface en $\mathfrak{M}^*$ por T' y también supongamos que γ se satisface en $\mathfrak{M}$ para cualquier $R : VAR \longrightarrow D$ si y solo si γ se satisface en $\mathfrak{M}^*$ por R'.
Demostremos que φ se satisface en $\mathfrak{M}$ por S si y solo si φ se satisface en $\mathfrak{M}^*$ por S'.
Supongamos que φ se satisface en $\mathfrak{M}$ por S, entonces $V_{S*}(\psi \rightarrow \gamma) = 1$, es decir, $V_{S*}(\psi) \leq V_{S*}(\gamma)$

a) Si $V_{S*}(\psi) = 1$, como $V_{S*}(\psi) \leq V_{S*}(\gamma)$, entonces $V_{S*}(\gamma) = 1$, así que ψ se satisface en $\mathfrak{M}$ por S y γ se satisface en $\mathfrak{M}$ por S, así que por hipótesis inductiva se tiene que ψ se satisface en $\mathfrak{M}^*$ por S' y γ se satisface en $\mathfrak{M}^*$ por S', es decir, $V_{(S')^*}(\psi) = 1 = V_{(S')^*}(\gamma) = 1$, así que $V_{(S')^*}(\psi) \leq V_{(S')^*}(\gamma)$, por lo que $V_{(S')^*}(\psi \rightarrow \gamma) = 1$

b) Si $V_{S*}(\psi) = 0$, entonces ψ no se satisface en $\mathfrak{M}$ por S, así por hipótesis inductiva, ψ no se satisface en $\mathfrak{M}^*$ por S', es decir, $V_{(S')^*}(\psi) = 0$, entonces $V_{(S')^*}(\psi) = 0 \leq V_{(S')^*}(\gamma)$, por lo que $V_{(S')^*}(\psi \rightarrow \gamma) = 1$

De a) y b) concluimos que φ se satisface en $\mathfrak{M}^*$ por S'.
De manera análoga, si suponemos que φ se satisface en $\mathfrak{M}^*$ por S' se concluye que φ se satisface en $\mathfrak{M}$ por S.

IV. $\varphi := (\forall x_i)\psi$ con $x_i \in VAR$ y sea $S : VAR \longrightarrow D$.
Supongamos que ψ se satisface en $\mathfrak{M}$ para cualquier R si y solo si ψ se satisface en $\mathfrak{M}^*$ por R'
Demostremos que φ se satisface en $\mathfrak{M}$ por S si y solo si φ se satisface en $\mathfrak{M}^*$ por S'.
Supongamos que φ se satisface en $\mathfrak{M}$ por S, entonces $V_{S^*}(\varphi) = 1$, es decir, $V_{S_0^*}(\psi) = 1$ para $S_0 : VAR \longrightarrow D$ tal que $S_0 \restriction_{VAR\setminus\{x_i\}} = S \restriction_{VAR\setminus\{x_i\}}$.
Demostremos que φ se satisface en $\mathfrak{M}^*$ por S'.
Veamos que se cumple que $V_{(S')^*}(\varphi) = 1$, es decir, sea $T : VAR \longrightarrow D^*$ tal que $T \restriction_{VAR\setminus\{x_i\}} = S' \restriction_{VAR\setminus\{x_i\}}$.
Veamos que $V_{T^*}(\psi) = 1$
Notemos que para $y_i \in VAR \setminus \{x_i\}$ se cumple que $T(y_i) = S'(y_i) = [S(y_i)] = [b_i]$, además, para $x_i \in VAR$ tenemos que $T(x_i) = [z]$ para algún $z \in D$ pues $T : VAR \longrightarrow D^*$, en síntesis tenemos que:

$$T(y) = \begin{cases} [S(y)] & \text{si} \quad y \neq x_i \\ [z] & \text{si} \quad y = x_i \end{cases}$$

Definamos $S_0 : VAR \longrightarrow D$ tal que

$$S_0(y) = \begin{cases} S(y) & \text{si} \quad y \neq x_i \\ z & \text{si} \quad y = x_i \end{cases}$$

Por como definimos S_0 tenemos que $S_0 \restriction_{VAR\setminus\{x_i\}} = S \restriction_{VAR\setminus\{x_i\}}$, y como por hipótesis φ se satisface en $\mathfrak{M}$ por S, entonces, $V_{S_0^*}(\psi) = 0$, es decir, tenemos que ψ se satisface en $\mathfrak{M}$ por S_0, entonces si ocupamos la hipótesis de inducción, inferimos que ψ se satisface en $\mathfrak{M}^*$ por S_0', es decir, $V_{(S_0')^*}(\psi) = 1$ donde $S_0' : VAR \longrightarrow D^*$ es tal que $S_0'(x_i) = [S_0(x_i)]$.

Vamos a ver ahora que $T = S_0'$.
Sea $y \in VAR$.

1. Si $y \neq x_i$, entonces $T(y) = [S(y)]$ y también $S_0(y) = S(y)$, así que $T(y) = [S_0(y)] = S_0'(y)$
2. Si $y = x_i$ entonces $T(y) = [z]$ y además $S_0(y) = z$, por lo que $T(y) = [S_0(y)] = S_0'(y)$

Así, se tiene que para $y \in VAR$, $T(y) = S'_0(y)$, es decir $T = S'_0$ y como $V_{(S'_0)^*}(\psi) = 1$, entonces concluimos que $V_{T^*}(\psi) = 1$.
Entonces φ se satisface en $\mathfrak{M}^*$ por S'.
De manera análoga si suponemos que φ se satisface en $\mathfrak{M}^*$ por S' podemos concluir que φ se satisface en $\mathfrak{M}$ por S.

Así que se cumple que para $\varphi \in \mathcal{FORM}$ y para cualquier $S : VAR \longrightarrow D$, φ se satisface en $\mathfrak{M}$ por S si y solo si φ se satisface en $\mathfrak{M}^*$ por S'. ∎

Con el Lema 2.10 demostrado, veamos que efectivamente $\mathfrak{M}^*$ es un modelo para K.
Demostremos que si φ es verdadera para $\mathfrak{M}$ entonces φ es verdadera para $\mathfrak{M}^*$.
Supongamos que φ es verdadera para $\mathfrak{M}$, entonces para toda $S : VAR \longrightarrow D$ $V_{S^*}(\varphi) = 1$.
Sea $T : VAR \longrightarrow D^*$.
Veamos que $V_{T^*}(\varphi) = 1$.
Notemos que para $x_i \in VAR$ se tiene que $T(x_i) = [b_i]$ con $b_i \in D$. Entonces, definamos $S_0 : VAR \longrightarrow D$ tal que $S_0(x_i) = b_i$, por hipótesis tenemos que $V_{S_0^*}(\varphi) = 1$. Además por el lema anterior, se cumple que $V_{(S'_0)^*}(\varphi) = 1$ donde $S'_0 : VAR \longrightarrow D^*$ tal que $S'_0(x_i) = [S_0(x_i)] = [b_i] = T(x_i)$, por lo que $T = S'_0$, y como $V_{(S'_0)^*}(\varphi) = 1$, entonces $V_{(T)^*}(\varphi) = 1$.

Por lo tanto, φ es verdadera para $\mathfrak{M}^*$.
Ahora, como $\mathfrak{M}$ es modelo para K, entonces todos los axiomas de K son verdaderos para $\mathfrak{M}$, así que, podemos concluir que los axiomas de K son verdaderos para $\mathfrak{M}^*$, así que, concluimos que $\mathfrak{M}^*$ es modelo para K.
Así que, hemos encontrado un modelo normal para K. ∎

Observación 2.3. En la Proposición 2.9 nos referimos al termino de "contraer" el modelo $\mathfrak{M}$ a un modelo normal $\mathfrak{M}^*$ debido a que, cuando realizamos la prueba, partimos de un dominio arbitrario D del modelo $\mathfrak{M}$, y a partir de este, construimos el conjunto de clases de equivalencia respecto a la relación E, a este conjunto lo llamamos D^* y es el nuevo dominio de nuestra nueva interpretación, además D^* es un conjunto que podría ser finito, así el término de "contraído" se refiere a que dependiendo de nuestro dominio D, D^* puede ser finito.

Corolario 1. *Si K es una teoría con igualdad consistente, entonces K tiene un modelo normal finito o numerable.*

Demostración. Como K es consistente, entonces por el Teorema 1.30, K tiene un modelo numerable $\mathfrak{M}$. Como K es una teoría con igualdad, por la Proposición 2.9 podemos "contraer" $\mathfrak{M}$ a un modelo normal $\mathfrak{M}^*$ para K.
Como $\mathfrak{M}$ es numerable, entonces su dominio D es un conjunto numerable, así que $\mathfrak{M}^*$ es finito o numerable, pues el dominio D^*, que es el conjunto de clases de equivalencia de la relación en D es numerable o finito.
Por lo tanto toda teoría con igualdad consistente K, tiene un modelo normal finito o numerable. ∎

Teorema 2.11. *Cualquier teoría con igualdad K que tiene un modelo normal $\mathfrak{M}$ infinito, tiene un modelo normal numerable.*

Demostración. Sea K' la teoria que surge de tomar el lenguaje y los axiomas de la teoría K y añadiremos lo siguiente:

I. Un conjunto de nuevas constantes $\{b_i | i \in \mathbb{N}\}$.

II. Para $i \neq j$ añadimos los axiomas $\neg A_1^2(b_i, b_j)$ (que abreviamos como $b_i \neq b_j$).

Veamos que K' es consistente.
Si K' no fuera consistente, entonces existe $\varphi \in \mathcal{FORM}$ donde φ es una fórmula de K tal que $\vdash_{K'} \varphi \wedge \neg\varphi$. Entonces existe una prueba formal en K' para $\varphi \wedge \neg\varphi$, es decir, existe una sucesión finita $\varphi_1, \ldots, \varphi_n \in \mathcal{FORM}$ tal que:

(a) $\varphi_n := \varphi \wedge \neg\varphi$

(b) Para $1 \leq i \leq n$ se cumple alguna de las siguientes:

i) φ_i es un axioma o

ii) existen $j, k < i$ tales que $\varphi_k := \varphi_j \rightarrow \varphi_i$ y φ_i se obtiene de φ_j y φ_k aplicando MP o

iii) $\varphi_i := (\forall x_p)\varphi_k$ con $k < i$ y φ_i se obtiene aplicando Gen a φ_k

Así que la prueba $\varphi_1, \ldots, \varphi_n$ ocupa un número finito de los axiomas $\neg A_1^2(b_i, b_j)$. Digamos que los axiomas que ocupó la prueba son:

$$b_{i_1} \neq b_{j_1}, b_{i_2} \neq b_{j_2}, \ldots, b_{i_m} \neq b_{j_m},$$

Como $\mathfrak{M}$ es infinito, entonces el dominio D es un conjunto infinito. Así, podemos escoger interpretaciones de $b_{i_1}, \ldots, b_{i_m}, b_{j_1}, \ldots, b_{j_m}$ en D y construir un nuevo modelo de K $\mathfrak{M}'$ donde las formulas $b_{i_1} \neq b_{j_1}, \ldots, b_{i_m} \neq b_{j_m}$ sean verdaderas. Pero $\varphi \wedge \neg\varphi$ es derivable de estas fórmulas y de los axiomas de K, entonces $\varphi \wedge \neg\varphi$ es verdadera para $\mathfrak{M}'$, pero no puede ocurrir que en un modelo φ sea verdadera y $\neg\varphi$ sea verdadera.
Por lo tanto K' es consistente. Como K' es consistente, entonces por el corolario anterior tenemos que K' tiene un modelo normal $\mathfrak{N}$ finito o numerable. Como en K' $b_i \neq b_j$ son axiomas, entonces son verdaderas en $\mathfrak{N}$ y como $\mathfrak{N}$ es normal entonces la interpretación de las formulas $A_1^2(t, s)$ es la relación de igualdad del dominio N de $\mathfrak{N}$.Así las interpretaciones de $b_1, b_2, \ldots$ deben ser elementos distintos en D, así el dominio N es numerable. Por lo que $\mathfrak{N}$ es un modelo normal para K'. Como K' es una extensión de K entonces $\mathfrak{N}$ es un modelo normal y numerable para K. ■

Capítulo 3

Aritmética de Peano

La aritmética de los números naturales ha sido utilizada desde el año 1500, la teoría de números ha sido ampliamente estudiada por muchos matemáticos debido a sus distintas aplicaciones. Pero, no fue hasta finales del siglo XIX que algunos matemáticos realizaron múltiples intentos de la formalización y axiomatización de la Teoría de números.
Entre los distintos intentos reconocemos a matemáticos como Gottlob Frege, Richard Dedekind y Giuseppe Peano que, dieron sus propias versiones de axiomatizacón de los números naturales impulsados por el estudio de la aritmética en el análisis real.

En 1884 Frege, en su trabajo ***Foundations of Arithmetic*** intentó dar una definición de número en términos de nociones puramente lógicas e intentó probar que todo el razonamiento aritmético que se conocía, en particular los conceptos de sucesor y el principio de inducción matemática podían ser reducidos a inferencias lógicas. Sin embargo, pese a que Frege tenía la idea de probar que los teoremas de la aritmética podían deducirse utilizando principios lógicos, hubo pruebas en las que surgieron dudas respecto a argumentos que parecían ocupar principios no lógicos.

El trabajo principal de Dedekind respecto a la aritmética fue publicado en 1888, titulado ***Was sind und was sollen die Zahlen?*** donde dio una idea diferente a la de Frege de la aritmética, en su trabajo, caracterizó a los números naturales utilizando nociones de la teoría de conjuntos. Sin embargo algunas nociones que utilizó no pudieron ser descritas de una manera formal sin evitar ambigüedades.

Finalmente llegamos al trabajo de Peano, que es considerado el trabajo más completo de axiomatización de los números naturales utilizando nociones de la lógica. Aunque Peano utilizó parte del trabajo de Dedekind para fundamentar sus axiomas y resultados, también contribuyó con una manera distinta de interpretar a la aritmética. Consideró cierto número de conceptos primitivos que no podían ser definidos pero que podían ser caracterizados de manera axiomática, que fueron los conceptos de número, unidad, sucesor e igualdad. Fue en 1889 cuando Peano introdujo en su trabajo ***Arithmetices principia*** los axiomas que, escritos de manera informal decían:

(P1) 0 es un número natural.

(P2) Si x es un número natural, existe otro número natural, denotado por x' y que llamamos el sucesor de x.

(P3) $0 \neq x$ para cada natural x.

(P4) Si $x' = y'$, entonces $x = y$.

(P5) Si Q es una propiedad que puede ser o no válida para cualquier número natural, y si además:

i) 0 tiene la propiedad Q.

ii) Siempre que un número natural x tenga la propiedad Q, entonces x' tambien tiene la propiedad Q.

entonces diremos que todos los números naturales cumplen la propiedad Q (Principio de inducción matemática)

Sin embargo, hay conceptos, como el de "propiedad" que resultan ambiguos a la hora de buscar que este sistema tenga una rigurosa formalización.
El objetivo de este capítulo es definir un lenguaje de primer orden para así construir una teoría S para ese lenguaje que esté basada en los postulados de Peano y que sea adecuada para los resultados elementales que conocemos de la teoría de números.

Definición 3.1. Se define el lenguaje de primer orden $\mathcal{L}_A$ (al que llamamos lenguaje aritmético) como el conjunto que consta de:

i) $VAR = \{x_n | n \in \mathbb{N}\}$, el conjunto de variables.

ii) Solo un símbolo constante a_1.

iii) Un solo símbolo predicativo A_1^2.

iv) $\mathcal{F} = \{f_1^1, f_1^2, f_2^2\}$, el conjunto de símbolos funcionales.

v) $A = \{(,)\}$, el conjunto de signos de agrupación.

vi) $S = \{\rightarrow, \neg\}$, el conjunto de conectivos primitivos.

vii) $N = \{\forall\}$, el conjunto del cuantificador universal.

Ahora, construiremos una teoría, que denotaremos por S para el lenguaje $\mathcal{L}_A$.

Observación 3.1. Los conjuntos $\mathcal{FORM}$ y $\mathcal{TERM}$ de S, serán los mismos que utilizamos en el calculo predicativo clásico

Observación 3.2. Para $t, r, s \in \mathcal{TERM}$:

1. Abreviaremos $A_1^2(t, s)$ por $t = s$.
2. Abreviaremos $f_1^1(t)$ por (t'), $f_1^2(t, s)$ por $(t + s)$ y $f_2^2(t, s)$ por $(t \cdot s)$.
3. Abreviaremos a la constante a_1 por 0.
4. Escribiremos $t', t + s$ y $t \cdot s$ omitiendo los paréntesis siempre que no haya confusión.

Definición 3.2. La teoría S del lenguaje aritmético cuenta con 9 axiomas:

(S1) $x_1 = x_2 \rightarrow (x_1 = x_3 \rightarrow x_2 = x_3)$

(S2) $x_1 = x_2 \rightarrow x_1' = x_2'$

(S3) $0 \neq x_1'$

(S4) $x_1' = x_2' \rightarrow x_1 = x_2$

(S5) $x_1 + 0 = x_1$

(S6) $x_1 + x_2' = (x_1 + x_2)'$

(S7) $x_1 \cdot 0 = 0$

(S8) $x_1 \cdot (x_2') = (x_1 \cdot x_2) + x_1$

(S9) $\varphi(0) \to ((\forall x)(\varphi(x) \to \varphi(x')) \to (\forall x)\varphi(x))$ para $\varphi(x) \in \mathcal{FORM}$

(S9) es lo que conocemos como el principio de inducción matemática.
En S tenemos dos reglas de inferencia: MP y Gen.

Observación 3.3. 1) (S1),...,(S8)$\in \mathcal{FORM}$ y (S9) es un esquema de axioma de la teoría S

2) $\varphi(0), (\forall x)(\varphi(x) \to \varphi(x')) \vdash_S (\forall x)\varphi(x)$, en efecto

1.	$\varphi(0) \to ((\forall x)(\varphi(x) \to \varphi(x')) \to (\forall x)\varphi(x))$	[(S9)]
2.	$\varphi(0)$	[Hipótesis]
3.	$(\forall x)(\varphi(x) \to \varphi(x')) \to (\forall x)\varphi(x)$	[MP(1,2)]
4.	$(\forall x)(\varphi(x) \to \varphi(x'))$	[Hipótesis]
5.	$(\forall x)\varphi(x)$	[MP(3,4)]

A este resultado lo llamamos regla de inducción.

Nuestro propósito ahora, es probar que S es una teoría con igualdad y establecer las reglas usuales de esta.

Lema 3.3. *Para $t, r, s \in \mathcal{TERM}$, las siguientes fórmulas bien formadas son teoremas de S*

(S1') $t = r \to (t = s \to r = s)$

(S2') $t = r \to t' = r'$

(S3') $0 \neq t'$

(S4') $t' = r' \to t = r$

(S5') $t + 0 = t$

(S6') $t + r' = (t + r)'$

(S7') $t \cdot 0 = 0$

(S8') $t \cdot (r') = (t \cdot r) + t$

Demostración. Sean $t, r, s \in \mathcal{TERM}$.
Probemos (S1'), es decir veamos que $\vdash_S t = r \to (t = s \to r = s)$.
Por (S1), tenemos que $\vdash_S x = y \to (x = z \to y = z)$ donde $x, y, z \in VAR$, aplicando GEN, tenemos que $\vdash_S (\forall z)(x = y \to (x = z \to y = z))$.
Sea $z_0 \in VAR$ que no ocurre en los términos t, r ó s, denotemos
$\varphi(z) := x = y \to (x = z \to y = z)$ y sea $\varphi(z_0) := x = y \to (x = z_0 \to y = z_0)$. Notemos que $\varphi(z)$ y $\varphi(z_0)$ son similares pues:

1. z_0 es libre para z en $\varphi(z)$ pues z no esta al alcance de $(\forall z_0)$ en $\varphi(z)$.

2. $\varphi(z)$ no tiene ocurrencias libres de z_0.

Como $\varphi(z)$ y $\varphi(z_0)$ son similares, entonces, por la Proposición 1.28 tenemos que

$$\vdash_S (\forall z)\varphi(z) \leftrightarrow (\forall z_0)\varphi(z_0)$$

Ya sabemos que $\vdash_S (\forall z)\varphi(z)$, entonces ocupando MP tenemos que $\vdash_S (\forall z_0)\varphi(z_0)$.

Sea $y_0 \in VAR$ que no ocurre en los términos t, r ó s, denotemos ahora $\varphi(y) := (\forall z_0)\varphi(z_0)$ y sea $\varphi(y_0) := (\forall z_0)(x = y_0 \to (x = z_0 \to y_0 = z_0))$. Notemos que $\varphi(y)$ y $\varphi(y_0)$ son similares pues:

1. y_0 es libre para y en $\varphi(y)$ pues y no está al alcance de $(\forall y_0)$ en $\varphi(y)$.

2. $\varphi(y)$ no tiene ocurrencias libres de y_0.

Entonces por la Proposición 1.28 tenemos que

$$\vdash_S (\forall y)\varphi(y) \leftrightarrow (\forall y_0)\varphi(y_0)$$

Sabemos que $\vdash_S (\forall z_0)\varphi(z_0)$ entonces usando GEN $\vdash_S (\forall y)(\forall z_0)\varphi(z_0)$, es decir $\vdash_S (\forall y)\varphi(y)$, y, usando MP, tenemos que $\vdash_S (\forall y_0)\varphi(y_0)$, es decir, $\vdash_S (\forall y_0)(\forall z_0)(x = y_0 \to (x = z_0 \to y_0 = z_0))$

Sea $x_0 \in VAR$ que no ocurre en los términos t, r ó s, denotemos ahora $\varphi(x) := (\forall y_0)\varphi(y_0)$ y sea $\varphi(x_0) := (\forall y_0)(\forall z_0)(x_0 = y_0 \to (x_0 = z_0 \to y_0 = z_0))$. Notemos que $\varphi(x)$ y $\varphi(x_0)$ son similares pues:

1. x_0 es libre para x en $\varphi(x)$ pues x no esta al alcance de $(\forall x_0)$ en $\varphi(x)$.

2. $\varphi(x)$ no tiene ocurrencias libres de x_0.

Entonces por la Proposición 1.28 tenemos que

$$\vdash_S (\forall x)\varphi(x) \leftrightarrow (\forall x_0)\varphi(x_0)$$

Sabemos que $\vdash_S (\forall y_0)\varphi(y_0)$ entonces usando Gen $\vdash_S (\forall x)(\forall y_0)\varphi(y_0)$, es decir $\vdash_S (\forall x)\varphi(x)$, y, usando MP, tenemos que $\vdash_S (\forall x_0)\varphi(x_0)$, es decir

$$\vdash_S (\forall x_0)(\forall y_0)(\forall z_0)(x_0 = y_0 \to (x_0 = z_0 \to y_0 = z_0))$$

donde x_0, y_0, z_0 son variables que no ocurren en los términos t, r ó s.

Ahora, sea $\psi(x_0) := (\forall y_0)(\forall z_0)(x_0 = y_0 \to (x_0 = z_0 \to y_0 = z_0))$, se tiene que t es libre para x_0 en $\psi(x_0)$ pues x_0 está al alcance de $(\forall y_0)$ y $(\forall z_0)$ pero y_0 y z_0 no ocurren en t, así que, por la regla de particularización (A4) tenemos que $(\forall x_0)\psi(x_0) \vdash_S \psi(t)$ y sabemos que $\vdash_S (\forall x_0)\psi(x_0)$, por lo que $\vdash_S \psi(t)$, es decir $\vdash_S (\forall y_0)(\forall z_0)(t = y_0 \to (t = z_0 \to y_0 = z_0))$.
Si $\psi(y_0) := (\forall z_0)(t = y_0 \to (t = z_0 \to y_0 = z_0))$, se tiene que r es libre para y_0 en $\psi(y_0)$ pues y_0 está al alcance de $(\forall z_0)$ pero z_0 no ocurren en r, así que, por la regla de particularización (A4) tenemos que $(\forall y_0)\psi(y_0) \vdash_S \psi(r)$ y sabemos que $\vdash_S (\forall y_0)\psi(y_0)$, por lo que $\vdash_S \psi(r)$, es decir $\vdash_S (\forall z_0)(t = r \to (t = z_0 \to r = z_0))$.
Si $\psi(z_0) := (t = r \to (t = z_0 \to r = z_0))$, se tiene que s es libre para z_0 en $\psi(z_0)$ pues z_0 no está al alcance de algún cuantificador, así que, por la regla de particularización (A4) tenemos que $(\forall z_0)\psi(z_0) \vdash_S \psi(s)$ y sabemos que $\vdash_S (\forall z_0)\psi(z_0)$, por lo que $\vdash_S \psi(r)$, es decir

$$\vdash_S t = r \to (t = s \to r = s)$$

Las pruebas de (S2'),...,(S8') son análogas a la prueba de (S1'), utilizando los mismos argumentos. ■

Proposición 3.4. *Para cualesquiera $t, r, s \in \mathcal{TERM}$ las siguientes fórmulas son teoremas de S.*

(a) $t = t$

(b) $t = r \to r = t$

(c) $t = r \to (r = s \to t = s)$

(d) $r = t \to (s = t \to r = s)$

(e) $t = r \to t + s = r + s$

(f) $t = 0 + t$

(g) $t' + r = (t + r)'$

(h) $t + r = r + t$

(i) $t = r \to s + t = s + r$

(j) $(t + r) + s = t + (r + s)$

(k) $t = r \to t \cdot s = r \cdot s$

(l) $0 \cdot t = 0$

(m) $t' \cdot r = t \cdot r + r$

(n) $t \cdot r = r \cdot t$

(o) $t = r \to s \cdot t = s \cdot r$

Demostración. Sean $t, r, s \in \mathcal{TERM}$.
(a) Veamos que $\vdash_S t = t$.

1.	$t + 0 = t$	[(S5')]
2.	$t + 0 = t \to (t + 0 = t \to t = t)$	[(S1') para $t + 0, t \in \mathcal{TERM}$]
3.	$t + 0 = t \to t = t$	[MP(1,2)]
4.	$t = t$	[MP(1,3)]

Por lo tanto

$$\vdash_S t = t$$

(e) Veamos que $\vdash_S t = r \to t + s = t + r$.
Primero demostremos que $\vdash_S x = y \to x + z = y + z$ donde $x, y, z \in VAR$ no ocurren en los términos t, r ó s. Sea $\varphi(z) := x = y \to x + z = y + z$, haremos la prueba por inducción sobre z.

(i) Veamos que $\vdash_S \varphi(0)$, es decir, $\vdash_S x = y \to x + 0 = y + 0$; por el Teorema de la deducción bastará demostrar que $x = y \vdash_S x + 0 = y + 0$

1.	$x + 0 = x$	[(S5') para $x \in \mathcal{TERM}$]
2.	$y + 0 = y$	[(S5') para $y \in \mathcal{TERM}$]
3.	$x = y$	[Hipótesis]
4.	$x + 0 = x \to (x = y \to x + 0 = y)$	[(c) para $x + 0, x, y \in \mathcal{TERM}$]
5.	$x + 0 = y$	[MP dos veces usando 1 y 3]
6.	$x + 0 = y \to (y + 0 = y \to x + 0 = y + 0)$	[(d) para $x + 0, y, y + 0 \in \mathcal{TERM}$]
7.	$x + 0 = y + 0$	[MP dos veces usando 2 y 5]

Así que $\varphi(0)$.

(ii) Veamos que $\vdash_S \varphi(z) \to \varphi(z')$; por el Teorema de la deducción bastará demostrar que $\varphi(z) \vdash_S \varphi(z')$, es decir $(x = y \to x + z = y + z) \vdash_S x = y \to x + z' = y + z'$. Por el Teorema de la deducción, demostraremos que $(x = y \to x + z = y + z), x = y \vdash_S x + z' = y + z'$

1.	$x = y \to x + z = y + z$	[Hipótesis]
2.	$x = y$	[Hipótesis]
3.	$x + z = y + z$	[MP(1,2)]
4.	$x + z' = (x + z)'$	[(S6)]
5.	$y + z' = (y + z)'$	[(S6)]
6.	$x + z = y + z \to (x + z)' = (y + z)'$	[(S2') para $x + z, y + z \in \mathcal{TERM}$]
7.	$(x + z)' = (y + z)'$	[MP(3,6)]
8.	$x + z' = (x + z)' \to ((x + z)' = (y + z)' \to x + z' = (y + z)')$ [(c) para $x + z', (x + z)', (y + z)' \in \mathcal{TERM}$]	
9.	$x + z' = (y + z)'$	[MP dos veces usando 4 y 7]
10.	$x + z' = (y + z)' \to (y + z' = (y + z)' \to x + z' = y + z')$ [(d) para $x + z', (y + z)', y + z' \in \mathcal{TERM}$]	
11.	$x + z' = y + z'$	[MP dos veces usando 9 y 5]

Así que, hemos probado que $\vdash_S \varphi(z) \to \varphi(z')$, aplicando Gen tenemos que $\vdash_S (\forall z)(\varphi(z) \to \varphi(z'))$, entonces por la regla de inducción matemática tenemos que $\vdash_S (\forall z)\varphi(z)$ es decir

$$\vdash_S (\forall z)x = y \to x + z = y + z$$

Aplicando Gen tenemos que

$$\vdash_S (\forall x)(\forall y)(\forall z)x = y \to x + z = y + z$$

Aplicando la regla de particularización (A4) para las variables x, y, z y los términos t, r, s respectivamente, concluimos que

$$\vdash_S t = r \to t + s = r + s$$

*(k)*Veamos que $\vdash_S t = r \to t \cdot s = r \cdot s$.
Probemos que $\vdash_S x = y \to x \cdot z = y \cdot z$ donde $x, y, z \in VAR$ no ocurren en t, r o s. Sea $\varphi(z) := x = y \to x \cdot z = y \cdot z$, haremos la prueba por inducción sobre z.

(i) Veamos que $\vdash_s \varphi(0)$, es decir $\vdash_S x = y \to (x \cdot 0 = y \cdot 0)$

1.	$x \cdot 0 = 0$	[(S7)]
2.	$y \cdot 0 = 0$	[(S7)]
3.	$x \cdot 0 = 0 \to (y \cdot 0 = 0 \to x \cdot 0 = y \cdot 0)$	[Parte *(d)*]
4.	$x \cdot 0 = y \cdot 0$	[MP usando 1 y 2]
5.	$x \cdot 0 = y \cdot 0 \to (x = y \to (x \cdot 0 = y \cdot 0))$	[(A1)]
6.	$x = y \to (x \cdot 0 = y \cdot 0)$	[MP(4,5)]

Así que, $\vdash_S \varphi(0)$

(ii) Veamos que $\vdash_S \varphi(z) \to \varphi(z')$, por el teorema de la deducción, basta demostrar que $\varphi(z) \vdash_S \varphi(z')$, es decir $(x = y \to x \cdot z = y \cdot z), (x = y) \vdash_S x \cdot z' = y \cdot z'$

1.	$x = y$	[Hipótesis]
2.	$x \cdot z = y \cdot z$	[Hipótesis]
3.	$x \cdot z' = x \cdot z + x$	[(S8)]
4.	$y \cdot z' = y \cdot z + y$	[(S8)]
5.	$x \cdot z = y \cdot z \to x \cdot z + y = y \cdot z + y$	[Parte *(e)*]
6.	$x \cdot z + y = y \cdot z + y$	MP(2,5)
7.	$x = y \to x \cdot z + x = x \cdot z + y$	[Parte *(i)*]
8.	$x \cdot z + x = x \cdot z + y$	MP(1,7)
9.	$x \cdot z + x = x \cdot z + y \to (x \cdot z + y = y \cdot z + y \to x \cdot z + x = y \cdot z + y)$	[Parte *(c)*]
10.	$x \cdot z + x = y \cdot z + y$	[MP usando 8 y 6]
11.	$x \cdot z' = x \cdot z + x \to (x \cdot z + x = y \cdot z + y \to x \cdot z' = y \cdot z + y)$	[Parte *(c)*]
12.	$x \cdot z' = y \cdot z + y$	[MP usando 3 y 10]
13.	$x \cdot z' = y \cdot z + y \to (y \cdot z' = y \cdot z + y \to x \cdot z' = y \cdot z')$	[Parte *(d)*]
14.	$x \cdot z' = y \cdot z'$	[MP usando 12 y 4]

Así que, hemos probado que $\vdash_S \varphi(z) \to \varphi(z')$, aplicando Gen tenemos que $\vdash_S (\forall z)(\varphi(z) \to \varphi(z'))$, entonces por la regla de inducción matemática tenemos que $\vdash_S (\forall z)\varphi(z)$ es decir

$$\vdash_S (\forall z)x = y \to x \cdot z = y \cdot z$$

Aplicando Gen tenemos que

$$\vdash_S (\forall x)(\forall y)(\forall z)x = y \to x \cdot z = y \cdot z$$

Aplicando la regla de particularización (A4) para las variables x, y, z y los términos t, r, s respectivamente, concluimos que

$$\vdash_S t = r \to t \cdot s = r \cdot s$$

(l) Veamos que $\vdash_S 0 \cdot t = 0$.
Primero probemos que $\vdash_S 0 \cdot x = 0$ donde $x \in VAR$ no ocurre en el término t.
Sea $\varphi(x) := 0 \cdot x = 0$. Haremos la prueba por inducción sobre x.

(i) Veamos que $\vdash_S \varphi(0)$, es decir $\vdash_S 0 \cdot 0 = 0$.
Como $0 \in \mathcal{TERM}$, entonces por (S7') se cumple que $0 \cdot 0 = 0$, así que $\vdash_S \varphi(0)$.

(ii) Veamos que $\vdash_S \varphi(x) \to \varphi(x')$; por el Teorema de la deducción bastará demostrar que $\varphi(x) \vdash_S \varphi(x')$, es decir $0 \cdot x = 0 \vdash_S 0 \cdot x' = 0$

1.	$0 \cdot x' = 0 \cdot x + 0$	[S8']
2.	$0 \cdot x = 0$	[Hipótesis]
3.	$0 \cdot x + 0 = 0 \cdot x$	[S5']
4.	$0 \cdot x' = 0 \cdot x + 0 \to (0 \cdot x + 0 = 0 \cdot x \to 0 \cdot x' = 0 \cdot x)$	[Parte *(c)*]
5.	$0 \cdot x' = 0 \cdot x$	[Mp usando 1 y 3]
6.	$0 \cdot x' = 0 \cdot x \to (= 0 \cdot x = 0 \to 0 \cdot x' = 0)$	[Parte *(c)*]
7.	$0 \cdot x' = 0$	[MP usando 5 y 2]

Así que, hemos probado que $\vdash_S \varphi(x) \to \varphi(x')$, y si aplicamos Gen tenemos que $(\forall x)(\varphi(x) \to \varphi(x'))$, así por la regla de inducción, tenemos que $\vdash_S (\forall x)\varphi(x)$, es decir

$$\vdash_S (\forall x) 0 \cdot x = 0$$

Por la regla de particularización (A4) concluimos que

$$\vdash_S 0 \cdot t = 0$$

(n) Veamos que $\vdash_S t \cdot r = r \cdot t$.
Probaremos que $\vdash_S x \cdot y = y \cdot x$ donde $x, y \in VAR$ no ocurren en los términos t o r. Sea $\varphi(x) := x \cdot y = y \cdot x$. Hagamos la prueba por inducción sobre x.

(i) Veamos que $\vdash_S \varphi(0)$, es decir probemos que $\vdash_S 0 \cdot y = y \cdot 0$.

1.	$y \cdot 0 = 0$	[(S7)]
2.	$0 \cdot y = 0$	[Parte *(l)*]
3.	$0 \cdot y = 0 \to (y \cdot 0 = 0 \to 0 \cdot y = y \cdot 0)$	[Parte *(d)*]
4.	$0 \cdot y = y \cdot 0$	[MP usando 2 y 1]

Por lo tanto $\vdash_S \varphi(0)$.

(ii) Probemos que $\varphi(x) \vdash_S \varphi(x')$, es decir, $(x \cdot y = y \cdot x) \vdash_S x' \cdot y = y \cdot x'$

1.	$x \cdot y = y \cdot x$	[Hipótesis]
2.	$x' \cdot y = x \cdot y + y$	[Parte *(m)*]
3.	$y \cdot x' = y \cdot x + y$	[(S8)]
4.	$x \cdot y + y = y \cdot x + y$	[Parte *(e)* y MP usando 1]
5.	$x' \cdot y = x \cdot y + y \to (x \cdot y + y = y \cdot x + y \to x' \cdot y = y \cdot x + y)$	[Parte *(c)*]
6.	$x' \cdot y = y \cdot x + y$	[MP usando 2 y 4]
7.	$x' \cdot y = y \cdot x + y \to (y \cdot x' = y \cdot x + y \to x' \cdot y = y \cdot x')$	[Parte *(d)*]
8.	$x' \cdot y = y \cdot x'$	[MP usando 6 y 3]

Así que, hemos probado que $\vdash_S \varphi(x) \to \varphi(x')$, y si aplicamos Gen tenemos que $(\forall x)(\varphi(x) \to \varphi(x'))$, así por la regla de inducción, tenemos que $\vdash_S (\forall x)\varphi(x)$, es decir

$$\vdash_S (\forall x) x \cdot y = y \cdot x$$

Aplicando una vez más Gen y por la regla de particularización (A4) concluimos que

$$\vdash_S t \cdot r = r \cdot t$$

El resto de incisos son análogos, los podemos deducir directamente como consecuencias del Lema 3.3 o utilizando el principio de inducción matemática. ∎

Corolario 2. *S es una teoría con igualdad.*

Demostración. Por la Proposición 2.5 para ver que S es una teoría con igualdad, solo nos basta demostrar los siguientes puntos:

1. $\vdash_S (\forall x_i)x_i = x_i$ con $x_i \in VAR$.
2. Si $\beta(x,x) \in \mathcal{FORM}$ es atómica sin constantes o letras funcionales y $\beta(x,y)$ surge de sustituir una ocurrencia de x por y en $\beta(x,x)$ entonces
$$\vdash_S x = y \to (\beta(x,x) \to \beta(x,y))$$
3. $\vdash_S x = y \to f_j^n(x, z_2, \ldots, z_n) = f_j^n(y, z_2, \ldots, z_n)$ donde f_j^n es una letra funcional de S y $f_j^n(y, z_2, \ldots, z_n)$ surge de sustituir en $f_j^n(x, z_2, \ldots, z_n)$ exactamente una ocurrencia de x por y.

1. Sea $x_i \in VAR$, como $x_i \in \mathcal{TERM}$ por (a) de la Proposición 3.4 se cumple que $\vdash_S x_i = x_i$, aplicando Gen tenemos que
$$\vdash_S (\forall x_i)x_i = x_i$$
2. Sea $\beta(x,x) \in \mathcal{FORM}$ atómica sin constantes o letras funcionales, entonces $\beta(x,x) := A_1^2(x,z)$ con $x, z \in VAR$. Sabemos que la abreviación de $A_1^2(x,z)$ es $x = z$. Ahora, $\beta(x,y)$ surge de sustituir una ocurrencia de x por y en $\beta(x,x)$, así que $\beta(x,y) := (y = z)$. Por (S1) se cumple que $\vdash_S x = y \to (x = z \to y = z)$, es decir
$$\vdash_S x = y \to (\beta(x,x) \to \beta(x,y))$$

3.

$\cdot$) Vamos a ver que $\vdash_S x = y \to f_1^1(x) = f_1^1(y)$.
Por (S2) $\vdash_S x = y \to x' = y'$, pero recordemos que $f_1^1(x)$ lo abreviamos como x' y $f_1^1(y)$ lo abreviamos como y', así que concluimos que
$$\vdash_S x = y \to f_1^1(x) = f_1^1(y)$$

$\cdot\cdot$) Vamos a ver que $\vdash_S x = y \to f_1^2(x,z) = f_1^2(y,z)$.
Por (e) de la Proposición 3.4 $\vdash_S x = y \to x + z = y + z$, pero recordemos que $f_1^2(x,z)$ lo abreviamos como $x + z$ y $f_1^2(y,z)$ lo abreviamos como $y + z$, así, concluimos que
$$\vdash_S x = y \to f_1^2(x,z) = f_1^2(y,z)$$

$\cdots$) Vamos a ver que $\vdash_S x = y \to f_2^2(x,z) = f_2^2(y,z)$.
Por (k) de la Proposición 3.4 $\vdash_S x = y \to x \cdot z = y \cdot z$, pero recordemos que $f_2^2(x,z)$ lo abreviamos como $x \cdot z$ y $f_2^2(y,z)$ lo abreviamos como $y \cdot z$, así, concluimos que
$$\vdash_S x = y \to f_2^2(x,z) = f_2^2(y,z)$$

Por lo tanto, de **1.**,**2.**, y **3.** concluimos que S es una teoría con igualdad. ∎

Nos podemos preguntar ahora acerca de la consistencia de S, tratemos de resolver esa interrogante.
Consideremos la siguiente interpretación de $\mathcal{L}_A$ que llamamos $\mathfrak{M}$:

I. El dominio de $\mathfrak{M}$ es $\mathbb{N} \cup \{0\}$.

II. Para la constante a_1 que denotamos por 0 consideremos $(a_1)^{\mathfrak{M}} = O \in \mathbb{N} \cup \{0\}$.

III. Consideremos:

1. $(f_1^1)^{\mathfrak{M}} : \mathbb{N} \cup \{0\} \longrightarrow \mathbb{N} \cup \{0\}$ tal que $(f_1^1)^{\mathfrak{M}}(n) = n + 1$.
2. $(f_1^2)^{\mathfrak{M}} : \mathbb{N} \cup \{0\} \times \mathbb{N} \cup \{0\} \longrightarrow \mathbb{N} \cup \{0\}$ tal que $(f_1^2)^{\mathfrak{M}}(n, m) = n + m$.
3. $(f_2^2)^{\mathfrak{M}} : \mathbb{N} \cup \{0\} \times \mathbb{N} \cup \{0\} \longrightarrow \mathbb{N} \cup \{0\}$ tal que $(f_2^2)^{\mathfrak{M}}(n, m) = nm$.

Son las interpretaciones de f_1^1, f_1^2, f_2^2.

IV. La interpretación $(A_1^2)^{\mathfrak{M}}$ de la letra predicativa A_1^2 es la relación de igualdad de $\mathbb{N} \cup \{0\}$.

Si aceptamos que los axiomas de S son lógicamente validos para la interpretación tendríamos que $\mathfrak{M}$ es un modelo para S, así que S es consistente pues admite un modelo.
Además $\mathfrak{M}$ es un modelo normal para S pues la interpretación de A_1^2 es la relación de igualdad en $\mathbb{N} \cup \{0\}$.
A $\mathfrak{M}$ lo llamamos el modelo estándar de S.
Sigamos analizando algunas teoremas que podemos deducir en S.

Proposición 3.5. *Sean $t, r, s \in \mathcal{TERM}$, las siguientes fórmulas son teoremas de S.*

(a) $t \cdot (r + s) = (t \cdot r) + (t \cdot s)$ ***(Distributividad).***

(b) $(r + s) \cdot t = (r \cdot t) + (s \cdot t)$.

(c) $(t \cdot r) \cdot s = t \cdot (r \cdot s)$ ***(Asociatividad del producto).***

(d) $t + s = r + s \to t = r$ ***(Cancelación de la suma).***

Demostración. *(a)* Veamos que $\vdash_S x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ para $x, y, z \in VAR$ que no ocurren en los términos t, r ó s. Hagamos la prueba por inducción sobre z.
Sea $\varphi(z) := x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.
i) Veamos que $\vdash_S \varphi(0)$, es decir, $\vdash_S x \cdot (y + 0) = (x \cdot y) + (x \cdot 0)$

1.	$y + 0 = y$	[(S5)]
2.	$y + 0 = y \to x \cdot (y + 0) = x \cdot y$	[(o) Prop. 3.4]
3.	$x \cdot (y + 0) = x \cdot y$	[MP(1,2)]
4.	$x \cdot 0 = 0$	[(S7)]
5.	$x \cdot 0 = 0 \to x \cdot y + x \cdot 0 = x \cdot y + 0$	[(i) Prop. 3.4]
6.	$x \cdot y + x \cdot 0 = x \cdot y + 0$	[MP(4,5)]
7.	$x \cdot y + 0 = x \cdot y$	[(S5')]
8.	$x \cdot y + x \cdot 0 = x \cdot y + 0 \to (x \cdot y + 0 = x \cdot y \to x \cdot y + x \cdot 0 = x \cdot y)$	[(o) Prop 3.4]
9.	$x \cdot y + x \cdot 0 = x \cdot y$	[MP usando 6 y 7]
10.	$x \cdot (y + 0) = x \cdot y \to (x \cdot y + x \cdot 0 = x \cdot y \to x \cdot (y + 0) = x \cdot y + x \cdot 0)$	[(d) Prop. 3.4]
11.	$x \cdot (y + 0) = x \cdot y + x \cdot 0$	[MP usando 3 y 9]

Por lo que $\vdash_S x \cdot (y + 0) = x \cdot y + x \cdot 0$, es decir

$$\vdash_S \varphi(0)$$

ii) Probemos que $\vdash_S \varphi(z) \to \varphi(z')$. Por el teorema de la deducción, basta probar que $\varphi(z) \vdash_S \varphi(z')$ es decir $(x \cdot (y+z) = (x \cdot y) + (x \cdot z)) \vdash_S x \cdot (y + z') = (x \cdot y) + (x \cdot z')$

1. $x \cdot (y+z) = (x \cdot y) + (x \cdot z)$ [Hipótesis]
2. $y + z' = (y+z)'$ [Hipótesis]
3. $x \cdot (y+z') = x \cdot (y+z)'$ [(o) Prop. 3.4]
4. $x \cdot (y+z)' = x \cdot (y+z) + x$ [(S8')]
5. $x \cdot (y+z') = x \cdot (y+z) + x$
   [(c) Prop. 3.4, $t := x \cdot (y+z'), r := x \cdot (y+z)', s := x \cdot (y+z) + x$
   y MP usando 3 y 4]
6. $x \cdot (y+z) + x = x \cdot y + x \cdot z + x$
   [(e) Prop. 3.4, $t := x \cdot (y+z), r := x \cdot y + x \cdot z, s := x$
   y MP usando 1]
7. $x \cdot (y+z') = x \cdot yx \cdot z + x$
   [(c) Prop. 3.4, $t := x \cdot (y+z'), r := x \cdot (y+z) + x, s := x \cdot y + x \cdot z + x$
   y MP usando 5 y 6]
8. $x \cdot z' = x \cdot z + x$ [(S8)]
9. $x \cdot y + x \cdot z' = x \cdot y + x \cdot z + x$
   [(i) Prop. 3.4, $t := x \cdot z', r := x \cdot z + x, s := x \cdot y$
   y MP usando 8]
10. $x \cdot (y+z') = x \cdot y + x \cdot z'$
   [(d) Prop. 3.4, $r := x \cdot (y+z'), t := x \cdot y + x \cdot z + x, s := x \cdot y + x \cdot z'$
   y MP usando 7 y 9]

Por lo que $\varphi(z) \vdash_S \varphi(z')$, y por el Teorema de la deducción tenemos que $\vdash_S \varphi(z) \to \varphi(z')$, aplicando Gen $\vdash_S (\forall z)(\varphi(z) \to \varphi(z'))$, y así, por el principio de inducción matemática concluimos que

$$\vdash_S (\forall z)\varphi(z)$$

Es decir

$$\vdash_S (\forall z)(x \cdot (y+z) = (x \cdot y) + (x \cdot z))$$

Si aplicamos Gen dos veces tenemos que $\vdash_S (\forall x)(\forall y)(\forall z)(x \cdot (y+z) = (x \cdot y) + (x \cdot z))$. Como tenemos que $x, y, z \in VAR$ no ocurren en los términos t, r ó s, podemos usar la regla de particularización (A4) para las variables x, y, z y los términos t, r, s respectivamente y concluir que

$$\vdash_S t \cdot (r+s) = (t \cdot r) + (t \cdot s)$$

(b) Veamos que $\vdash_S (r+s) \cdot t = r \cdot t + s \cdot t$

1. $t \cdot (r+s) = (r+s) \cdot t$ [(n) Prop. 3.4]
2. $t \cdot (r+s) = (t \cdot r) + (t \cdot s)$ [Parte *(a)* de esta Proposición]
3. $(r+s) \cdot t = (t \cdot r) + (t \cdot s)$ [(S1') y MP dos veces usando 1 y 2]
4. $t \cdot r = r \cdot t$ [(n) Prop. 3.4]
5. $t \cdot r + t \cdot s = r \cdot t + t \cdot s$ [(e) Prop 3.4 y MP usando 4]
6. $t \cdot s = s \cdot t$ [(n) Prop. 3.4]
7. $r \cdot t + t \cdot s = r \cdot t + s \cdot t$ [(e) Prop 3.4 y MP usando 6]
8. $t \cdot r + t \cdot s = r \cdot t + s \cdot t$ [(c) Prop. 3.4 y MP dos veces usando 5 y 7]
9. $(r+s) \cdot t = r \cdot t + s \cdot t$ [(c) Prop. 3.4 y MP dos veces usando 3 y 8]

Por lo tanto $\vdash_S (r+s) \cdot t = r \cdot t + s \cdot t$

Los incisos *(c)* y *(d)* se pueden realizar con inducción sobre la variable z como en *(a)*. ■

En nuestra teoría S a partir de la constante 0, podemos obtener el término $f_1^1(0)$, que abreviamos por $0'$, así sucesivamente podemos obtener los términos $0', 0'', 0''', \ldots$, estos nuevos términos los llamaremos numerales y los denotaremos por $\overline{1}, \overline{2}, \overline{3}, \ldots$ respectivamente, esta notación la utilizamos para no confundirnos con los números naturales de la metateoría.

Definición 3.6. Para $n \in \mathbb{N}$, definimos el numeral $\overline{n}$ como el término que consiste de la constante 0 seguido de n apostrofes. $\overline{n} := (0 \underbrace{'' \cdots '}_{\text{n-veces}})$.

De manera más general tenemos que $\overline{n+1} := (\overline{n})'$ y $\overline{0} := 0$.
De manera recursiva podemos establecer que:

i) 0 es un numeral.

ii) Si u es un numeral, entonces u' es numeral

Observación 3.4. Para $m, n \in \mathbb{N}$, si $m = n$ entonces $\vdash_S \overline{m} = \overline{n}$.

Efectivamente, por definición $\overline{m} := 0 \overbrace{'' \cdots '}^{\text{m-veces}}$, pero en la metateoría tenemos que $m = n$, así que $\overline{m} := 0 \overbrace{'' \cdots '}^{\text{n-veces}}$, y como $\overline{n} := 0 \overbrace{'' \cdots '}^{\text{n-veces}}$, entonces $\overline{m}$ y $\overline{n}$ representan el mismo término en la teoría. Además sabemos que para $t \in \mathcal{TERM}$ $\vdash_S t = t$, así que $\vdash_S \overline{m} = \overline{m}$, es decir $\vdash_S \overline{m} = \overline{n}$.

Proposición 3.7. *Para $t, r, s \in \mathcal{TERM}$ las siguientes fórmulas son teoremas de S:*

(a) $t + \overline{1} = t'$

(b) $t \cdot \overline{1} = t$

(c) $t \cdot \overline{2} = t + t$

(d) $t + s = 0 \to t = 0 \wedge s = 0$

(e) $t \neq 0 \to (s \cdot t = 0 \to s = 0)$

(f) $t + s = \overline{1} \to (t = 0 \wedge s = \overline{1}) \vee (t = \overline{1} \wedge s = 0)$

(g) $t \cdot s = \overline{1} \to (t = \overline{1} \wedge s = \overline{1})$

(h) $t \neq 0 \to (\exists y)(t = y')$

(i) $s \neq 0 \to (t \cdot s = r \cdot s \to t = r)$

(j) $t \neq 0 \to (t \neq \overline{1} \to (\exists y)(t = y''))$

Demostración. *(a)*

1. $t + 0' = (t + 0)'$ [(S6')]
2. $t + 0 = t$ [(S5')]
3. $t + 0 = t \to (t + 0)' = t'$ [(S2')]
4. $(t + 0)' = t'$ [MP(2,3)]
5. $t + 0' = (t + 0)' \to ((t + 0)' = t' \to t + 0' = t')$ [(c) Prop. 3.4]
6. $t + 0' = t'$ [MP usando 1 y 4]
7. $t + \overline{1} = t'$ [Definicion de $0'$]

Por lo tanto

$$\vdash_S t + \overline{1} = t'$$

(e) Veamos que $\vdash_S t \neq 0 \to (s \cdot t = 0 \to s = 0)$. Sean $x, y \in VAR$ que no ocurren en los términos t o s. Demostraremos que $\vdash_S x \neq 0 \to (y \cdot x = 0 \to y = 0)$.
Sea $\varphi(y) := x \neq 0 \to (y \cdot x = 0 \to y = 0)$.Haremos la prueba por inducción sobre y.

I)Veamos que $\vdash_S \varphi(0)$, es decir, $\vdash_S x \neq 0 \to (0 \cdot x = 0 \to 0 = 0)$

1. $0 = 0$ [(a) Prop. 3.4]
2. $0 = 0 \to (0 \cdot x = 0 \to 0 = 0)$ [(A1)]
3. $0 \cdot x = 0 \to 0 = 0$ [MP(1,2)]
4. $(0 \cdot x = 0 \to 0 = 0) \to (x \neq 0 \to (0 \cdot x = 0 \to 0 = 0))$ [(A1)]
5. $x \neq 0 \to (0 \cdot x = 0 \to 0 = 0)$ [MP(3,4)]

Por lo tanto $\vdash_S \varphi(0)$

II) Veamos que $\vdash_S \varphi(y) \to \varphi(y')$. Probemos que $(x \neq 0) \vdash_S y' \cdot x \neq 0$

1. $y' \cdot x = 0$ [Hipótesis]
2. $y' \cdot x = y \cdot x + x$ [$(m)Prop.3.4$]
3. $y' \cdot x = y \cdot x + x \to (y' \cdot x = 0 \to y \cdot x + x = 0)$ [(S2')]
4. $y \cdot x + x = 0$ [MP usando 2 y 1]
5. $y \cdot x + x = 0 \to (y \cdot x = 0 \ \wedge \ x = 0)$ [Parte *(d)*]
6. $y \cdot x = 0 \ \wedge x = 0$ [MP(4,5)]
7. $x = 0 \ \wedge \ x \neq 0$ [que es una contradicción]

Por lo que $\vdash_S y' \cdot x \neq 0$, así que:

1. $y' \cdot x \neq 0$
2. $y' \cdot x \neq 0 \to (y' \cdot x = 0 \to y' = 0)$ [$\neg\varphi \to (\varphi \to \psi)$]
3. $y' \cdot x = 0 \to y' = 0$ [MP(1,2)]
4. $(y' \cdot x = 0 \to y' = 0) \to (x \neq 0 \to (y' \cdot x = 0 \to y' = 0))$ [(A1)]
5. $x \neq 0 \to (y' \cdot x = 0 \to y' = 0)$ [MP(3,4)]

Es decir $\vdash_S \varphi(y')$ y por (A1) se tiene que $\vdash_S \varphi(y') \to (\varphi(y) \to \varphi(y'))$, entonces, ocupando MP concluimos que $\vdash_S \varphi(y) \to \varphi(y')$, y por Gen

$$\vdash_S (\forall y)(\varphi(y) \to \varphi(y'))$$

Así que, por la regla de inducción concluimos que $\vdash_S (\forall y)\varphi(y)$, es decir:

$$\vdash_S (\forall y) x \neq 0 \to (y \cdot x = 0 \to y = 0)$$

Finalmente ocupando Gen y la regla de particularización (A4) podemos concluir que

$$\vdash_S t \neq 0 \to (s \cdot t = 0 \to s = 0)$$

(h) Veamos que $\vdash_S t \neq 0 \to (\exists y)(t = y')$, sea $x \in VAR$ que no ocurre en el término t. Sea $\varphi(x) := x \neq 0 \to (\exists w)(x = w')$. Haremos inducción sobre x.

I) Veamos que $\vdash_S \varphi(0)$.

1. $0 = 0$ [(a) Prop. 3.4]
2. $0 = 0 \to (0 \neq 0 \to (\exists w)(0 = w'))$ [$\vdash_S \beta \to (\neg\beta \to \psi)$]
3. $0 \neq 0 \to (\exists w)(0 = w')$ [MP(1,2)]

Por lo tanto $\vdash_S \varphi(0)$.

II) Veamos que $\varphi(x) \vdash_S \varphi(x')$, es decir,
$(x \neq 0 \to (\exists w_0)(x = w_0')), (x' \neq 0) \vdash_S (\exists w_1)(x' = w_1')$

$\cdot$) Si $x = 0$

1. $x = 0$ [Hipótesis]
2. $x = 0 \to x' = 0'$ [(S2')]
3. $x' = 0'$ [MP(1,2)]

Si $w_1 \in VAR$, notemos que $0 \in \mathcal{TERM}$ es libre para w_1 en $\beta(w_1) := x' = w_1'$, entonces por la regla existencial (E4) se tiene que $x' = 0' \vdash_S (\exists w_1)\beta(w_1)$, es decir

$$\vdash_S (\exists w_1)x' = w_1'$$

Sabemos que, por (A1) $\vdash_S (\exists w_1)x' = w_1' \to (x' \neq 0 \to (\exists w_1)x' = w_1')$, y utilizando MP tenemos que $\vdash_S x' \neq 0 \to (\exists w_1)x' = w_1'$, así que, $\vdash_S \varphi(x) \to \varphi(x')$.

$\cdot\cdot$) Si $x \neq 0$

1. $x \neq 0 \to (\exists w_0)(x = w_0')$ [Hipótesis]
2. $x \neq 0$ [Hipótesis]
3. $(\exists w_0)(x = w_0')$ [MP(1,2)]
4. $x = b'$ [Regla C, con b una constante]
5. $x = b' \to x' = b''$ [(S2')]
6. $x' = b''$ [MP(4,5)]

Ahora, si $w_1 \in VAR$, notemos que $b' \in \mathcal{TERM}$ es libre para w_1 en $\beta(w_1) := x' = w_1'$, entonces por la regla existencial (E4) se tiene que $x' = b'' \vdash_S (\exists w_1)\beta(w_1)$, es decir

$$\vdash_S (\exists w_1)x' = w_1'$$

Sabemos que, por (A1) $\vdash_S (\exists w_1)x' = w_1' \to (x' \neq 0 \to (\exists w_1)x' = w_1')$, y utilizando MP tenemos que $\vdash_S x' \neq 0 \to (\exists w_1)x' = w_1'$, así que, $\vdash_S \varphi(x) \to \varphi(x')$.

De $\cdot$) y $\cdot\cdot$) tenemos que $\vdash_S \varphi(x) \to \varphi(x')$, y por Gen $(\forall x)\varphi(x) \to \varphi(x')$. Entonces por la regla de inducción tenemos que $\vdash_S (\forall x)\varphi(x)$, es decir

$$\vdash_S (\forall x)(x \neq 0 \to (\exists w)(x = w'))$$

Por último, ocupando la regla de particularización (A4) podemos concluir que

$$\vdash_S t \neq 0 \to (\exists y)(t = y')$$

El resto de incisos los podemos hacer por inducción y aplicando resultados que ya tenemos. ∎

Proposición 3.8. *En S se cumple que:*

a) Sean $m, n \in \mathbb{N}$:

i. Si $m \neq n$ entonces $\vdash_S \overline{m} \neq \overline{n}$

ii. $\vdash_S \overline{m+n} = \overline{m} + \overline{n}$ y $\vdash_S \overline{m \cdot n} = \overline{m} \cdot \overline{n}$

b) Cualquier modelo de S es infinito.

c) Para cualquier cardinal $\aleph_\beta$, S tiene un modelo normal de cardinalidad $\aleph_\beta$.

Demostración. a) Sean $m, n \in \mathbb{N}$
i. Supongamos que $m \neq n$, entonces $m < n$ o $n < m$. Sin pérdida de generalidad supongamos

que $m < n$.
Hagamos la prueba por contradicción, es decir, supongamos que $\vdash_S \overline{m} = \overline{n}$

1. $\overline{m} = \overline{n}$ [Hipótesis]
2. $0\overbrace{''\cdots'}^{\text{m-veces}} = 0\overbrace{''\cdots'}^{\text{n-veces}}$ [Definición de numeral]
3. $0\overbrace{''\cdots'}^{\text{m-veces}} = 0\overbrace{''\cdots'}^{\text{n-veces}} \to 0\overbrace{''\cdots'}^{\text{m-1-veces}} = 0\overbrace{''\cdots'}^{\text{n-1-veces}}$ [(S4')]
4. $0\overbrace{''\cdots'}^{\text{m-1-veces}} = 0\overbrace{''\cdots'}^{\text{n-1-veces}}$ [MP(2,3)]

Ahora aplicamos (S4') y MP $m-1$ veces más y obtenemos que

$$\vdash_S 0 = 0\overbrace{''\cdots'}^{\text{n-m-veces}}$$

Sea $t := \overline{n-m-1}$, como $m < n$ entonces $n - m > 0$ y así $n - m - 1 \geq 0$. Tenemos que $t := \overline{n-m-1} := \overbrace{0''\cdots'}^{\text{n-m-1-veces}}$, por lo que $t' := 0\overbrace{''\cdots'}^{\text{n-m-veces}}$.

Como $\vdash_S 0 = 0\overbrace{''\cdots'}^{\text{n-m-veces}}$, entonces $\vdash_S 0 = t'$, pero por (S3') tenemos que $\vdash_S 0 \neq t'$, por lo que $\vdash_S 0 = t' \ \wedge \ 0 \neq t'$, lo que es una contradicción. Por lo tanto

$$\vdash_S \overline{m} \neq \overline{n}$$

ii. Solo haremos la prueba de que $\vdash_S \overline{m \cdot n} = \overline{m} \cdot \overline{n}$ pues probar $\vdash_S \overline{m+n} = \overline{m} + \overline{n}$ se hace de manera análoga. Hagamos la prueba por inducción en el metalenguaje sobre $n \in \mathbb{N}$.

1. Veamos que $\vdash_S \overline{m \cdot 0} = \overline{m} \cdot \overline{0}$. Notemos que en el metalenguaje se tiene que $m \cdot 0 = 0$, así que por la Observación 3.4 $\vdash_S \overline{m \cdot 0} = \overline{0}$, pero $\overline{0} := 0$ por definición, entonces $\vdash_S \overline{m \cdot 0} = 0$, además $\overline{m} \cdot \overline{0} := \overline{m} \cdot 0$ y por (S7') se tiene que $\vdash_S \overline{m} \cdot 0 = 0$. Ahora, por (d) de la Proposición 3.4 se cumple que $\vdash_S \overline{m \cdot 0} = 0 \to (\overline{m} \cdot 0 = 0 \to \overline{m \cdot 0} = \overline{m} \cdot 0)$. Si aplicamos MP dos veces concluimos que $\vdash_S \overline{m \cdot 0} = \overline{m} \cdot 0$, es decir

$$\vdash_S \overline{m \cdot 0} = \overline{m} \cdot \overline{0}$$

2. Supongamos que $\vdash_S \overline{m \cdot n} = \overline{m} \cdot \overline{n}$. Ahora por (e) de la Proposición 3.4 tenemos que como $\overline{m \cdot n}, \overline{m} \cdot \overline{n}, \overline{m} \in \mathcal{TERM}$ entonces $\vdash_S \overline{m \cdot n} = \overline{m} \cdot \overline{n} \to \overline{m \cdot n} + \overline{m} = \overline{m} \cdot \overline{n} + \overline{m}$, y ocupando MP entre estos dos resultados tenemos que $\vdash_S \overline{m \cdot n} + \overline{m} = \overline{m} \cdot \overline{n} + \overline{m}$. Ahora bien, se tiene que $\vdash_S \overline{m \cdot n} + \overline{m} = \overline{m \cdot n + m}$, es decir $\vdash_S \overline{m \cdot n} + \overline{m} = \overline{m \cdot (n+1)}$, Si ocupamos (S2') y MP podemos deducir que $\vdash_S \overline{m \cdot (n+1)} = \overline{m} \cdot \overline{n} + \overline{m}$; como $\overline{m} \in \mathcal{TERM}$, entonces $\vdash_S \overline{m} \cdot \overline{1} = \overline{m}$, por (i) de la Proposición 3.4 tenemos que $\vdash_S \overline{m} \cdot \overline{1} = \overline{m} \to \overline{m} \cdot \overline{n} + \overline{m} \cdot \overline{1} = \overline{m} \cdot \overline{n} + \overline{m}$, así que por MP tenemos que $\vdash_S \overline{m} \cdot \overline{n} + \overline{m} \cdot \overline{1} = \overline{m} \cdot \overline{n} + \overline{m}$.
   Como $\vdash_S \overline{m \cdot (n+1)} = \overline{m} \cdot \overline{n} + \overline{m}$ y $\vdash_S \overline{m} \cdot \overline{n} + \overline{m} \cdot \overline{1} = \overline{m} \cdot \overline{n} + \overline{m}$, entonces ocupando (d) de la Proposición 3.4 y aplicando MP tenemos que $\vdash_S \overline{m \cdot (n+1)} = \overline{m} \cdot \overline{n} + \overline{m} \cdot \overline{1}$.
   Sabemos, por la distributividad en S, $\vdash_S \overline{m} \cdot (\overline{n} + \overline{1}) = \overline{m} \cdot \overline{n} + \overline{m} + \overline{1}$, y, nuevamente por (d) de la Proposición 3.4 y usando MP obtenemos que $\vdash_S \overline{m \cdot (n+1)} = \overline{m} \cdot (\overline{n} + \overline{1})$.
   Sabemos que $\vdash_S \overline{n+1} = \overline{n} + \overline{1}$, así que si utilizamos (o) de la Proposición 3.4 y aplicando MP obtenemos que $\vdash_S \overline{m} \cdot \overline{n+1} = \overline{m} \cdot (\overline{n} + \overline{1})$.
   Como $\vdash_S \overline{m \cdot (n+1)} = \overline{m} \cdot (\overline{n} + \overline{1})$ y $\vdash_S \overline{m} \cdot \overline{n+1} = \overline{m} \cdot (\overline{n} + \overline{1})$, así que nuevamente por (d) de la Proposición 3.4 y utilizando MP, podemos concluir que

$$\vdash_S \overline{m \cdot (n+1)} = \overline{m} \cdot \overline{n+1}$$

   Así, para $n \in \mathbb{N}$ se tiene que

$$\vdash_S \overline{m \cdot n} = \overline{m} \cdot \overline{n}$$

b) Veamos que cualquier modelo de S es infinito.
Sea $\mathfrak{M}$ un modelo de S. Como S es una teoría con igualdad, sabemos que podemos "contraer" a $\mathfrak{M}$ a un modelo normal $\mathfrak{M}^*$, es decir la interpretación de A_1^2 en $\mathfrak{M}^*$ es la relación usual de igualdad del dominio de $\mathfrak{M}^*$. Ahora, consideremos $m, n \in \mathbb{N}$ tales que $m \neq n$, sea
$\varphi := \overline{m} \neq \overline{n} := \neg(\overline{m} = \overline{n}) \in \mathcal{FORM}$, por el inciso *i.* de la parte *a)* se cumple $\vdash_S \varphi$, así que $\models_{\mathfrak{M}} \varphi$, es decir, para cualquier $V : VAR \longrightarrow D$ se tiene que $V'(\varphi) = 1$, es decir,
$(V^*(\overline{m}), V^*(\overline{n})) \notin (A_1^2)^{\mathfrak{M}^*}$. Y como $(A_1^2)^{\mathfrak{M}^*}$ es la relación de igualdad en el dominio, entonces concluimos que $V^*(\overline{m})$ y $V^*(\overline{n})$ son distintas, es decir, las interpretaciones de los numerales $\overline{m}$ y $\overline{n}$ son distintas en el dominio de $\mathfrak{M}^*$.
Por la definición de estos, el conjunto de numerales es numerable.
Así que para $m \neq n$ se tiene que las interpretaciones de $\overline{m}$ y $\overline{n}$ son distintas en el dominio. Por lo que el conjunto de las interpretaciones de todos los numerales, es numerable. Por lo tanto $\mathfrak{M}^*$ es infinito, así que $\mathfrak{M}$ también es infinito.

c) Hay un resultado en teoría de modelos que dice que si se tiene una teoría K con igualdad y K tiene un modelo normal infinito, entonces K siempre tiene un modelo normal de cardinalidad $\aleph_\beta$ para cualquier $\beta \geq 0$. Para ver la prueba de este resultado véase en [1] el Corolario 2.34, páginas 114-115. Utilizaremos este resultado para probar lo que deseamos.
S es una teoría con igualdad, y ya construimos el modelo estándar para S, que es un modelo normal y numerable, por lo que S tiene un modelo normal infinito, así que por lo anterior tenemos que para cualquier cardinal $\beta \geq 0$ S tiene un modelo normal de cardinalidad $\aleph_\beta$. ∎

Ahora introduciremos en S una "relación de orden".

Definición 3.9. Para $t, s \in \mathcal{TERM}$ se tiene que:

1. Abreviaremos a la fórmula bien formada
$(\exists w)(w \neq 0 \ \wedge \ w + t = s)$ por $t < s$ donde $w \in VAR$ es la primera variable que no ocurre en t ni en s. Cuando $t < s$ decimos que "t es menor que s".
2. $t \leq s$ es la abreviación de la fórmula $t < s \ \vee \ t = s$.
3. $t > s$ es la fórmula $s < t$.
4. $t \geq s$ es la fórmula $s \leq t$
5. $t \not< s$ es la abreviación de la fórmula $\neg(t < s)$.

Proposición 3.10. *Para $t, r, s \in \mathcal{TERM}$ las siguientes fórmulas son teoremas de S.*

(a) $t \not< t$

(b) $t < s \rightarrow (s < r \rightarrow t < r)$

(c) $t < s \rightarrow s \not< t$

(d) $t < s \leftrightarrow (t + r < s + r)$

(e) $t \leq t$

(f) $t \leq s \rightarrow (s \leq r \rightarrow t \leq r)$

(g) $t \leq s \leftrightarrow (t + r \leq s + r)$

(h) $t \leq s \rightarrow (s < r \rightarrow t < r)$

(i) $0 \leq t$

(j) $0 < t'$

(k) $t < r \leftrightarrow t' \leq r$

(l) $t \leq r \leftrightarrow t < r'$

(m) $t < t'$

(n) $0 < \overline{1}, \overline{1} < \overline{2}, \ldots$

(o) $t \neq r \rightarrow (t < r \ \vee \ r < t)$

(p) $t = r \ \vee \ t < r \ \vee \ r < t$

(q) $t \leq r \ \vee \ r \leq t$

(r) $t + r \geq t$

(s) $r \neq 0 \to t + r > t$

(t) $r \neq 0 \to t \cdot r \geq t$

(u) $r \neq 0 \leftrightarrow r > 0$

(v) $r > 0 \to (t > 0 \to r \cdot t > 0)$

(w) $r \neq 0 \to (t > 1 \to t \cdot r > r)$

(x) $r \neq 0 \to (t < s \leftrightarrow t \cdot r < s \cdot r)$

(y) $r \neq 0 \to (t \leq s \leftrightarrow t \cdot r \leq s \cdot r)$

(z) $t \not< 0$

(z') $t \leq r \ \wedge \ r \leq t \to t = r$

Demostración. Haremos la prueba de los incisos *(m)* y *(o)*, el resto de incisos se hacen de manera similar, utilizando inducción y los incisos anteriormente demostrados.

(m) Demostremos que $\vdash_S t < t'$ con $t \in \mathcal{TERM}$.

1. $t + \overline{1} = t'$ [Parte (a) Prop. 3.7]
2. $1 \neq 0$ [En el metalenguaje]
3. $\overline{1} \neq 0$ [$m \neq n \vdash_S \overline{m} \neq \overline{n}$]
4. $\overline{1} \neq 0 \ \wedge \ t + \overline{1} = t'$ [$\vdash_S \varphi$ y $\vdash_S \psi$ entonces $\vdash_S \varphi \wedge \psi$]

Ahora, se tiene que $\overline{1}$ es libre para x en $\varphi(x) := t + x = t'$, entonces por la regla existencial (E4) se cumple que

5. $(\exists x) x \neq 0 \ \wedge \ t + x = t'$
6. $t < t'$ [6 es la abreviación de 5]

(o) Demostremos que $\vdash_S t \neq r \to (t < r \ \vee \ r < t)$.
Sea $\varphi(x) := x \neq y \to (x < y \ \vee \ y < x)$ donde $x, y \in VAR$ no ocurren en t ni r. Veamos que $\vdash_S \varphi(x)$. Hagamos la prueba por inducción sobre x.

Demostraremos que $\vdash_S \varphi(0)$, es decir, veamos que $\vdash_S 0 \neq y \to (0 < y \ \vee \ y < 0)$. Por el Teorema de la deducción nos bastará demostrar que $0 \neq y \vdash_S 0 < y \ \vee \ y < 0$.

1. $0 \neq y$ [Hipótesis]
2. $0 \leq y$ [Inciso (i)]
3. $0 < y \ \vee \ y = 0$ [2 es la abreviación de 3]
4. $0 < y \ \vee \ y = 0 \to (\neg(y = 0) \to 0 < y)$ [$\vdash_S \varphi \vee \psi \to (\neg\psi \to \varphi)$]
5. $\neg(y = 0) \to 0 < y$ [MP(3,4)]
6. $0 < y$ [MP(1,5)]
7. $0 < y \to (0 < y \ \vee \ y < 0)$ [$\vdash_S \varphi \to \varphi \vee \psi$]
8. $0 < y \ \vee \ y < 0$ [MP(6,7)]

Por lo que $\vdash_S \varphi(0)$.

2. Supongamos que $\vdash_S x \neq y \to (x < y \ \vee \ y < x)$, veamos que
$\vdash_S x' \neq y \to (x' < y \ \vee \ y < x')$

·) Notemos que si $x = y$ entonces

1. $x < x'$ [inciso (m)]
2. $x = y \to (x < x' \to y < x')$ [(A7) para $\varphi(x, x) := x < x'$]
3. $x < x' \to y < x'$ [MP usando la hipótesis]
4. $y < x'$ [MP(1,3)]
5. $y < x' \to (x' < y \ \vee \ y < x')$ [$\vdash_S \varphi \to (\psi \vee \varphi)$]
6. $x' < y \ \vee \ y < x'$ [MP(4,5)]

$\cdot\cdot$) Si $x \neq y$, entonces por hipótesis inductiva tenemos que $x < y \ \vee \ y < x$.
i) Si $y < x$ se tiene que

1. $y < x$	[Hipótesis]
2. $x < x'$	[inciso (m)]
3. $y < x \rightarrow (x < x' \rightarrow y < x')$	[inciso (b)]
4. $y < x'$	[MP utilazando 1 y 2]
5. $y < x' \rightarrow x' < y \ \vee \ y < x'$	[$\vdash_S \varphi \rightarrow \psi \vee \varphi$]
6. $x' < y \ \vee \ y < x'$	[MP(4,5)]

Así que $x \neq y', y < x \vdash_S x' < y \ \vee \ y < x'$.

ii) Si $x < y$, entonces

1. $x < y$	[Hipótesis]
2. $x' \neq y$	[Hipótesis]
3. $x < y \rightarrow x' \leq y$	[inciso (k)]
4. $x' \leq y$	[MP (1,3)]
5. $x' < y \ \vee \ x' = y$	[4 es la abreviación de 5]
6. $x' < y \ \vee \ x' = y \rightarrow (x' \neq y \rightarrow x' < y)$	[$\vdash_S \varphi \vee \psi \rightarrow (\neg\psi \rightarrow \varphi)$]
7. $x' < y$	[MP usando 5 y 2]
8. $x' < y \ \vee \ y < x'$	[$\vdash_S \varphi \rightarrow \varphi \vee \psi$ y MP usando 7]

Así que $x \neq y', x < y \vdash_S x' < y \ \vee \ y < x'$

Sabemos que si $\varphi \vdash_S \beta$ y $\psi \vdash_S \beta$ entonces $\varphi \vee \psi \vdash_S \beta$. Como tenemos que $x \neq y', y < x \vdash_S x' < y \ \vee \ y < x'$ y también que $x \neq y', x < y \vdash_S x' < y \ \vee \ y < x'$, entonces concluimos que $x \neq y', x < y \vee y < x \vdash_S x' < y \vee y < x'$. Así, por $\cdot$) y $\cdot\cdot$) tenemos $\vdash_S x' \neq y \rightarrow x' < y \vee y < x'$. Por el Principio de inducción concluimos que $\vdash_S (\forall x) x \neq y \rightarrow x < y \vee y < x$, y por Gen tenemos que $\vdash_S (\forall x)(\forall y) x \neq y \rightarrow x < y \ \vee \ y < x$. Como tenemos que x, y no ocurren en los términos t, r, entonces usando la regla de particularización (A4) tenemos que

$$\vdash_S t \neq r \rightarrow t < r \ \vee \ r < t$$

■

Proposición 3.11. *En S se cumple lo siguiente:*

a) *Para cualquier $k \in \mathbb{N}$, $\vdash_S x = 0 \ \vee \cdots \vee \ x = \overline{k} \leftrightarrow x \leq \overline{k}$.*

a') *Para cualquier $k \in \mathbb{N}$ y $\varphi \in \mathcal{FORM}$, $\vdash_S \varphi(0) \ \wedge \ \varphi(\overline{1}) \ \wedge \cdots \wedge \ \varphi(\overline{k}) \leftrightarrow (\forall x)(x \leq \overline{k} \rightarrow \varphi(x))$*

b) *Para cualquier natural $k > 0$, $\vdash_S x = 0 \ \vee \cdots \vee \ x = \overline{k-1} \leftrightarrow x < \overline{k}$*

b') *Para cualquier natural $k > 0$ y $\varphi \in \mathcal{FORM}$,*
$\vdash_S \varphi(0) \ \wedge \ \varphi(\overline{1}) \ \wedge \cdots \wedge \ \varphi(\overline{k-1}) \leftrightarrow (\forall x)(x < \overline{k} \rightarrow \varphi(x))$

c) $\vdash_S ((\forall x)(x < y \rightarrow \varphi(x)) \ \wedge \ (\forall x)(x \geq y \rightarrow \psi(x))) \rightarrow (\forall x)(\varphi(x) \vee \psi(x))$

Demostración. a) Probemos que $\vdash_S x = 0 \ \vee \cdots \vee \ x = \overline{k} \leftrightarrow x \leq \overline{k}$ por inducción en el metalenguaje sobre $k \in \mathbb{N}$.

1. Analicemos el caso $k = 0$. Probaremos que que $\vdash_S x = 0 \leftrightarrow x \leq 0$

·) Supongamos que $x = 0$.

1. $x = 0$ [Hipótesis]
2. $x = 0 \to x = 0 \ \vee \ x < 0$ [$\vdash_S \varphi \to \varphi \vee \psi$]
3. $x = 0 \ \vee \ x < 0$ [MP(1,2)]
4. $x \leq 0$ [4 es la abreviación de 3]

Así que $\vdash_S x = 0 \to x \leq 0$

··) Supongamos que $x \leq 0$.

1. $x \geq 0$ [(i) Prop. 3.10]
2. $x \leq 0$ [Hipótesis]
3. $x \leq 0 \ \wedge \ x \geq 0$ [Si $\vdash_S \varphi$ y $\vdash_S \psi$ entonces $\vdash_S \varphi \wedge \psi$]
4. $x \leq 0 \ \wedge \ x \geq 0 \to x = 0$ [(z′) Prop. 3.10]
5. $x = 0$ [MP(3,4)]

Así que $\vdash_S x \leq 0 \to x = 0$

Por lo que de ·) y ··) concluimos que $\vdash_S x = 0 \leftrightarrow x \leq 0$.

2. Supongamos que $\vdash_S x = 0 \ \vee \cdots \vee \ x = \overline{k} \leftrightarrow x \leq \overline{k}$

i) Supongamos que $\vdash_S x = 0 \ \vee \cdots \vee \ x = \overline{k} \ \vee \ x = \overline{k+1}$.
Notemos que si, $x = \overline{k+1}$, entonces $\vdash_S x \leq \overline{k+1}$ pues se cumple que $\vdash_S x < \overline{k+1} \ \vee \ x = \overline{k+1}$.
Si se tiene que $x = 0 \ \vee \cdots \vee \ x = \overline{k}$, entonces por Hipótesis inductiva se cumplirá que $\vdash_S x = 0 \ \vee \cdots \vee \ x = \overline{k} \to x \leq \overline{k}$.
Por (n) de la Proposición 3.10 se cumple que $\vdash_S \overline{k} < \overline{k+1}$, entonces $\vdash_S \overline{k} \leq \overline{k+1}$, así que:

1. $x = 0 \ \vee \cdots \vee \ x = \overline{k}$ [Hipótesis]
2. $x = 0 \ \vee \cdots \vee \ x = \overline{k} \to x \leq \overline{k}$ [Hipótesis Inductiva]
3. $x \leq \overline{k}$ [MP(1,2)]
4. $\overline{k} \leq \overline{k+1}$
5. $x \leq \overline{k} \to (\overline{k} \leq \overline{k+1} \to x \leq \overline{k+1})$ [(f) Prop. 3.10]
6. $x \leq \overline{k+1}$ [MP usando 3 y 4]

Por lo que $\vdash_S x = 0 \ \vee \ldots \vee \ x = \overline{k} \ \vee \ x = \overline{k+1} \to x \leq \overline{k+1}$

ii) Supongamos que $\vdash_S x \leq \overline{k+1}$
Como $\vdash_S x \leq \overline{k+1}$, entonces $\vdash_S x < \overline{k+1} \ \vee \ x = \overline{k+1}$.
Notemos que si $x = \overline{k+1}$ entonces $\vdash_S x = 0 \vee \ldots \vee x = \overline{k} \vee x = \overline{k+1}$ pues sabemos que $\vdash_S \varphi \to \psi \vee \varphi$.
Ahora, si $x < \overline{k+1}$, recordemos que, por definición $\overline{k+1} := (\overline{k})'$, así que $\vdash_S x < (\overline{k})'$

1. $x < (\overline{k})'$ [Hipótesis]
2. $x < (\overline{k})' \to x \leq \overline{k}$ [(l) Prop. 3.10]
3. $x \leq \overline{k}$ [MP(1,2)]
4. $x \leq \overline{k} \to x = 0 \ \vee \ldots \vee \ x = \overline{k}$ [HI]
5. $x = 0 \ \vee \ldots \vee \ x = \overline{k}$ [MP(3,4)]
6. $x = 0 \ \vee \ldots \vee \ x = \overline{k} \to x = 0 \ \vee \ldots \vee \ x = \overline{k} \ \vee \ x = \overline{k+1}$ [$\vdash_S \varphi \to \varphi \vee \psi$]
7. $x = 0 \ \vee \ldots \vee \ x = \overline{k} \ \vee \ x = \overline{k+1}$ [MP(5,6)]

Por lo tanto $\vdash_S x = 0 \ \vee \ldots \vee \ x = \overline{k} \ \vee \ x = \overline{k+1}$. Así hemos probado que $\vdash_S x = 0 \ \vee \ldots \vee \ x = \overline{k} \ \vee \ x = \overline{k+1} \leftrightarrow x \leq \overline{k+1}$.

Por lo tanto, para toda $k \in \mathbb{N}$

$$\vdash_S x = 0 \ \vee \ldots \vee \ x = \overline{k} \leftrightarrow x \leq \overline{k}$$

a') Probemos que $\vdash_S \varphi(0) \ \wedge \ \varphi(\overline{1}) \ \wedge \cdots \wedge \ \varphi(\overline{k}) \leftrightarrow (\forall x)(x \leq \overline{k} \rightarrow \varphi(x))$ por inducción en el metalenguaje sobre $k \in \mathbb{N}$.

1. Para $k = 0$ veamos que $\vdash_S \varphi(0) \leftrightarrow (\forall x)(x \leq \overline{0} \rightarrow \varphi(x))$

   ·) Supongamos que $\vdash_S \varphi(0)$ y que $\vdash_S x \leq 0$

1. $x \leq 0$	[Hipótesis]
2. $x \leq 0 \rightarrow x = 0$	[Inciso a]
3. $x = 0$	[MP(1,2)]
4. $x = 0 \rightarrow (\varphi(0) \rightarrow \varphi(x))$	[A7′]
5. $\varphi(0)$	[Hipótesis]
6. $\varphi(x)$	[MP usando 3, 4 y 5]

   Así, por el teorema de la deducción tenemos que $\vdash_S x \leq 0 \rightarrow \varphi(x)$, usando Gen concluimos que $\vdash_S (\forall x)(x \leq 0 \rightarrow \varphi(x))$.
   Por lo tanto, $\vdash_S \varphi(0) \rightarrow (\forall x)(x \leq 0 \rightarrow \varphi(x))$.

   ··) Supongamos que $\vdash_S (\forall x)(x \leq 0 \rightarrow \varphi(x))$.
   Como 0 es libre para x en la fórmula $(x \leq 0 \rightarrow \varphi(x))$, entonces por la regla de particularización (A4) se cumple que $\vdash_S 0 \leq 0 \rightarrow \varphi(0)$ además:

1. $0 = 0$	[$\vdash_S t = t$]
2. $0 = 0 \rightarrow (0 = 0 \vee 0 < 0)$	[$\vdash_S \gamma \rightarrow (\gamma \vee \beta)$]
3. $0 = 0 \vee 0 < 0$	[MP usando 1 y 2]
4. $0 \leq 0$	[Abreviación de 3]
5. $0 \leq 0 \rightarrow \varphi(0)$	
6. $\varphi(0)$	[MP usando 4 y 5]

   Por lo tanto $\vdash_S (\forall x)(x \leq 0 \rightarrow \varphi(x)) \rightarrow \varphi(0)$

   Así que

   $$\vdash_S \varphi(0) \leftrightarrow (\forall x)(x \leq 0 \rightarrow \varphi(x))$$

2. Supongamos que $\vdash_S \varphi(0) \wedge \ldots \wedge \varphi(\overline{k}) \leftrightarrow (\forall x)(x \leq \overline{k} \rightarrow< \varphi(x))$

   I) Supongamos que $\vdash_S \varphi(0) \wedge \ldots \wedge \varphi(\overline{k}) \wedge \varphi(\overline{k+1})$ y que $\vdash_S x \leq \overline{k+1}$.

1. $x \leq \overline{k+1}$	[Hipótesis]
2. $x \leq \overline{k+1} \rightarrow x = 0 \vee \ldots \vee x = \overline{k} \vee x = \overline{k+1}$	[inciso a)]
3. $x = 0 \vee \ldots \vee x = \overline{k} \vee x = \overline{k+1}$	[MP usando 1 y 2]

i) Si $x = 0 \vee \ldots \vee x = \overline{k}$

4. $x = 0 \vee \ldots \vee x = \overline{k} \to x \leq \overline{k}$ [inciso a)]
5. $x \leq \overline{k}$ [MP usando 4 y i)]
6. $\varphi(0) \wedge \ldots \wedge \varphi(\overline{k})$ [Hipótesis]
7. $\varphi(0) \wedge \ldots \wedge \varphi(\overline{k}) \to (\forall x)(x \leq \overline{k} \to \varphi(x))$ [Hipótesis Inductiva]
8. $(\forall x)(x \leq \overline{k} \to \varphi(x))$ [MP usando 6 y 7]
9. $x \leq \overline{k} \to \varphi(x)$ [Regla A4]
10. $\varphi(x)$ [MP 5 y 8]

ii) Si $x = \overline{k+1}$ entonces

4. $x = \overline{k+1} \to (\varphi(\overline{k+1}) \to \varphi(x))$ [A7′]
5. $x = \overline{k+1}$ [Hipótesis]
6. $\varphi(\overline{k+1}) \to \varphi(x)$ [MP usando 5 y 4]
7. $\varphi(\overline{k+1})$ [Hipótesis]
8. $\varphi(x)$ [MP usando 7 y 6]

De i) y ii) concluimos que $\vdash_S \varphi(x)$, así que pr el teorema de la deducción tenemos que $\vdash_S x \leq \overline{k+1} \to \varphi(x)$, aplicando Gen, concluimos que $\vdash_S (\forall x)(x \leq \overline{k+1} \to \varphi(x))$

II) Supongamos que $\vdash_S (\forall x)(x \leq \overline{k+1} \to \varphi(x))$.
Notemos que para $i \in \{0, 1, \ldots, k+1\}$ se tiene que $\bar{i}$ es un término libre para x en la fórmula $x \leq \overline{k+1} \to \varphi(x)$, entonces por la regla de particularización A4 se cunple que $\vdash_S \bar{i} \leq \overline{k+1} \to \varphi(\bar{i})$. Ademas también se cumple que $\vdash_S \bar{i} \leq \overline{k+1}$, así que, aplicando MP concluimos que $\vdash_S \varphi(\bar{i})$ para $i \in \{0, 1, \ldots, k+1\}$, así que

$$\vdash_S \varphi(0) \wedge \ldots \wedge \varphi(\overline{k}) \wedge \varphi(\overline{k+1})$$

De I) y II) concluimos que $\vdash_S \varphi(0) \wedge \ldots \wedge \varphi(\overline{k}) \wedge \varphi(\overline{k+1}) \leftrightarrow (\forall x)(x \leq \overline{k+1} \to \varphi(x))$

Así que, para $k \in \mathbb{N}$ y $\varphi \in \mathcal{FORM}$ se cumple que

$$\vdash_S \varphi(0) \wedge \ldots \wedge \varphi(\overline{k}) \leftrightarrow (\forall x)(x \leq \overline{k} \to \varphi(x))$$

b) Veamos primero que $\vdash_S x = 0 \ \vee \ldots \vee \ x = \overline{k-1} \to x < \overline{k}$.
Por *a)* tenemos que $\vdash_S x = 0 \ \vee \ldots \vee \ x = \overline{k-1} \to x \leq \overline{k-1}$.

1. $x = 0 \ \vee \ldots \vee \ x = \overline{k-1}$ [Hipótesis]
2. $x = 0 \ \vee \ldots \vee \ x = \overline{k-1} \to x \leq \overline{k-1}$
3. $x \leq \overline{k-1}$ [MP(1,2)]
4. $\overline{k-1} < \overline{k}$ [(n) Prop. 3.10]
5. $x \leq \overline{k-1} \to (\overline{k-1} < \overline{k} \to x < \overline{k})$ [(h) Prop. 3.10]
6. $x < \overline{k}$ [MP usando 3 y 4]

Por lo tanto

$$\vdash_S x = 0 \ \vee \ldots \vee \ x = \overline{k-1} \to x < \overline{k}$$

Ahora veamos que $\vdash_S x < \overline{k} \to x = 0 \ \vee \ldots \vee \ x = \overline{k-1}$

1. $x < \overline{k}$ [Hipótesis]
2. $x < \overline{k} \to (x = \overline{k} \ \vee \ x < \overline{k})$ $[\vdash_S \varphi \to \psi \vee \varphi]$
3. $x = \overline{k} \ \vee \ x < \overline{k}$ [MP(1,2)]
4. $x \leq \overline{k}$ [4 es la abreviación de 3]
5. $x \leq \overline{k} \to x = 0 \ \vee \ldots \vee \ x = \overline{k-1} \ \vee \ x = \overline{k}$ [*Partea*)]
6. $x = 0 \ \vee \ldots \vee \ x = \overline{k-1} \ \vee \ x = \overline{k}$ [MP(5,6)]

Si $\vdash_S x = \overline{k}$ entonces como $\vdash_S x < \overline{k}$ se tiene que $\vdash_S (\exists w) w \neq 0 \ \wedge \ x + w = \overline{k}$, por la Regla C tenemos que $\vdash_S b \neq 0 \ \wedge \ x + b = \overline{k}$. Así que $\vdash_S x = \overline{k} \ \wedge \ x + b = \overline{k}$, por lo que $\vdash_S x + b = x$, y como $\vdash_S x + b = x \to b = 0$, entonces por MP se tiene que $\vdash_S b = 0$. Así que $\vdash_S b \neq 0$ y $\vdash_S b = 0$ lo que es una contradicción. Por lo tanto se tiene que $\vdash_S x \neq \overline{k}$.
Recordando que $\vdash_S \varphi \vee \psi \to (\neg\psi \to \varphi)$ tenemos que
$\vdash_S x = 0 \ \vee \ldots \vee \ x = \overline{k-1} \ \vee \ x = \overline{k} \to (x \neq \overline{k} \to x = 0 \ \vee \ldots \vee \ x = \overline{k-1})$, y, aplicando MP dos veces tenemos que $\vdash_S x = 0 \ \vee \ldots \vee \ x = \overline{k-1}$. Por lo tanto

$$\vdash_S x < \overline{k} \to x = 0 \ \vee \ldots \vee \ x = \overline{k-1}$$

Así que concluimos que

$$\vdash_S x = 0 \ \vee \ldots \vee \ x = \overline{k-1} \leftrightarrow x < \overline{k}$$

b') Se prueba de manera análoga a *a')*

c) Queremos probar que
$\vdash_S ((\forall x)(x < y \to \varphi(x)) \ \wedge \ (\forall x)(x \geq y \to \psi(x))) \to (\forall x)(\varphi(x) \vee \psi(x))$. Veamos que $((\forall x)(x < y \to \varphi(x)) \ \wedge \ (\forall x)(x \geq y \to \psi(x))) \vdash_S (\forall x)(\varphi(x) \vee \psi(x))$.
Notemos que si ocurriera que $\vdash_S x = y$, entonces

1. $(\forall x)(x \geq y \to \psi(x))$ [Hipótesis]
2. $x \geq y \to \psi(x)$ [(A4) y MP pues x es libre para x]
3. $x = y$ [Hipótesis]
4. $y < x \ \vee \ x = y$ $[\vdash_S \varphi \to \psi \vee \varphi$ y MP $]$
5. $x \geq y$ [4 es a abreviación de 3]
6. $\psi(x)$ [MP(4,2)]
7. $\varphi(x) \vee \psi(x)$ $[[\vdash_S \alpha \to \beta \vee \alpha$ y MP $]$
8. $(\forall x)(\varphi(x) \vee \psi(x))$ [Gen(7)]

Por lo tanto, si $\vdash_S x = y$ se tiene que
$((\forall x)(x < y \to \varphi(x)) \ \wedge \ (\forall x)(x \geq y \to \psi(x))) \vdash_S (\forall x)(\varphi(x) \wedge \psi(x))$

Ahora supongamos que $\vdash_S x \neq y$

1. $(\forall x)(x < y \to \varphi(x))$ [Hipótesis]
2. $(\forall x)(x \geq y \to \psi(x))$ [Hipótesis]
3. $(\forall x)(x < y \to \varphi(x)) \to (\forall x)x < y \to (\forall x)\varphi(x)$ [$\vdash_S (\forall x)(\alpha \to \gamma) \to ((\forall x)\alpha \to (\forall x)\gamma)$]
4. $(\forall x)x < y \to (\forall x)\varphi(x)$ [MP(1,3)]
5. $x \neq y$ [Hipótesis]
6. $x \neq y \to x < y \ \vee \ y < x$ [(o) Prop 3.10]
7. $x < y \ \vee \ y < x$ [MP(5,6)]
8. $(\forall x)(x < y \ \vee \ y < x)$ [Gen(7)]
9. $(\forall x)(x < y \ \vee \ y < x) \to ((\forall x)x < y \ \vee \ (\forall x)y < x)$ [$\vdash_S (\forall x)(\alpha \vee \gamma) \to ((\forall x)\alpha \vee (\forall x)\gamma)$]
10. $(\forall x)x < y \ \vee \ (\forall x)y < x$ [MP(8,9)]

Si $\vdash_S (\forall x)x < y$, entonces

11. $(\forall x)x < y$ [Hipótesis]
12. $(\forall x)\varphi(x)$ [MP(4,11)]
13. $(\forall x)\varphi(x) \to (\forall x)\varphi(x) \ \vee \ (\forall x)\psi(x)$ [$\vdash_S \alpha \to \alpha \vee \beta$]
14. $(\forall x)\varphi(x) \ \vee \ (\forall x)\psi(x)$ [MP(12,13)]
15. $(\forall x)\varphi(x) \ \vee \ (\forall x)\psi(x) \to ((\forall x)\varphi(x) \ \vee \ \psi(x))$ [$\vdash_S ((\forall x)\alpha \vee (\forall x)\gamma) \to (\forall x)(\alpha \vee \gamma)$]
16. $(\forall x)\varphi(x) \ \vee \ \psi(x)$ [MP(14,15)]

El caso $\vdash_S (\forall x)y < x$ es análogo.
Por lo tanto, si $\vdash_S x \neq y$ se tiene que

$$((\forall x)(x < y \to \varphi(x)) \ \wedge \ (\forall x)(x \geq y \to \psi(x))) \vdash_S (\forall x)(\varphi(x) \vee \psi(x))$$

En la prueba las aplicaciones de Gen no se hicieron a fórmulas que dependen de la fórmula $((\forall x)(x < y \to \varphi(x)) \ \wedge \ (\forall x)(x \geq y \to \psi(x)))$, así que por el teorema de la deducción tenemos que

$$\vdash_S ((\forall x)(x < y \to \varphi(x)) \ \wedge \ (\forall x)(x \geq y \to \psi(x))) \to (\forall x)(\varphi(x) \vee \psi(x))$$

■

Proposición 3.12. *Los siguientes dos, son teoremas de S:*

a) Inducción fuerte:
$\vdash_S (\forall x)((\forall z)(z < x \to \varphi(z)) \to \varphi(x)) \to (\forall x)\varphi(x)$.
Es decir, si se tiene una propiedad P tal q para cualquier x, P se satisface para los elementos menores que x, entonces P se cumple para x, así, se concluye que P se cumple para todo x.

b) Principio del menor número:
$\vdash_S (\exists x)\varphi(x) \to (\exists y)\varphi(y) \ \wedge \ (\forall z)(z < y \to \neg\varphi(z))$.
Es decir, si P se cumple para algún x, entonces existe el menor elemento que cumple la propiedad P.

Demostración. Probemos *a)*.
Sea $\gamma(x) := (\forall z)(z \leq x \to \varphi(z))$. y supongamos que $\vdash_S (\forall x)((\forall z)(z < x \to \varphi(z)) \to \varphi(x))$

1. $(\forall x)((\forall z)(z < x \to \varphi(z)) \to \varphi(x))$ [Hipótesis]

Notemos que 0 es libre para x en la fórmula $(\forall z)(z < x \to \varphi(z)) \to \varphi(x)$, así que por la regla de particularización (A4) se tiene que
$(\forall x)((\forall z)(z < x \to \varphi(z)) \vdash_S (\forall z)(z < 0 \to \varphi(z)) \to \varphi(0)$. Así que

2. $(\forall z)(z < 0 \to \varphi(z)) \to \varphi(0)$	
3. $z \not< 0$	[(z) Prop. 3.10]
4. $z \not< 0 \to (z < 0 \to \varphi(z))$	$[\vdash_S \neg\alpha \to (\alpha \to \psi)]$
5. $z < 0 \to \varphi(z)$	[MP(3,4)]
6. $(\forall z)(z < 0 \to \varphi(z))$	[Gen (5)]
7. $\varphi(0)$	[MP(2,6)]
8. $\varphi(0) \to (\forall z)(z \leq 0 \to \varphi(z))$	[Parte a′) Prop. 3.11]
9. $(\forall z)(z \leq 0 \to \varphi(z))$	[MP(7,8)]
10. $\gamma(0)$	10 es la abreviación de 9

Así que $(\forall x)((\forall z)(z < x \to \varphi(z)) \to \varphi(x)) \vdash_S \gamma(0)$

Probemos ahora que $(\forall x)((\forall z)(z < x \to \varphi(z)) \to \varphi(x)), \gamma(x) \vdash_S \gamma(x')$

1. $(\forall x)((\forall z)(z < x \to \varphi(z)) \to \varphi(x))$	[Hipótesis]
2. $(\forall z)(z \leq x \to \varphi(z))$	[Hipótesis]

Notemos ahora que z es libre para z en la fórmula $z \leq x \to \varphi(z)$, así que por (A4) se cumple que $\vdash_S z \leq x \to \varphi(z)$. Entonces

3. $z \leq x \to \varphi(z)$	
4. $z < x' \to z \leq x$	[(l) Prop. 3.10]
5. $z < x' \to z \leq x \to ((z \leq x \to \varphi(z)) \to (z < x' \to \varphi(z)))$	$[\vdash_S \alpha \to \beta \to ((\beta \to \psi) \to (\alpha \to \psi))]$
6. $z < x' \to \varphi(z)$	[MP usando 4 y 3]
7. $(\forall z)(z < x' \to \varphi(z))$	[Gen(6)]

Notemos que x' es libre para x en la fórmula $(\forall z)(z < x \to \varphi(z)) \to \varphi(x)$, así que por (A4) se cumple que $\vdash_S (\forall z)(z < x' \to \varphi(z)) \to \varphi(x')$. Entonces

8. $(\forall z)(z < x' \to \varphi(z)) \to \varphi(x')$	
9. $\varphi(x')$	[MP(7,8)]
10. $z \leq x' \to z \leq x'$	$[\vdash_S \alpha \to \alpha]$
11. $\leq x' \to z < x' \ \vee \ z = x'$	[abreviación de $z \leq x'$]
12. $x' = z \to (\varphi(x') \to \varphi(z))$	[(A7)]
13. $z = x' \to x' = z$	[(b) Prop. 3.4]
14. $z = x' \to (\varphi(x') \to \varphi(z))$	$[\vdash_S \alpha \to \beta \to ((\beta \to \psi) \to (\alpha \to \psi))$ y MP usando 13 y 12]
15. $z = x' \to \varphi(z)$	$[\vdash_S (\alpha \to (\beta \to \psi)) \to (\beta \to (\alpha \to \psi))$ y MP usando 14 y 9]
16. $z = x' \to \varphi(z) \ \wedge \ z < x' \to \varphi(z)$	[si $\vdash_S \alpha$ y $\vdash_S \beta$, ent, $\vdash_S \alpha \wedge \beta$]
17. $z = x' \ \vee \ z < x' \to \varphi(z)$	$[\vdash_S ((\alpha \to \psi) \wedge (\beta \to \psi)) \to ((\alpha \vee \beta) \to \psi)$ y MP usando 16]
18.$z \leq x' \to \varphi(z)$	[abreviación de $z \leq x'$]
19. $\gamma(x')$	

Por lo tanto $(\forall x)((\forall z)(z < x \to \varphi(z)) \to \varphi(x)), \gamma(x) \vdash_S \gamma(x')$.

Así, por el principio de inducción matemática, tenemos que $(\forall x)((\forall z)(z < x \to \varphi(z)) \to \varphi(x)) \vdash_S (\forall x)\gamma(x)$, es decir,

$$(\forall x)((\forall z)(z < x \to \varphi(z)) \to \varphi(x)) \vdash_S (\forall x)(\forall z)(z \leq x \to \varphi(z)).$$

Como x es libre para x en la fórmula $(\forall z(z \leq x \to \varphi(z)))$, entonces por la regla de particularización (A4) se cumple que $(\forall x)((\forall z)(z < x \to \varphi(z)) \to \varphi(x)) \vdash_S (\forall z)(z \leq x \to \varphi(z))$. Como x es libre para z en la fórmula $z \leq x \to \varphi(z)$, entonces por la regla de particularización (A4) se cumple que $(\forall x)((\forall z)(z < x \to \varphi(z)) \to \varphi(x)) \vdash_S x \leq x \to \varphi(x)$. Pero sabemos que $\vdash_S x \leq x$, así que, aplicando MP tenemos que $(\forall x)((\forall z)(z < x \to \varphi(z)) \to \varphi(x)) \vdash_S \varphi(x)$. Si aplicamos Gen tenemos que $(\forall x)((\forall z)(z < x \to \varphi(z)) \to \varphi(x)) \vdash_S (\forall x)\varphi(x)$.
Por último, las aplicaciones de Gen en la prueba no dependen de la fórmula $(\forall x)((\forall z)(z < x \to \varphi(z)) \to \varphi(x))$, así que, por el teorema de la deducción concluimos que

$$\vdash_S (\forall x)((\forall z)(z < x \to \varphi(z)) \to \varphi(x)) \to (\forall x)\varphi(x)$$

■

Definición 3.13. A la fórmula bien formada $(\exists z)(s = t \cdot z)$ la abreviaremos $t|s$ donde $z \in VAR$ es la primera que no ocurre en los términos t y r.

Proposición 3.14. *Las siguientes fórmulas son teoremas en S para $t, r, s \in \mathcal{TERM}$*

(a) $t|t$

(b) $\overline{1}|t$

(c) $t|0$

(d) $t|s \ \wedge \ s|r \to t|r$

(e) $s \neq 0 \ \wedge \ t|s \to t \leq s$

(f) $t|s \ \wedge \ s|t \to s = t$

(g) $t|s \to t|(r \cdot s)$

(h) $t|s \ \wedge \ t|r \to t|(s + r)$

Demostración. *(a)* Notemos que por (b) de la Proposición 3.7 se cumple que $\vdash_S t = t \cdot \overline{1}$. Ahora bien, $\overline{1}$ es libre para z en la fórmula $\varphi(z) := t = t \cdot z$, entonces por la regla (E4) tenemos que $\varphi(\overline{1}) \vdash_S (\exists z)\varphi(z)$, es decir,

$$t = t \cdot \overline{1} \vdash_S (\exists z)t = t \cdot z$$

Por lo que $t|t$.

(b) Sabemos que $\vdash_S t \cdot \overline{1} = \overline{1} \cdot t$, también, por (b) de la Proposición 3.7 se cumple que $\vdash_S t = t \cdot \overline{1}$. Por (c) de la Proposición 3.4 se tiene que $\vdash_S t = t \cdot \overline{1} \to (t \cdot \overline{1} = \overline{1} \cdot t \to t = \overline{1} \cdot t)$. Si ocupamos MP dos veces tenemos que $\vdash_S t = \overline{1} \cdot t$.
Ahora, si denotamos $\varphi(x) := t = \overline{1} \cdot x$. Se cumple que t es libre para x en $\varphi(x)$, entonces, por la regla (E4) se tiene que $\varphi(t) \vdash_S (\exists x)\varphi(x)$, así por el teorema de la deducción, se tiene que $\varphi(t) \to (\exists x)\varphi(x)$, y si ocupamos MP concluimos que $\vdash_S (\exists x)\varphi(x)$, es decir, $\vdash_S (\exists x)t = \overline{1} \cdot x$.
Por lo que $\overline{1}|t$.

(f)

1. $(\exists z)(s = t \cdot z)$ [pues $t|s$]
2. $(\exists w)(t = s \cdot w)$ [pues $s|t$]
3. $s = t \cdot a$ [Regla C a 1]
4. $t = s \cdot b$ [Regla C a 2]
5. $t = s \cdot b \to t \cdot a = (s \cdot b) \cdot a$ [(k) Prop. 3.4]
6. $t \cdot a = (s \cdot b) \cdot a$ [MP(4,5)]
7. $s = t \cdot a \to (t \cdot a = (s \cdot b) \cdot a \to s = (s \cdot b) \cdot a)$ [(c) Prop. 3.4]
8. $s = (s \cdot b) \cdot a$ [MP usando 3 y 6]
9. $s = (s \cdot b) \cdot a \to \overline{1} = b \cdot a$ [(i) Prop. 3.7]
10. $\overline{1} = b \cdot a$ [MP(8,9)]
11. $\overline{1} = b \cdot a \to (b = \overline{1} \ \wedge \ a = \overline{1})$ [(g) Prop. 3.7]
12. $b = \overline{1}$ [MP usando 11 y eliminación de la conjunción]
13. $b = \overline{1} \to s \cdot b = s \cdot \overline{1}$ [(o) Prop. 3.4]
14. $s \cdot b = s \cdot \overline{1}$ [MP(12,13)]
15. $s \cdot \overline{1} = s$ [(b) Prop. 3.7]
16. $s \cdot b = s \cdot \overline{1} \to (s \cdot \overline{1} = s \to s \cdot b = s)$ [(c) Prop. 3.4]
17. $s \cdot b = s$ [MP usando 14 y 15]
18. $t = s \cdot b \to (s \cdot b = s \to t = s)$ [(c) Prop. 3.4]
19. $t = s$ [MP usando 4 y 17]
20. $t = s \to s = t$ [(b) Prop. 3.4]
21. $s = t$ [MP(19,20)]

Por lo que $\vdash_S t|s \ \wedge \ s|t \to s = t$

(g)

1. $t|s$ Hipótesis
2. $(\exists w)s = t \cdot$ [2 es la abreviación de 1]
3. $s = t \cdot a$ [Regla C a 2]
4. $s = t \cdot a \to r \cdot s = r \cdot (t \cdot a)$ [(o) Prop. 3.4]
5. $r \cdot s = r \cdot (t \cdot a)$ [MP(3,4)]

Entonces si $\varphi(z) := r \cdot s = t \cdot z$, se cumple que $t \cdot a$ es libre para z en $\varphi(z)$, entonces por la regla (E4) se tiene que

6. $r \cdot s = r \cdot (t \cdot a) \to (\exists z) r \cdot s = r \cdot z$ [Regla (E4)]
7. $(\exists z) r \cdot s = r \cdot z$ [MP(5,6)]
8. $t|(r \cdot s)$ [8 es la abreviación de 7]

Por lo tanto $t|s \vdash_S t|(r \cdot s)$, y por el teorema de la deducción se cumple que $\vdash_S t|s \to t|(r \cdot s)$.

(h)

1. $(\exists w)r = t \cdot w$ [Pues $t|r$]
2. $(\exists z)s = t \cdot z$ [Pues $t|s$]
3. $r = t \cdot a$ [Regla C a 1]
4. $s = t \cdot b$ [Regla C a 2]
5. $s = t \cdot b \to s + r = (t \cdot b) + r$ [(e) Prop. 3.4]
6. $s + r = (t \cdot b) + r$ [MP(4,5)]
7. $r = t \cdot a \to t \cdot b + r = t \cdot b + t \cdot a$ [(i) Prop. 3.4]
8. $t \cdot b + r = t \cdot b + t \cdot a$ [MP(3,7)]
9. $s + r = (t \cdot b) + r \to (t \cdot b + r = t \cdot b + t \cdot a \to s + r = t \cdot b + t \cdot a)$ [(c) Prop. 3.4]
10. $s + r = t \cdot b + t \cdot a$ [MP usando 6 y 8]
11. $t \cdot b + t \cdot a = t \cdot (b + a)$ [distributividad]
12. $s + r = t \cdot b + t \cdot a \to (t \cdot b + t \cdot a = t(b + a) \to s + r = t \cdot (b + a))$ [(c) Prop. 3.4]
13. $s + r = t \cdot (b + a)$ [MP usando 10 y 11]

Entonces si $\varphi(x) := s + r = t \cdot x$, se cumple que $b + a$ es libre para x en $\varphi(x)$, entonces por la regla (E4) se tiene que

14. $s + r = t \cdot (b + a) \to (\exists x)s + r = t \cdot x$ [Regla (E4)]
15. $(\exists x)s + r = t \cdot x$ [MP(13,14)]
16. $t|(r + s)$ [16 es la abreviación de 15]

$\blacksquare$

Proposición 3.15. *En S es válido el algoritmo de la división, es decir:*
$\vdash_S y \neq 0 \to (\exists u)(\exists v)[x = y \cdot u + v \wedge (v < y) \wedge (\forall u_1)(\forall v_1)((x = y \cdot u_1 + v_1 \wedge (v_1 < y)) \to u = u_1 \wedge v = v_1)]$

Demostración. Sea $\varphi(x) := (\exists u)(\exists v)(x = y \cdot u + v \ \wedge \ v < y)$. Supongamos que $y \neq 0$.

1. $y \neq 0$ [Hipótesis]
2. $y \cdot 0 = 0$ [(S7)]
3. $y \cdot 0 + 0 = y \cdot 0$ [(S5)]
4. $y \cdot 0 + 0 = 0$ [Parte (c) Prop. 3.4 y MP usando 3 y 2]
5. $y \neq 0 \to y > 0$ [Parte (u) Prop. 3.10]
6. $y > 0$ [MP(1,4)]
7. $0 = y \cdot 0 + 0$ [Parte (c) Prop. 3.4 y MP usando 3 y 2]
8. $0 = y \cdot 0 + 0 \ \wedge \ y > 0$ [Inclusión de la conjunción]
9. $(\exists v)(0 = y \cdot 0 + v \ \wedge v < y)$ [(E4)]
10. $(\exists u)(\exists v)(0 = y \cdot u + v \ \wedge v < y)$ [(E4)]

Suponiendo que $y \neq 0$, tenemos que $\vdash_S \varphi(0)$.

Ahora, supongamos que $\vdash_S \varphi(x)$, es decir, $\vdash_S (\exists u)(\exists v)(x = y \cdot u + v \ \wedge v < y)$

1. $(\exists u)(\exists v)(x = y \cdot u + v \ \wedge v < y)$ [Hipótesis]
2. $(\exists v)(x = y \cdot a + v \ \wedge v < y)$ [Regla C]
3. $x = y \cdot a + b \ \wedge b < y$ [Regla C]
4. $b < y$ [$\vdash_S \alpha \wedge \beta \to \beta$ y MP con 3]
5. $b' \leq y$ [Parte (k) Prop. 3.10 y MP con 4]
6. $b' < y \ \vee \ b' = y$ [5 es la abreviación de 6]

i) Si $b' < y$

7. $x = y \cdot a + b$ [$\vdash_S \alpha \wedge \beta \to \alpha$ y MP con 3]
8. $x' = (y \cdot a + b)'$ [(S2') y MP con 7]
9. $y \cdot a + b' = (y \cdot a + b)'$ [(S6')]
10. $x' = y \cdot a + b'$ [Parte (d) Prop. 3.4 y MP con 8 y 9]
11. $x' = y \cdot a + b' \ \wedge \ b' < y$
12. $(\exists v)(x' = y \cdot a + v \ \wedge \ v < y)$ [Regla E4]
13. $(\exists u)(\exists v)(x' = y \cdot u + v \ \wedge \ v < y)$ [Regla E4]
14. $b' < y \to (\exists u)(\exists v)(x' = y \cdot u + v \ \wedge \ v < y)$ [Teorema de la deducción]

ii) Si $b' = y$

$7'$. $x' = y \cdot a + b'$ [Se deduce 7' de manera analoga a i)]
$8'$. $b' = y \to (x' = y \cdot a + b' \to x' = y \cdot a + y)$ [(A7)]
$9'$. $x' = y \cdot a + y$ [MP con ii) y 7']
$10'$. $y = y \cdot \overline{1}$ [Parte (b) Prop. 3.7]
$11'$. $x' = y \cdot a + y \cdot \overline{1}$ [(A7) y MP con 10' y 9']
$12'$. $y \cdot (a + \overline{1}) = y \cdot a + y \cdot \overline{1}$ [Distributividad]
$13'$. $x' = y \cdot (a + \overline{1})$ [Parte (d) Prop. 3.4 y MP con 11' y 12']
$14'$. $0 < y$ [Pues $y \neq 0$]
$15'$. $x' = y \cdot (a + \overline{1}) + 0$ [(c) Prop 3.4 y MP usando (S5') y 13']
$16'$. $x' = y \cdot (a + \overline{1}) + 0 \ \wedge \ 0 < y$
$17'$. $(\exists v)(x' = y \cdot (a + \overline{1}) + v \ \wedge \ v < y)$ [Regla E4]
$18'$. $(\exists u)(\exists v)(x' = y \cdot u + v \ \wedge \ v < y)$ [Regla E4]
$19'$. $b' = y \to (\exists u)(\exists v)(x' = y \cdot u + v \ \wedge \ v < y)$ [Teorema de la deducción]

Así, tenemos que $\vdash_S b' < y \to (\exists u)(\exists v)(x' = y \cdot u + v \ \wedge \ v < y)$ y que $\vdash_S b' = y \to (\exists u)(\exists v)(x' = y \cdot u + v \ \wedge \ v < y)$, por lo que $\vdash_S b' < y \ \vee \ b' = y \to (\exists u)(\exists v)(x' = y \cdot u + v \ \wedge \ v < y)$, ocupando MP tenemos que $\vdash_S (\exists u)(\exists v)(x' = y \cdot u + v \ \wedge \ v < y)$ siempre que $y \neq 0$ es decir, $\vdash_S y \neq 0 \to (\exists u)(\exists v)(x' = y \cdot u + v \ \wedge \ v < y)$, y por el teorema de la deducción, se tiene que $\vdash_S \varphi(x) \to \varphi(x')$, y por el principio de inducción, podemos concluir que $\vdash_S (\forall x)\varphi(x)$.

Ahora suponiendo que $(x = y \cdot u + v \ \wedge \ v < y)$ demostremos que $(x = y \cdot u_1 + v_1 \ \wedge \ v_1 < y) \vdash_S u = u_1 \ \wedge \ v = v_1$.
Por la parte (p) de la Proposición 3.10 tenemos que $\vdash_S u = u_1 \ \vee \ u < u_1 \ \vee \ u_1 < u$.

1. Si $u = u_1$
   Por (S5') tenemos que $x = y \cdot u + v \to (x = y \cdot u_1 + v_1 \to y \cdot u + v = y \cdot u_1 + v_1)$, aplicando MP con las hipótesis se tiene que $\vdash_S y \cdot u + v = y \cdot u_1 + v_1$.
   Por (A7) $\vdash_S u = u_1 \to (y \cdot u + v = y \cdot u_1 + v_1 \to y \cdot u_1 + v = y \cdot u_1 + v_1)$, aplicando MP obtenemos que $\vdash_S y \cdot u_1 + v = y \cdot u_1 + v_1$.Por la cancelación de la suma tenemos que $\vdash_S y \cdot u_1 + v = y \cdot u_1 + v_1 \to v = v_1$, y por MP se cumple que $v = v_1$

2. Si $u < u_1$, entonces por definición se tiene que
   $\vdash_S (\exists w)(u + w = u_1 \ \wedge \ w \neq 0)$. Ocupando la regla C tenemos que $\vdash_S u + a = u_1 \ \wedge \ a \neq 0$. Por (A7) tenemos que $u + a = u_1 \to (y \cdot u + v = y \cdot u_1 + v_1 \to y \cdot u + v = y \cdot (u + a) + v_1)$, y, aplicando MP se tiene que $\vdash_S y \cdot u + v = y \cdot (u + a) + v_1$. Por la distributividad de la suma, tenemos que $\vdash_S y \cdot (u + a) + v_1 = y \cdot u + y \cdot a + v_1$, así por la parte (c) de la Proposición 3.4 y MP, tenemos que $\vdash_S y \cdot u + v = y \cdot u + y \cdot a + v_1$. Aplicando otra vez la cancelación de la suma y MP tenemos que $\vdash_S v = y \cdot a + v_1$.
   Como $\vdash_S a \neq 0$, entonces por la parte (t) de la Proposición 3.10 y MP tenemos que $\vdash_S y \cdot a \geq y$. También, por la parte (r) de la Proposición 3.10 se tiene que $\vdash_S y \cdot a + v_1 \geq y \cdot a$. Usando la parte (b) de la Proposición 3.10 tenemos que $\vdash_S y \cdot a + v_1 \geq y$. Usando (A7) tenemos que $\vdash_S v = y \cdot a + v_1 \to (y \cdot a + v_1 \geq y \to v \geq y)$, y por MP concluimos que $\vdash_S v \geq y$. Así que, $\vdash_S v \geq y \ \wedge \ v < y$ lo cual es una contradicción. Por lo tanto $\vdash_S u \not< u_1$

3. Si $u_1 < u$ de manera análoga a 2. podemos concluir que $\vdash_S u_1 \not< u$

De 1.,2. y 3. podemos concluir que $\vdash_S u = u_1$, por lo que $\vdash_S v = v_1$,
así que $\vdash_S u = u_1 \ \wedge \ v = v_1$.
Por el teorema de la deducción podemos concluir que $\vdash_S x = y \cdot u_1 + v_1 \ \wedge \ v_1 < y \to u = u_1 \ \wedge \ v = v_1$, y, aplicando Gen, concluimos que

$$\vdash_S (\forall u_1)(\forall v_1)(x = y \cdot u_1 + v_1 \ \wedge \ v_1 < y \to u = u_1 \ \wedge \ v = v_1)$$

■

Hasta ahora, a partir de nuestros 9 axiomas aceptados en S hemos podido definir conceptos y demostrar propiedades básicas de la teoría de números. Así como lo hicimos durante este capítulo es posible definir distintos conceptos que usualmente se manejan en la teoría de números (por ejemplo el concepto de x^n) asociando fórmulas bien formadas en S a dichos conceptos, así, nos damos cuenta que todo lo que se trabaja respecto a la teoría de números siempre tiene una base lógica bien fundamentada.
En la siguiente parte de este trabajo, trataremos de encontrar una relación entre las funciones y relaciones de la metateoría (los números naturales) con lo que hemos trabajado de la teoría S y, a través de esto poder probar los teoremas de incompletitud.

Capítulo 4

Funciones recursivas

4.1. Funciones y relaciones número teóricas

En este capítulo cuando hablemos de los números naturales, nos referimos al conjunto de números $\mathbb{N}$ de la metateoría.

Definición 4.1. Una función número-teórica es una función $f : \mathbb{N}^n \longrightarrow \mathbb{N}$.

Ejemplo 5. Las funciones $f_+ : \mathbb{N}^2 \longrightarrow \mathbb{N}$ tal que para $n, m \in \mathbb{N}$, $f_+(n,m) = n+m$ y $f_. : \mathbb{N}^2 \longrightarrow \mathbb{N}$ tal que para $n, m \in \mathbb{N}$, $f_.(n,m) = n \cdot m$ son funciones número teóricas.

Definición 4.2. Si $R \subseteq \mathbb{N}^n$ decimos que R es una relación número-teórica.

Ejemplo 6. La relación $<$ de los números naturales es una relación número-teórica, pues definimos $<$ como:

$$<:= \{(n,m) \in \mathbb{N}^n | \exists r \in \mathbb{N} : n + r = m \ \wedge \ r \neq 0\}$$

Observación 4.1. Si tenemos una relación $R \subseteq \mathbb{N}^n$ para $k_1, \ldots, k_n \in \mathbb{N}, R(k_1, \ldots, k_n)$ representa el hecho de que $(k_1, \ldots, k_n) \in R$.

Definición 4.3. Sea K una teoría en el lenguaje $\mathcal{L}_A$ de la aritmética. Decimos que una relación número teórica R de n argumentos es expresable en K si y solo si existe una fórmula bien formada $\varphi(x_1, \ldots, x_n)$ de K donde $x_1, \ldots, x_n$ son variables libres tal que, para cualesquiera $k_1, \ldots, k_n \in \mathbb{N}$ se cumplen las siguientes dos condiciones:

1. Si $R(k_1, \ldots, k_n)$ es verdadera, entonces $\vdash_K \varphi(\overline{k_1}, \ldots, \overline{k_n})$.
2. Si $R(k_1, \ldots, k_n)$ es falsa, entonces $\vdash_K \neg\varphi(\overline{k_1}, \ldots, \overline{k_n})$.

Ejemplos 1. Veamos unos ejemplos de relaciones expresables.

1. La relación de igualdad de los números naturales es expresable en S.
   Veamos $\varphi(x_1, x_2) := A_1^2(x_1, x_2) := (x_1 = x_2) \in \mathcal{FORM}$ es la fórmula que expresa a a relación de igualdad de $\mathbb{N}$. Sean $k_1, k_2 \in \mathbb{N}$.

   i. Supongamos que $k_1 = k_2$.
      Por la Observación 3.4 se tiene que como $k_1 = k_2$, entonces $\vdash_S \overline{k_1} = \overline{k_2}$, es decir, $\vdash_S \varphi(\overline{k_1}, \overline{k_2})$

   ii. Supongamos que $k_1 \neq k_2$.
      Como $k_1 \neq k_2$, entonces por la parte *i.* del inciso *a)* de la Proposición 3.8 se tiene que $\vdash_S \overline{k_1} \neq \overline{k_n}$, es decir, $\vdash_S \neg\varphi(\overline{k_1}, \overline{k_2})$

   Por lo tanto, la relación de igualdad de $\mathbb{N}$ es expresable en S.

2. La relación $<$ es expresable en S por la fórmula
$\varphi(x_1, x_2) := (x_1 < x_2) := (\exists w)(w \neq 0 \ \wedge \ w + x_1 = x_2) \in \mathcal{FORM}$

   i. Supongamos que $k_1 < k_2$.
   Como $k_1 < k_2$, entonces existe $n \in \mathbb{N}$ tal que $n \neq 0$ y $k_1 + n = k_2$.
   Como $k_1 + n = k_2$ entonces por la Observación 3.4 se tiene que $\vdash_S \overline{k_1 + n} = \overline{k_2}$. Ahora, por la parte *ii.* del inciso *a)* de la Proposición 3.8 se tiene que $\vdash_S \overline{k_1 + n} = \overline{k_1} + \overline{n}$, si usamos $(S1')$ y MP tenemos que $\vdash_S \overline{k_1} + \overline{n} = \overline{k_2}$.
   Como $n \neq 0$ entonces por la parte *i.* del inciso *a)* de la Proposición 3.8 se tiene que $\vdash_S \overline{n} \neq \overline{0}$, es decir $\vdash_S \overline{n} \neq 0$.
   Así, tenemos que $\vdash_S \overline{n} \neq 0 \ \wedge \ \overline{k_1} + \overline{n} = \overline{k_2}$, entonces por la regla (E4) concluimos que $\vdash_S (\exists w)(w \neq 0 \ \wedge \ \overline{k_1} + w = \overline{k_2})$, es decir $\vdash_S \overline{k_1} < \overline{k_2}$. Por lo tanto

$$\vdash_S \varphi(\overline{k_1}, \overline{k_2})$$

   ii. Supongamos que $k_1 \not< k_2$.
   Como $k_1 \not< k_2$, entonces $k_2 < k_1 \ \vee \ k_1 = k_2$.
   Si $k_2 < k_1$, análogo a i. tendríamos que $\vdash_S \overline{k_2} < \overline{k_1}$. Por la parte (c) de la Proposición 3.10 tenemos que $\vdash_S \overline{k_2} < \overline{k_1} \rightarrow \overline{k_1} \not< \overline{k_2}$, así por MP, $\vdash_S \overline{k_1} \not< \overline{k_2}$, es decir,

$$\vdash_S \neg\varphi(\overline{k_1}, \overline{k_2})$$

   Si $k_1 = k_2$, entonces por la Observación 3.8 tenemos que $\vdash_S \overline{k_1} = \overline{k_2}$. Supongamos que $\vdash_S \overline{k_1} < \overline{k_2}$. Por (A7) se cumple que $\vdash_S \overline{k_1} = \overline{k_2} \rightarrow (\overline{k_1} < \overline{k_2} \rightarrow \overline{k_2} < \overline{k_2})$, y si aplicamos MP dos veces tenemos que $\vdash_S \overline{k_2} < \overline{k_2}$. Por la parte (a) de la Proposición 3.10 se tiene que $\vdash_S \overline{k_2} \not< \overline{k_2}$, así que $\vdash_S \overline{k_2} < \overline{k_2} \wedge \overline{k_2} \not< \overline{k_2}$ lo cual es una contradicción, por lo que $\vdash_S \overline{k_1} \not< \overline{k_2}$, es decir,

$$\vdash_S \neg\varphi(\overline{k_1}, \overline{k_2})$$

Por lo tanto, la relación $<$ de $\mathbb{N}$ es expresable en S.

Observación 4.2. Si R es una relación número-teórica que es expresable en una teoría K, entonces R es expresable en cualquier extensión de K.

Demostración. Sea K' una extensión de la teoría K, entonces para $\beta \in \mathcal{FORM}$ se tiene que si $\vdash_K \beta$ entonces $\vdash_{K'} \beta$.
Como R es expresable en K entonces existe $\varphi(x_1, \ldots, x_n) \in \mathcal{FORM}$ tal que para $k_1, \ldots, k_n \in \mathbb{N}$ se cumple:

1. Si $R(k_1, \ldots, k_n)$ es verdadera, entonces $\vdash_K \varphi(\overline{k_1}, \ldots, \overline{k_n})$

2. Si $R(k_1, \ldots, k_n)$ es falsa, entonces $\vdash_K \neg\varphi(\overline{k_1}, \ldots, \overline{k_n})$

Demostremos que R es expresable en K'.
Veamos que $\varphi(x_1, \ldots, x_n) \in \mathcal{FORM}$ es la que necesitamos para probarlo.

I. Si $R(k_1, \ldots, k_n)$ es verdadera, entonces por 1. $\vdash_K \varphi(\overline{k_1}, \ldots, \overline{k_n})$, y como K' es extensión, entonces, $\vdash_{K'} \varphi(\overline{k_1}, \ldots, \overline{k_n})$.

II. Si $R(k_1, \ldots, k_n)$ es falsa, entonces por 2. $\vdash_K \neg\varphi(\overline{k_1}, \ldots, \overline{k_n})$, y como K' es extensión, entonces, $\vdash_{K'} \neg\varphi(\overline{k_1}, \ldots, \overline{k_n})$.

Por lo tanto, R es expresable en K'. ∎

Definición 4.4. Sea K una teoría con igualdad en el lenguaje $\mathcal{L}_A$ de la aritmética. Una función número-teórica de n argumentos es representable en K si y solo si existe $\varphi(x_1, \dots, x_n, y) \in \mathcal{FORM}$, donde $x_1, \dots, x_n, y$ son variables libres, donde para $k_1, \dots, k_n \in \mathbb{N}$ se cumple que:

1. Si $f(k_1, \dots, k_n) = m$, entonces $\vdash_K \varphi(\overline{k_1}, \dots, \overline{k_n}, \overline{m})$.
2. $\vdash_K (\exists_1 y)\varphi(\overline{k_1}, \dots, \overline{k_n}, y)$

Si en esta definición reemplazamos la condición 2. por

2'. $\vdash_K (\exists_1 y)\varphi(x_1, \dots, x_n, y)$

decimos que f es fuertemente representable en K.

Observación 4.3. Si f es fuertemente representable, entonces f es representable.

Demostración. Como f es fuertemente representable, entonces existe $\varphi(x_1, \dots, x_n, y) \in \mathcal{FORM}$ con $x_1, \dots, x_n$ variables libres en φ donde para $k_1, \dots, k_n \in \mathbb{N}$ se cumplen 1. y 2'. de la Definición 4.4.Veamos que f es representable, proponemos a $\varphi((x_1, \dots, x_n, y)$ como la fórmula que buscamos.
Por hipótesis, ya se cumple 1. de la Definición 4.4.
Demostremos que $\vdash_K (\exists_1 y)\varphi(\overline{k_1}, \dots, \overline{k_n}, y)$.
Por hipótesis, se cumple 2'., es decir, $\vdash_K (\exists_1 y)\varphi(x_1, \dots, x_n, y)$. Si aplicamos Gen n veces tenemos que $\vdash_K (\forall x_1)(\forall x_2)\dots(\forall x_n)(\exists_1 y)\varphi(x_1, \dots, x_n, y)$. Notemos que para $i \in \{1, \dots, n\}$, x_i es libre en $\varphi(x_1, \dots, x_n, y)$, es decir, x_i no esta al alcance de $(\forall z)$. Así que, se cumple que $\overline{k_i}$ es libre para x_i en $\varphi(x_1, \dots, x_n, y)$. Entonces por la regla de particularización (A4) se tiene que $(\forall x_1)(\forall x_2)\dots(\forall x_n)(\exists_1 y)\varphi(x_1, \dots, x_n, y) \vdash_K (\forall x_2)\dots(\forall x_n)(\exists_1 y)\varphi(\overline{k_1}, \dots, x_n, y)$.
Si volvemos aplicar la regla (A4) $n-1$ veces, tenemos que

$$\vdash_K (\exists_1 y)\varphi(\overline{k_1}, \dots, \overline{k_n}, y)$$

Por lo tanto, f es representable en K. ■

Proposición 4.5 (V.H. Dyson)**.** *Si una función número-teórica $f : \mathbb{N}^n \longrightarrow \mathbb{N}$ es representable en K, entonces f es fuertemente representable en K.*

Demostración. Supongamos que $f : \mathbb{N}^n \longrightarrow \mathbb{N}$ es representable en K por $\varphi(x_1, \dots, x_n, y) \in \mathcal{FORM}$, donde $x_1, \dots, x_n, y$ son variables libres.
Demostremos que f es fuertemente representable en K.
Proponemos la siguiente $\beta(x_1, \dots, x_n, y) \in \mathcal{FORM}$:

$$\beta(x_1, \dots, x_n, y) := ([(\exists_1 y)\varphi(x_1, \dots, x_n, y)] \wedge \varphi(x_1, \dots, x_n, y)) \vee (\neg[(\exists_1 y)\varphi(x_1, \dots, x_n, y)] \wedge y = 0)$$

Demostremos que f es fuertemente representable en k por $\beta(x_1, \dots, x_n, y)$.
Sean $k_1, \dots, k_n \in \mathbb{N}$.

1. Supongamos que $f(k_1, \dots, k_n) = m$. Demostremos que $\vdash_K \beta(\overline{k_1}, \dots, \overline{k_n}, \overline{m})$.
Como $f(k_1, \dots, k_n) = m$ y f es representable en K por $\varphi(x_1, \dots, x_n, y)$, entonces por 1. y 2 de la Definición 4.4 tenemos que $\vdash_K \varphi(\overline{k_1}, \dots, \overline{k_n}, \overline{m})$ y $\vdash_K (\exists_1 y)\varphi(\overline{k_1}, \dots, \overline{k_n}, y)$ respectivamente, así que

$$\vdash_K [(\exists_1 y)\varphi(\overline{k_1}, \dots, \overline{k_n}, y)] \;\wedge\; \varphi(\overline{k_1}, \dots, \overline{k_n}, \overline{m})$$

Sabemos que para $\alpha, \gamma \in \mathcal{FORM}$, $\vdash_K \alpha \to \alpha \vee \gamma$, así que, podemos concluir que

$$\vdash_K ([(\exists_1 y)\varphi(\overline{k_1}, \dots, \overline{k_n}, y)] \;\wedge\; \varphi(\overline{k_1}, \dots, \overline{k_n}, \overline{m})) \;\vee\; (\neg[(\exists_1 y)\varphi(x_1, \dots, x_n, y) \;\wedge\; \overline{m} = 0])$$

es decir:

$$\vdash_K \beta(\overline{k_1}, \dots, \overline{k_n}, \overline{m})$$

2'. Demostremos que $\vdash_K (\exists_1 y)\beta(x_1, \dots, x_n, y)$

i) Supongamos que $\vdash_K (\exists_1 y)\varphi(x_1, \ldots, x_n, y)$,entonces

1. $(\exists_1 y)\varphi(x_1, \ldots, x_n, y)$
   [Hipótesis]
2. $(\exists y)\varphi(x_1, \ldots, x_n, y) \ \wedge \ (\forall x)(\forall y)(\varphi(x_1, \ldots, x_n, x) \wedge \varphi(x_1, \ldots, x_n, y) \rightarrow x = y)$
   [1 es la abreviación de 2]
3. $(\exists y)\varphi(x_1, \ldots, x_n, y)$
   [$\vdash_K \alpha \wedge \gamma \rightarrow \alpha$]
4. $\varphi(x_1, \ldots, x_n, b)$
   [Regla C]
5. $[(\exists_1 y)\varphi(x_1, \ldots, x_n, y)] \ \wedge \ \varphi(x_1, \ldots, x_n, b)$
   [Si $\vdash_K \alpha$ y $\vdash_K \gamma$ entonces $\vdash_K \alpha \wedge \gamma$]
6. $([(\exists_1 y)\varphi(x_1, \ldots, x_n, y)] \ \wedge \ \varphi(x_1, \ldots, x_n, b)) \ \vee \ (\neg[(\exists_1 y)\varphi(x_1, \ldots, x_n, y)] \wedge b = 0)$
   [$\vdash_K \alpha \rightarrow \alpha \vee \gamma$]
7. $\beta(x_1, \ldots, x_n, b)$
   [Abreviación de 6]
8. $(\exists y)\beta(x_1, \ldots, x_n, y)$
   [Regla E4]

Por lo tanto

$$\vdash_K (\exists y)\beta(x_1, \ldots, x_n, y)$$

.
Ahora, supongamos que $\vdash_K \beta(x_1, \ldots, x_n, u) \wedge \beta(x_1, \ldots, x_n, y)$. Como $\vdash_K \beta(x_1, \ldots, x_n, u)$, entonces

$$\vdash_K ([(\exists_1 y)\varphi(x_1, \ldots, x_n, y)] \ \wedge \ \varphi(x_1, \ldots, x_n, u)) \ \vee \ (\neg[(\exists_1 y)\varphi(x_1, \ldots, x_n, b)] \wedge u = 0)$$

Si $\vdash_K \neg[(\exists_1 y)\varphi(x_1, \ldots, x_n, b)] \wedge u = 0$, entonces se cumpliría que $\vdash_K \neg[(\exists_1 y)\varphi(x_1, \ldots, x_n, y)]$, pero estamos suponiendo que $\vdash_K (\exists_1 y)\varphi(x_1, \ldots, x_n, y)$, por lo que $\vdash_K \neg(\neg[(\exists_1 y)\varphi(x_1, \ldots, x_n, y)])$. Recordando que si $\alpha, \gamma \in \mathcal{FORM}$, $\vdash_K \alpha \vee \gamma \rightarrow (\neg\gamma \rightarrow \alpha)$ podemos concluir que $\vdash_K [(\exists_1 y)\varphi(x_1, \ldots, x_n, y)] \ \wedge \ \varphi(x_1, \ldots, x_n, u)$, así que

$$\vdash_K \varphi(x_1, \ldots, x_n, u)$$

De manera análoga podemos obtener que

$$\vdash_K \varphi(x_1, \ldots, x_n, y)$$

Como $\vdash_K (\exists y)\varphi(x_1, \ldots, x_n, y) \ \wedge \ (\forall x)(\forall y)(\varphi(x_1, \ldots, x_n, x) \wedge \varphi(x_1, \ldots, x_n, y)) \rightarrow x = y$, entonces
$\vdash_K \varphi(x_1, \ldots, x_n, u) \wedge \varphi(x_1, \ldots, x_n, y) \rightarrow u = y$, es decir

$$\vdash_K u = y$$

Por lo tanto $\beta(x_1, \ldots, x_n, u) \ \wedge \ \beta(x_1, \ldots, x_n, y) \vdash_K u = y$. Usando el teorema de la deducción y Gen dos veces, tenemos que

$$\vdash_K (\forall u)(\forall y)\beta(x_1, \ldots, x_n, u) \ \wedge \ \beta(x_1, \ldots, x_n, y) \rightarrow u = y$$

Ya tenemos que $\vdash_K (\exists y)\beta(x_1, \ldots, x_n, y)$ y que
$\vdash_K (\forall u)(\forall y)\beta(x_1, \ldots, x_n, u) \ \wedge \ \beta(x_1, \ldots, x_n, y) \rightarrow u = y$, entonces concluimos que

$$\vdash_K (\exists_1 y)\beta(x_1, \ldots, x_n, y)$$

Así concluimos que

$$\vdash_K (\exists_1 y)\varphi(x_1,\ldots,x_n,y) \to (\exists_1 y)\beta(x_1,\ldots,x_n,y)$$

ii) Supongamos que $\vdash_K \neg(\exists_1 y)\varphi(x_1,\ldots,x_n,y)$.
Sabemos que $\vdash_K 0=0$, así que $\vdash_K \neg(\exists_1 y)\varphi(x_1,\ldots,x_n,y) \ \wedge \ 0=0$, por lo que $\vdash_K ([(\exists_1 y)\varphi(x_1,\ldots,x_n,y)] \ \wedge \ \varphi(x_1,\ldots,x_n,0)) \ \vee \ (\neg[(\exists_1 y)\varphi(x_1,\ldots,x_n,y)] \wedge 0=0)$, es decir $\vdash_K \beta(x_1,\ldots,x_n,0)$.
Como 0 es libre para y en $\beta(x_1,\ldots,x_n,0)$, por la regla E4 se tiene que

$$\vdash_K (\exists y)\beta(x_1,\ldots,x_n,y)$$

Ahora, supongamos que $\vdash_K \beta(x_1,\ldots,x_n,u) \wedge \beta(x_1,\ldots,x_n,y)$. Como $\vdash_K \beta(x_1,\ldots,x_n,u)$, entonces

$$\vdash_K ([(\exists_1 y)\varphi(x_1,\ldots,x_n,y)] \ \wedge \ \varphi(x_1,\ldots,x_n,u)) \ \vee \ (\neg[(\exists_1 y)\varphi(x_1,\ldots,x_n,b)] \wedge u=0)$$

Si ocurriera que $\vdash_K [(\exists_1 y)\varphi(x_1,\ldots,x_n,y)] \wedge \varphi(x_1,\ldots,x_n,u)$, entonces $\vdash_K (\exists_1 y)\varphi(x_1,\ldots,x_n,y)$ pero por hipótesis tenemos que $\vdash_K \neg(\exists_1 y)\varphi(x_1,\ldots,x_n,y)$, así que $\vdash_K \neg([(\exists_1 y)\varphi(x_1,\ldots,x_n,y)] \ \wedge \ \varphi(x_1,\ldots,x_n,u))$, y así, $\vdash_K (\neg[(\exists_1 y)\varphi(x_1,\ldots,x_n,b)] \wedge u=0)$, por lo tanto $\vdash_K u=0$.
De manera análoga, se puede obtener que $\vdash_K y=0$. Así, se tiene que $\vdash_K u=y$
Por lo tanto $\beta(x_1,\ldots,x_n,u) \ \wedge \ \beta(x_1,\ldots,x_n,y) \vdash_K u=y$. Usando el teorema de la deducción y Gen dos veces, tenemos que

$$\vdash_K (\forall u)(\forall y)\beta(x_1,\ldots,x_n,u) \ \wedge \ \beta(x_1,\ldots,x_n,y) \to u=y$$

Así que

$$\vdash_K (\exists_1 y)\beta(x_1,\ldots,x_n,y)$$

Así, $(\exists_1 y)\neg\varphi(x_1,\ldots,x_n,y) \vdash_K (\exists_1 y)\beta(x_1,\ldots,x_n,y)$ y por el Teorema de la deducción se tiene que

$$\vdash_K (\exists_1 y)\neg\varphi(x_1,\ldots,x_n,y) \to (\exists_1 y)\beta(x_1,\ldots,x_n,y)$$

De i) y ii) tenemos que $\vdash_K (\exists_1 y)\varphi(x_1,\ldots,x_n,y) \to (\exists_1 y)\beta(x_1,\ldots,x_n,y)$ y que $\vdash_K (\exists_1 y)\neg\varphi(x_1,\ldots,x_n,y) \to (\exists_1 y)\beta(x_1,\ldots,x_n,y)$. Sabemos que si $\alpha,\gamma \in \mathcal{FORM}$, $\vdash_K ((\alpha\to\gamma) \ \wedge \ (\neg\alpha\to\gamma)) \to \gamma$, entonces con lo que tenemos y MP, concluimos que

$$\vdash_K (\exists_1 y)\beta(x_1,\ldots,x_n,y)$$

Por lo tanto f es fuertemente representable. ■

Ahora veamos unos ejemplos de funciones número teóricas que son representables.

Ejemplos 2. Las siguientes funciones son representables en una teoría K con igualdad del lenguaje $\mathcal{L}_A$.

a. La función cero en los naturales, definida como $Z:\mathbb{N}\longrightarrow\mathbb{N}$ tal que $Z(x)=0$.
Consideremos la siguiente $\varphi(x_1,y)\in\mathcal{FORM}$ tal que $\varphi(x_1,y) := (x_1=x_1 \ \wedge \ y=0)$. Sean $x,m\in\mathbb{N}$.

1. Supongamos que $Z(x)=m$, demostremos que $\vdash_K \varphi(\overline{x},\overline{m})$, es decir, veamos que $\vdash_K \overline{x}=\overline{x} \ \wedge \ \overline{m}=0$.
Tenemos que $Z(x)=0$ por definición y que $Z(x)=m$ por hipótesis, así que $m=0$, ademas por la Observación 3.4 se tiene que $\vdash_K \overline{m}=0$ y también tenemos que $\vdash_K \overline{x}=\overline{x}$, así que $\vdash_K \overline{x}=\overline{x} \ \wedge \ \overline{m}=0$.

2. Demostremos que $\vdash_K (\exists_1 y)\varphi(\overline{x}, y)$.
Sabemos que $\vdash_K \overline{x} = \overline{x}$ y que $\vdash_K 0 = 0$, entonces $\vdash_K \overline{x} = \overline{x} \ \wedge \ 0 = 0$, entonces por la regla (E4) se tiene que $\vdash_K (\exists y)(\overline{x} = \overline{x} \ \wedge \ y = 0)$.
Ahora, supongamos que $\vdash_K (\overline{x} = \overline{x} \ \wedge \ v = 0)$ y que $\vdash_K (\overline{x} = \overline{x} \ \wedge \ u = 0)$.
Demostremos que $v = u$.
Se tiene que $\vdash_K v = 0 \ \wedge \ u = 0$, así que $\vdash_K v = u$.
Por lo tanto se cumple que $\vdash_K (\exists_1 y)\varphi(\overline{x}, y)$

Así que, Z es representable en K.

b. La función sucesor, definida como $N : \mathbb{N} \longrightarrow \mathbb{N}$ tal que $N(x) = x + 1$ es representable en K por la fórmula $\varphi(x_1, y) := (y = x_1')$. En efecto para $x, m \in \mathbb{N}$ se tiene que:

1. Si $N(x) = m$, entonces $m = x+1$ y por la Observación 3.4 se tiene que $\vdash_K \overline{m} = \overline{x+1}$. Por el inciso *ii.* de la Proposición 3.8 y *(c)* de la Proposición 3.4 se cumple que $\vdash_K \overline{m} = \overline{x} + \overline{1}$. Así, recordando *(a)* de la Proposición 3.7 tenemos que $\vdash_K \overline{x} + \overline{1} = \overline{x}'$
Por lo que concluimos que $\vdash_K \overline{m} = \overline{x}'$, es decir $\vdash_K \varphi(\overline{x}, \overline{m})$
2. Por *(a)* de la Proposición 3.7 tenemos que $\vdash_K x_1 + \overline{1} = x_1'$, por la regla (E4) se tiene que $\vdash_K (\exists y)(y = x_1')$ y usando *(d)* de la Proposición 3.4 podemos concluir que $\vdash_K (\exists_1 y)(y = x_1')$, así, $\vdash_K (\exists_1 y)\varphi(x_1, y)$

Por lo que N es representable en K.

c. La función proyección, definida como $U_j^n : \mathbb{N}^n \longrightarrow \mathbb{N}$ tal que $U_j^n(x_1, \ldots, x_n) = x_j$ es representable en K por la fórmula $\varphi(x_1, \ldots, x_n, y) := (x_1 = x_1 \ \wedge \ldots \wedge x_n = x_n \ \wedge \ y = x_j)$

d. Sean $g : \mathbb{N}^m \longrightarrow \mathbb{N}$, $h_1 : \mathbb{N}^n \longrightarrow \mathbb{N}, \ldots, h_m : \mathbb{N}^n \longrightarrow \mathbb{N}$ funciones fuertemente representables en K por las fórmulas $\varphi(x_1, \ldots, x_m, z), \beta_1(x_1, \ldots, x_n, y_1), \ldots, \beta_m(x_1, \ldots, x_n)$, respectivamente. Definimos la función $f : \mathbb{N}^m \longrightarrow \mathbb{N}$ tal que

$$f(x_1, \ldots, x_m) = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_m)).$$

Decimos que obtenemos f por sustitución a partir de $g, h_1, \ldots, h_m$. Como probamos enseguida, f es fuertemente representable en K por la fórmula

$$\gamma(x_1, \ldots, x_m, z) := (\exists y_1) \ldots (\exists y_m)(\beta_1(x_1, \ldots, x_n, y_1) \wedge \ldots \wedge \beta_m(x_1, \ldots, x_n) \wedge \varphi(y_1, \ldots, y_m, z))$$

Sean $k_1, \ldots, k_m, p \in \mathbb{N}$

1. Para $j \in \{1, \ldots, m\}$ denotemos a $h_j(x_1, \ldots, x_n) = r_j$. Supongamos que $f(k_1, \ldots, k_m) = p$, entonces se tiene que $g(r_1, \ldots, r_m) = p$. Como $h_j(x_1, \ldots, x_n) = r_j$ y $\beta_j(x_1, \ldots, x_n, y_1)$ representa a h_j en K, tenemos que $\vdash_K \beta_j(\overline{k_1}, \ldots, \overline{k_n}, \overline{r_j})$. Como $g(r_1, \ldots, r_m) = p$ y $\varphi(x_1, \ldots, x_m, z)$ representa a g en K entonces $\vdash_K \varphi(\overline{r_1}, \ldots, \overline{r_m}, \overline{p})$. Así que $\vdash_K \beta_1(\overline{k_1}, \ldots, \overline{k_n}, \overline{r_1}) \wedge \ldots \wedge \beta_m(\overline{k_1}, \ldots, \overline{k_n}, \overline{r_m}) \wedge \ \varphi(\overline{r_1}, \ldots, \overline{r_m}, \overline{p})$, así, por la regla (E4) se cumple que
$$\vdash_K \gamma(\overline{k_1}, \ldots, \overline{k_m}, \overline{p})$$
.
2. Como $\beta_j(x_1, \ldots, x_n, y_1)$ representa a h_j en K se cumple que $\vdash_K (\exists y_j)\beta(x_1, \ldots, x_m, y_j)$ para $j \in \{1, \ldots, m\}$. Así que $\vdash_K (\exists y_1) \ldots (\exists y_m)\beta_1(x_1, \ldots, x_n, y_1) \wedge \ldots \wedge \beta_m(x_1, \ldots, x_n, y_m)$.
Como $\varphi(x_1, \ldots, x_m, z)$ representa a g en K entonces $\vdash_K (\exists z)\varphi(x_1, \ldots, x_m, z)$.
Ahora, supongamos que $\vdash_K \gamma(x_1, \ldots, x_m, u)$ y $\vdash_K \gamma(x_1, \ldots, x_m, v)$, veamos que $u = v$.
Como $\vdash_K \gamma(x_1, \ldots, x_m, u)$, entonces es teorema en K:
$$(\exists y_1) \ldots (\exists y_m)(\beta_1(x_1, \ldots, x_n, y_1) \wedge \ldots \wedge \beta_m(x_1, \ldots, x_n, y_m) \wedge \varphi(y_1, \ldots, y_m, u)) \quad (1)$$

Si aplicamos la regla C a (1) m veces tenemos que

$$\vdash_K \beta_1(x_1,\ldots,x_n,b_1)\wedge\ldots\wedge\beta_m(x_1,\ldots,x_n,b_m)\wedge\varphi(b_1,\ldots,b_m,u)$$

Como $\vdash_K \gamma(x_1,\ldots,x_m,v)$, entonces es teorema en K:

$$(\exists y_1)\ldots(\exists y_m)(\beta_1(x_1,\ldots,x_n,y_1)\wedge\ldots\wedge\beta_m(x_1,\ldots,x_n,y_m)\wedge\varphi(y_1,\ldots,y_m,v)) \quad (2)$$

Si aplicamos la regla C a (2) m veces tenemos que

$$\vdash_K \beta_1(x_1,\ldots,x_n,c_1)\wedge\ldots\wedge\beta_m(x_1,\ldots,x_n,c_m)\wedge\varphi(c_1,\ldots,c_m,v)$$

Sabemos que para $j\in\{1,\ldots,m\}$, $\vdash_K (\exists_1 y_j)\beta_j(x_1,\ldots,x_m,y_j)$ y como tenemos que $\vdash_K \beta_j(x_1,\ldots,x_n,b_1)$ y $\vdash_K \beta_j(x_1,\ldots,x_n,c_j)$, concluimos que $b_j = c_j$. Como $\vdash_K \varphi(c_1,\ldots,c_m,v)$, si aplicamos (A7) m veces tenemos que $\vdash_K \varphi(b_1,\ldots,b_m,v)$ pero también tenemos que $\vdash_K \varphi(b_1,\ldots,b_m,u)$, y, como $\varphi(x_1,\ldots,x_m,z)$ representa a g en K se tiene que $\vdash_K (\exists_1 z)(\varphi(x_1,\ldots,x_m,z))$ concluimos que $\vdash_K u=v$.
Por lo tanto

$$\vdash_K (\exists_1 z)\gamma(x_1,\ldots,x_m,z)$$

De 1. y 2. concluimos que f es fuertemente representable en K.

Definición 4.6. Sea R una relación de n argumentos, definimos la función característica $C_R:\mathbb{N}^n\longrightarrow\{0,1\}$ como sigue:

$$C_R(x_1,\ldots,x_n)=\begin{cases}0 & \text{si} \quad R(x_1,\ldots,x_n) \text{ es verdadera}\\ 1 & \text{si} \quad R(x_1,\ldots,x_n) \text{ es falsa}\end{cases}$$

Proposición 4.7. *Si K es una teoría con igualdad en el lenguaje $\mathcal{L}_A$ tal que $\vdash_K 0\neq\overline{1}$, entonces una relación número-teórica R es expresable en K si y solo si C_R es representable en K.*

Demostración. Supongamos que R es expresable en K por una fórmula $\varphi(x_1,\ldots,x_n)\in\mathcal{FORM}$. Veamos que C_R es representable en K.
Proponemos la fórmula

$$\psi(x_1,\ldots,x_n,y):=(\varphi(x_1,\ldots,x_n)\wedge y=0)\vee(\neg\varphi(x_1,\ldots,x_n)\wedge y=\overline{1}).$$

Sean $k_1,\ldots,k_n,m\in\mathbb{N}$.

1. Supongamos que $C_R(k_1,\ldots,k_n)=m$

   i. Si $m=1$, entonces $C_R(k_1,\ldots,k_n)=1$, así que $R(k_1,\ldots,k_n)$ es falsa y como R es representable, entonces $\vdash_K \neg\varphi(\overline{k_1},\ldots,\overline{k_n})$, además sabemos que $\vdash_K \overline{1}=\overline{1}$, así que $\vdash_K \neg\varphi(\overline{k_1},\ldots,\overline{k_n})\wedge\overline{1}=\overline{1}$. Entonces podemos concluir que

   $$\vdash_K (\varphi(\overline{k_1},\ldots,\overline{k_n})\wedge\overline{1}=0)\vee(\neg\varphi(\overline{k_1},\ldots,\overline{k_n})\wedge\overline{1}=\overline{1})$$

   es decir
   $$\vdash_K \psi(\overline{k_1},\ldots,\overline{k_n},\overline{1}).$$

   ii. Si $m=0$, entonces $C_R(k_1,\ldots,k_n)=0$, así que $R(k_1,\ldots,k_n)$ es verdadera y como R es representable, entonces $\vdash_K \varphi(\overline{k_1},\ldots,\overline{k_n})$, además sabemos que $\vdash_K 0=0$, así que $\vdash_K \varphi(\overline{k_1},\ldots,\overline{k_n})\wedge 0=0$. Entonces podemos concluir que

   $$\vdash_K (\varphi(\overline{k_1},\ldots,\overline{k_n})\wedge 0=0)\vee(\neg\varphi(\overline{k_1},\ldots,\overline{k_n})\wedge 0=\overline{1})$$

   es decir
   $$\vdash_K \psi(\overline{k_1},\ldots,\overline{k_n},0)$$

Entonces, si $C_R(k_1, \ldots, k_n) = m$ se cumple que $\vdash_K \psi(\overline{k_1}, \ldots, \overline{k_n}, \overline{m})$

2. Sin pérdida de generalidad supongamos que $C_R(k_1, \ldots, k_n) = 0$, entonces por 1. tenemos que $\vdash_K \psi(\overline{k_1}, \ldots, \overline{k_n}, 0)$, y por la regla (E4) se cumple que

$$\vdash_K (\exists y)\psi(\overline{k_1}, \ldots, \overline{k_n}, y).$$

Ahora supongamos que $\vdash_K \psi(\overline{k_1}, \ldots, \overline{k_n}, y)$ y $\vdash_K \psi(\overline{k_1}, \ldots, \overline{k_n}, x)$.
Como R es expresable en K y $R(k_1, \ldots, k_n)$ es verdadera entonces, $\vdash_K \varphi(\overline{k_1}, \ldots, \overline{k_n})$, así que $\vdash_K \neg\neg\varphi(\overline{k_1}, \ldots, \overline{k_n})$, entonces $\vdash_K \neg\neg\varphi(\overline{k_1}, \ldots, \overline{k_n}) \vee y \neq \overline{1}$, por lo que
$\vdash_K \neg(\neg\varphi(\overline{k_1}, \ldots, \overline{k_n}) \wedge y = \overline{1})$. Como $\vdash_K \psi(\overline{k_1}, \ldots, \overline{k_n}, y)$, entonces
$\vdash_K (\varphi(\overline{k_1}, \ldots, \overline{k_n}) \wedge y = 0) \vee (\neg\varphi(\overline{k_1}, \ldots, \overline{k_n}) \wedge y = \overline{1})$ Recordando que $\vdash_K \alpha \vee \beta \to \neg\beta \to \alpha$ y utilizando MP concluimos que $\vdash_K (\varphi(\overline{k_1}, \ldots, \overline{k_n}) \wedge y = 0)$.
De la misma manera al razonamiento anterior podemos deducir que $(\varphi(\overline{k_1}, \ldots, \overline{k_n}) \wedge x = 0)$.
Entonces $\vdash_K y = 0$ y $\vdash_K x = 0$, así que $\vdash_K x = y$ Por lo tanto

$$\vdash_K (\exists_1 y)\psi(\overline{k_1}, \ldots, \overline{k_n}, y).$$

Así, C_R es representable en K.

Supongamos ahora que C_R es representable por una fórmula $\varphi(x_1, \ldots, x_n, y) \in \mathcal{FORM}$. Veamos que R es expresable en K. Proponemos a la fórmula $\varphi(x_1, \ldots, x_n, 0)$. Sean $k_1, \ldots, k_n \in \mathbb{N}$

1. Si R es verdadera, entonces por definición de C_R se tiene que $C_R(k_1, \ldots, k_n) = 0$, y como C_R es representable en K obtenemos que $\vdash_K \varphi(\overline{k_1}, \ldots, \overline{k_n}, 0)$.

2. Si R es falsa, entonces $C_R(k_1, \ldots, k_n) = 1$ y como C_R es representable en K, se tiene que $\vdash_K \varphi(\overline{k_1}, \ldots, \overline{k_n}, \overline{1})$. Además también sabemos que $\vdash_K (\exists_1 y)\varphi(\overline{k_1}, \ldots, \overline{k_n}, y)$, es decir

$$\vdash_K (\exists y)\varphi(\overline{k_1}, \ldots, \overline{k_n}, y) \wedge (\forall u)(\forall v)(\varphi(\overline{k_1}, \ldots, \overline{k_n}, u) \wedge \varphi(\overline{k_1}, \ldots, \overline{k_n}, u) \to u = v)$$

Como $\vdash_K (\forall u)(\forall v)(\varphi(\overline{k_1}, \ldots, \overline{k_n}, u) \wedge \varphi(\overline{k_1}, \ldots, \overline{k_n}, u) \to u = v)$ y además $0, \overline{1}$ son términos libres para u y v respectivamente, por la regla (A4) tenemos que

$$\vdash_K \varphi(\overline{k_1}, \ldots, \overline{k_n}, 0) \wedge \varphi(\overline{k_1}, \ldots, \overline{k_n}, \overline{1}) \to 0 = \overline{1}$$

Si suponemos que $\vdash_K \varphi(\overline{k_1}, \ldots, \overline{k_n}, 0)$, entonces tendríamos que
$\vdash_K \varphi(\overline{k_1}, \ldots, \overline{k_n}, 0) \wedge \varphi(\overline{k_1}, \ldots, \overline{k_n}, \overline{1})$, así que por MP se cumpliría que $\vdash_K 0 = \overline{1}$, pero por hipótesis tenemos que $\vdash_K 0 \neq \overline{1}$. Por lo tanto $\vdash_K \neg\varphi(\overline{k_1}, \ldots, \overline{k_n}, 0)$.

Así, R es expresable en K. ∎

4.2. Funciones y relaciones recursivas

En la sección anterior estudiamos la representabilidad y expresabilidad de funciones y relaciones número-teóricas. En esta nos enfocaremos en estudiar una clase específica de funciones y relaciones número-teóricas: las recursivas.
Primero veamos qué son las funciones y relaciones recursivas y el proceso que seguimos para obtenerlas. Comencemos estudiando las siguientes funciones número-teóricas

Definición 4.8. 1. Llamamos a las siguientes funciones número-teóricas *funciones iniciales*:

I. La función cero $Z : \mathbb{N} \longrightarrow \mathbb{N}$ tal que para $x \in \mathbb{N}$, $Z(x) = 0$.

II. La función sucesor $S : \mathbb{N} \longrightarrow \mathbb{N}$ tal que para $x \in \mathbb{N}$, $S(x) = x + 1$.

III. Las funciones proyección $P_i^n : \mathbb{N}^n \longrightarrow \mathbb{N}$ tal que para $(x_1, \ldots, x_n) \in \mathbb{N}^n$
$P_i^n(x_1, \ldots, x_n) = x_i$.

2. La siguientes son reglas para obtener funciones número-teóricas a partir de las funciones iniciales:

IV. *Regla de sustitución*: $f : \mathbb{N}^n \longrightarrow \mathbb{N}$ tal que

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

Donde $g : \mathbb{N}^m \to \mathbb{N}$ y para $i \in \{1, \ldots, m\}$ $h_i : \mathbb{N}^n \longrightarrow \mathbb{N}$. Decimos que obtenemos f por sustitución de las funciones g y h_i

V. *Regla de recursión*: Si $g : \mathbb{N}^n \longrightarrow \mathbb{N}$ y $h : \mathbb{N}^{n+2} \longrightarrow \mathbb{N}$, entonces definimos la función $f : \mathbb{N}^{n+1} \longrightarrow \mathbb{N}$ como:

$$f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n)$$

$$f(x_1, \ldots, x_n, y+1) = h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y))$$

Para el caso en el que $n = 0$ tenemos que

$$f(0) = k, \text{ donde } k \in \mathbb{N}$$

$$f(y+1) = h(y, f(y))$$

Decimos que obtenemos f de g y h por recursión y a $x_1, \ldots, x_n$ los llamamos parámetros de la recursión.

VI. *Regla del $\mu-$ Operador restringido*: Supongase que $g : \mathbb{N}^m \longrightarrow \mathbb{N}$ y que para cualesquiera $x_1, \ldots, x_n \in \mathbb{N}$ se tiene que existe al menos un $y \in \mathbb{N}$ tal que
$g(x_1, \ldots, x_n, y) = 0$. Denotaremos por $\mu y_0\big(g(x_1, \ldots, x_n, y_0) = 0\big)$ al menor $y_0 \in \mathbb{N}$ tal que $g(x_1, \ldots, x_n, y_0) = 0$.
Sea $f : \mathbb{N}^n \longrightarrow \mathbb{N}$ donde $f(x_1, \ldots, x_n) = \mu y_0\big(g(x_1, \ldots, x_n, y_0) = 0\big)$.
Decimos que obtenemos f a partir de g a través del $\mu-$operador restringido siempre que se cumplan las condiciones para g.

En general podemos aplicar la regla del $\mu-$operador restringido para cualquier relación.
Para cualquier relación $R(x_1, \ldots, x_n, y)$, denotamos por $\mu y_0\big(R(x_1, \ldots, x_n, y)\big)$ al menor $y_0 \in \mathbb{N}$ tal que $R(x_1, \ldots, x_n, y_0)$ es verdadera, siempre que exista al menos un $y \in \mathbb{N}$ en la que se cumple $R(x_1, \ldots, x_n, y)$

3. Una función f es una *función primitiva recursiva* si y solo si puede ser obtenida a partir de las funciones iniciales aplicando un número finito de veces las reglas IV y V, es decir si existe una sucesión de funciones $f_0, \ldots, f_n$ tales que $f_n = f$ y para $i \in \{0, \ldots, n\}$ f_i es una función inicial o f_i surge de las funciones anteriores de la sucesión por aplicaciones de las reglas IV o V.

4. Decimos que una función f es *recursiva* si es obtenida de las funciones iniciales con un numero finito de aplicaciones de las reglas IV, V y VI, Así, toda función primitiva recursiva es recursiva.

Nota. De aquí en adelante, se hará saber al lector cuando sea necesario la distinción entre función recursiva primitiva y función recursiva.

Ejemplos 3. Cuando construimos funciones recursivas, la idea siempre es partir de funciones iniciales y aplicar las reglas IV, V y VI de la Definición 4.8. Veamos algunos ejemplos:

a) Si tomamos las funciones iniciales $S : \mathbb{N} \longrightarrow \mathbb{N}$ tal que $S(n) = n+1$ y $P_3^3 : \mathbb{N}^3 \longrightarrow \mathbb{N}$ tal que $P_3^3(m, n, r) = r$ podemos obtener una nueva función primitiva recursiva con la composición de S con P_3^3, así definimos $h : \mathbb{N}^3 \longrightarrow \mathbb{N}$ tal que $h(m, n, r) = S(P_3^3(m, n, r)) = S(r) = r+1$.

b) La función $f_1 : \mathbb{N}^2 \longrightarrow \mathbb{N}$ tal que $f_1(m, n) = m + n$ es una función primitiva recursiva, en efecto:
Podemos definir a f_1 utilizando la regla de V de recursión como sigue:

$$\begin{aligned} f_1(m, 0) = &\quad P_1^1(m) \\ f_1(m, n+1) = &\quad h(m, n, f_1(m, n)) \end{aligned}$$

Donde $h : \mathbb{N}^3 \longrightarrow \mathbb{N}$ es la función primitiva recursiva expuesta en el inciso a), así tenemos que

$$\begin{aligned} f_1(m, 0) = &\quad P_1^1(m) = m \\ f_1(m, n+1) = &\quad S(P_3^3(m, n, f_1(m, n))) = f_1(m, n) + 1 \end{aligned}$$

c) La función $f_2 : \mathbb{N}^2 \longrightarrow \mathbb{N}$ tal que $f_2(m, n) = mn$ es una función primitiva recursiva. En efecto, notemos primero lo siguiente:
En el inciso b) vimos que $f_1 : \mathbb{N}^2 \longrightarrow \mathbb{N}$ tal que $f_1(m, n) = m + n$ es primitiva recursiva. Si definimos la función $h : \mathbb{N}^3 \longrightarrow \mathbb{N}$ tal que $h(m, n, r) = f_1(P_1^3(m, n, r), P_3^3(m, n, r))$. h se obtiene por sustitución de las funciones f_1, P_1^3 y P_3^3, entonces como P_1^3 y P_3^3 son funciones iniciales y f_1 es primitiva recursiva, entonces h es primitiva recursiva.
Ahora, definamos la función f_2 utilizando la regla de recursión:

$$\begin{aligned} f_2(m, 0) = &\quad Z(m) \\ f_2(m, n+1) = &\quad h(m, n, f_2(m, n)) \end{aligned}$$

Pero $h(m, n, f_2(m, n)) = f_1(P_1^3(m, n, f_2(m, n)), P_3^3(m, n, f_2(m, n)))$, es decir, $h(m, n, f_2(m, n)) = f_1(m, f_2(m, n))$. Así que:

$$\begin{aligned} f_2(m, 0) = &\quad 0 \\ f_2(m, n+1) = &\quad f_1(m, f_2(m, n)) \end{aligned}$$

Por lo que f_2 es una función recursiva.

d) La función $g : \mathbb{N} \longrightarrow \mathbb{N}$ tal que $g(n) = n^2$ es primitiva recursiva pues podemos definir a g de la siguiente manera:

$$g(n) = f_2(P_1^1(n), P_1^1(n))$$

Es decir obtuvimos g por sustitución de la función primitiva recursiva f_2 y la función inicial P_1^1, por lo tanto g es primitiva recursiva.

e) La función $f : \mathbb{N}^2 \longrightarrow \mathbb{N}$ tal que $f(m, n) = m^2 + mn$ es primitiva recursiva, en efecto, definamos a f de la siguiente manera:

$$f(m, n) = f_2(P_1^2(m, n), f_1(m, n))$$

Así, f se obtiene por sustitución de las funciones f_2, P_1^2 y f_1, por lo que f es primitiva recursiva.

f) La función $f : \mathbb{N}^2 \longrightarrow \mathbb{N}$ tal que $f(n, p) = q$ donde q es el menor número tal que $n + q \equiv 0 \operatorname{mód} p$ donde $n, p \in \mathbb{N}$, se tiene que f es recursiva. En efecto:
Notemos que para $n, p, q \in \mathbb{N}$, por el algoritmo de la división se cumple que existen únicos $z, r \in \mathbb{N}$ tales que $n + q = pz + r$ con $0 \leq r < p$. Entonces podemos definir la función $g : \mathbb{N}^3 \longrightarrow \mathbb{N}$ tal que $g(n, p, q) = r$ donde r es el residuo de dividir $n + q$ por p.
Así podemos definir a $f : \mathbb{N}^2 \longrightarrow \mathbb{N}$ tal que $f(n, p) = \mu q_0(g(n, p, q_0) = r)$, así, f se obtuvo a partir de g a través del $\mu-$operador restringido.

Proposición 4.9. *Sea* $g : \mathbb{N}^k \longrightarrow \mathbb{N}$ *una función recursiva. Sean* $x_1, \ldots, x_n \in \mathbb{N}$ *variables distintas, y para* $1 \leq i \leq k$*, sea* z_i *alguna de las variables* $x_1, \ldots, x_n$*. Entonces la función* $f : \mathbb{N}^n \longrightarrow \mathbb{N}$ *tal que* $f(x_1, \ldots, x_n) = g(z_1, \ldots, z_k)$ *es una función recursiva.*

Demostración. Como para $1 \leq i \leq k$, z_i es alguna de las variables $x_1, \ldots, x_n$, podemos denotar, para $1 \leq i \leq k$, $z_i = x_{j_i}$, entonces se tiene que $z_i = P^n_{j_i}(x_1, \ldots, x_n)$. Así, se cumple que $g(z_1, \ldots, z_k) = g(P^n_{j_1}(x_1, \ldots, x_n), \ldots, P^n_{j_k}(x_1, \ldots, x_n))$. Pero teníamos que
$f(x_1, \ldots, x_n) = g(z_1, \ldots, z_k)$, entonces,

$$f(x_1, \ldots, x_n) = g(P^n_{j_1}(x_1, \ldots, x_n), \ldots, P^n_{j_k}(x_1, \ldots, x_n))$$

Sabemos que g es recursiva y P_{j_i} son funciones iniciales, así que f se obtiene por sustitución de las funciones g y P_{j_i}, por lo tanto, f es recursiva. ∎

Ejemplos 4. Podemos usar la proposición anterior para definir nuevas funciones recursivas a partir de funciones ya conocidas:

1. *Añadir variables tontas:* Si $g : \mathbb{N}^2 \longrightarrow \mathbb{N}$ es recursiva y definimos $f : \mathbb{N}^3 \longrightarrow \mathbb{N}$ tal que $f(x_1, x_2, x_3) = g(x_1, x_2)$ entonces f es recursiva, en efecto, por la Proposición 4.9 si $z_1 = x_1$ y $z_2 = x_2$, se tiene que la función $f(x_1, x_2, x_3) = g(z_1, z_2)$ es recursiva.

2. *Permutar variables:* Si $g : \mathbb{N}^3 \longrightarrow \mathbb{N}$ es recursiva y definimos $f : \mathbb{N}^3 \longrightarrow \mathbb{N}$ tal que $f(x_1, x_2, x_3) = g(x_3, x_1, x_2)$, entonces f es recursiva pues por la proposición 4.9 consideramos $z_1 = x_3, z_2 = x_1$ y $z_3 = x_2$.

3. *Identificar variables:* Si la función $g : \mathbb{N}^3 \longrightarrow \mathbb{N}$ es una función recursiva, entonces, la función $f : \mathbb{N}^2 \longrightarrow \mathbb{N}$ tal que $f(x_1, x_2) = g(x_1, x_2, x_1)$ también es recursiva pues podemos considerar $z_1 = x_1, z_2 = x_2$ y $z_3 = x_1$ y aplicamos la Proposición 4.9.

Proposición 4.10. *La siguientes funciones número-teóricas son recursivas:*

a) $f_1(x, y) = x + y$

b) $f_2(x, y) = xy$

c) La función constante para $k \in \mathbb{N}$*:*
$C_k(x) = k$

d) $f_3(x, y) = x^y$

e) La función antecesor δ*:*
$$\delta(x) = \begin{cases} x - 1 & si \quad x > 0 \\ 0 & si \quad x = 0 \end{cases}$$

f) La función resta:
$$x \dot{-} y = \begin{cases} x - y & si \quad x \geq y \\ 0 & si \quad x < y \end{cases}$$

g) La función distancia:
$$|x - y| = \begin{cases} x - y & si \quad x \geq y \\ y - x & si \quad x < y \end{cases}$$

h) La función signo:
$$sg(x) = \begin{cases} 0 & si \quad x = 0 \\ 1 & si \quad x \neq 0 \end{cases}$$

i) $\overline{sg}(x) = \begin{cases} 1 & si \quad x = 0 \\ 0 & si \quad x \neq 0 \end{cases}$

j) $f_4(x) = x!$

k) *La función mínimo:*
$min(x, y) :=$ *el mínimo de* x *e* y

l) $min(x_1, \ldots, x_n)$

m) *La función máximo:*
$max(x, y) :=$ *el máximo de* x *e* y

n) $max(x_1, \ldots, x_n)$

o) *La función residuo:*
$rm(x, y) :=$ *el residuo de la división de* y *por* x

p) *La función cociente:*
$qt(x, y) :=$ *el cociente de la división de* y *por* x

Demostración. Ya probamos en los Ejemplos 3 (incisos b) y c)) que las funciones f_1, f_2 son recursivas.

c) Podemos definir a C_k de manera recursiva como sigue:

$$\begin{aligned} C_k(0) = &\quad k \\ C_k(y+1) = &\quad P_2^2(y, C_k(y)). \end{aligned}$$

Como P_2^2 es función inicial, entonces C_k es función recursiva.

d) Podemos definir a f_3 de manera recursiva como sigue:

$$\begin{aligned} f_3(x, 0) = &\quad C_1(x) = 1 \\ f_3(x, y+1) = &\quad f_2(x, f_3(x, y)). \end{aligned}$$

Como $C_1(x)$ y f_2 son funciones recursivas, podemos concluir que f_3 es una función recursiva.

e) Podemos definir a δ de manera recursiva como sigue:

$$\begin{aligned} \delta(0) = &\quad Z(0) = 0 \\ \delta(y+1) = &\quad P_1^2(y, \delta(y)). \end{aligned}$$

Como $Z(x)$ y P_1^2 son funciones iniciales, podemos concluir que δ es una función recursiva.

f) Definimos a $x \dot{-} y$ de manera recursiva:

$$\begin{aligned} x \dot{-} 0 = &\quad P_1^1(x) \\ x \dot{-} (y+1) = &\quad \delta(x \dot{-} y). \end{aligned}$$

g) Podemos definir a $|x - y|$ de la siguiente manera:

$$|x - y| = f_1(x \dot{-} y, y \dot{-} x).$$

Así $|x - y|$ se obtiene de sustitución de las funciones recursivas f_1 y $x \dot{-} y$.

h) Denotemos $f(x, y) := x \dot{-} y$. Podemos definir a sg de la siguiente manera:

$$sg(x) = f(P_1^1(x), \delta(x)).$$

Es decir:

$$sg(x) = x \dot{-} \delta(x).$$

Así, sg se obtuvo por sustitución de las funciones f, P_1^1 y δ, que son funciones recursivas, por lo tanto, sg es recursiva.

i) Denotemos $f(x,y) := x \dot{-} y$. Podemos definir a $\overline{sg}$ de la siguiente manera:

$$\overline{sg}(x) = f(C_1(x), sg(x)).$$

Es decir:

$$\overline{sg}(x) = 1 \dot{-} sg(x).$$

Así, $\overline{sg}$ se obtuvo por sustitución de las funciones f, C_1 y sg, que son funciones recursivas, por lo tanto, $\overline{sg}$ es recursiva.

j) Definamos f_4 de manera recursiva como sigue:

$$\begin{aligned} f_4(0) =& \quad 1 \\ f_4(y+1) =& \quad f_2(f_4(y), S(y)). \end{aligned}$$

Es decir:

$$\begin{aligned} f_4(0) =& \quad 1 \\ f_4(y+1) =& \quad (f_4(y))(y+1). \end{aligned}$$

Como, f_2 es recursiva y S es función inicial, podemos concluir que f_4 es recursiva.

k) Denotemos $f(x,y) := x \dot{-} y$. Podemos definir a min como sigue:

$$min(x,y) = f(P_1^2(x,y), f(x,y)),$$

es decir:

$$min(x,y) = x \dot{-} (x \dot{-} y).$$

Así, min se obtuvo por sustitución de las funciones f y P_1^2, por lo que min es recursiva.

l) Hagamos la prueba por inducción sobre n.
Para $n = 2$, ya sabemos que $min(x_1, x_2)$ es función recursiva.
Ahora, supongamos que $min(x_1, \ldots, x_n)$ es recursiva.
Demostremos que $min(x_1, \ldots, x_n, x_{n+1})$ es recursiva.
Sea $f(x_1, \ldots, x_n, x_{n+1}) = min(x_1, \ldots, x_n)$ Por la proposición 4.9 tenemos que $f : \mathbb{N}^{n+1} \longrightarrow \mathbb{N}$ es una función recursiva. Ahora, podemos definir a $min(x_1, \ldots, x_n, x_{n+1})$ de la siguiente manera:

$$min(x_1, \ldots, x_n, x_{n+1}) = min(f(x_1, \ldots, x_n, x_{n+1}), P_{n+1}^{n+1}(x_1, \ldots, x_n, x_{n+1})).$$

Es decir:

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

Así, $min(x_1, \ldots, x_n, x_{n+1})$ se obtuvo por sustitución de las funciones f y P_{n+1}^{n+1}. Por tanto $min(x_1, \ldots, x_n, x_{n+1})$ es recursiva. Así que $min(x_1, \ldots, x_n)$ es recursiva.

m) Denotemos $f(x,y) := x \dot{-} y$. Podemos definir a max de la siguiente manera:

$$max(x,y) = f_1(P_2^2(x,y), f(x,y)).$$

Es decir:

$$max(x,y) = y + (x \dot{-} y).$$

max se obtuvo por sustitución de las funciones f_1, P_2^2 y f, que son recursivas, por tanto, max es recursiva.

n) De manera análoga a l), podemos probar que $max(x_1, \ldots, x_n)$ es recursiva.

o) Notemos que si $r(x, y) = r$ y $qt(x, y) = q$ entonces se cumple que, por el algoritmo de la división en los números naturales, $y = qx+r$ donde $0 \leq r < x$, entonces, $y+1 = qx+(r+1)$. Como $r < x$ entonces $r + 1 \leq x$.

- Si $r + 1 < x$ entonces tenemos que $rm(x, y + 1) = r + 1$ y $qt(x, y) = x$.
- Si $r + 1 = x$ entonces $y + 1 = qx + x = x(q + 1)$, así que $rm(x, y + 1) = 0$ y $qt(x, y + 1) = q + 1$

Con esto en mente podemos definir a rm de manera recursiva:

$$\begin{aligned} rm(x, 0) = &\quad 0 \\ rm(x, y + 1) = &\quad f_2(S(rm(x, y)), sg(|x - S(rm(x, y))|)), \end{aligned}$$

donde $f_2, S, sg, |x - y|$ son funciones recursivas, por tanto rm es recursiva.

p) Con el desarrollo de o) podemos definir a qt de manera recursiva:

$$\begin{aligned} qt(x, 0) = &\quad 0 \\ qt(x, y + 1) = &\quad f_1(qt(x, y), \overline{sg}(|x - S(rm(x, y))|)), \end{aligned}$$

donde $f_1, S, \overline{sg}, |x - y|, rm$ son funciones recursivas, por tanto qt es recursiva.

■

Definición 4.11. Dadas expresiones para relaciones número-teóricas, es posible aplicar los conectivos del cálculo proposicional para obtener nuevas relaciones. Si R_1, R_2 son relaciones número-teóricas, entonces:

1. $R_1 \wedge R_2$ es una relación que se cumple siempre que R_1 y R_2 se cumplan.
2. $\neg R_1$ es una relación que se cumple siempre que R_1 no se cumpla.
3. $R_1 \vee R_2$ es una relación que se cumple siempre que se cumpla alguna de las dos relaciones.
4. $R_1 \Rightarrow R_2$ es una relación que se cumple si siempre que R_1 se cumpla, R_2 también se cumple.
5. Denotamos como $(\forall y)_{y<z} R(x_1, \ldots, x_n, y)$ a la relación: Para toda y si $y < z$, entonces $R(x_1, \ldots, x_n, y)$ se cumple. Lo llamamos cuantificador acotado.
6. Se define el μ-operador acotado:

$$\mu y_{y<z} R(x_1, \ldots, x_n, y) = \begin{cases} \text{el menor } y < z \text{ para el cual } R(x_1, \ldots, x_n, y) \text{ se cumple} & \text{si existe tal } y \\ z & \text{en cualquier otro caso} \end{cases}$$

Observación 4.4. También se pueden generar de manera análoga a 5. de la definición anterior las relaciones
$(\forall y)_{y\leq z} R(x_1, \ldots, x_n, y), (\exists y)_{y<z} R(x_1, \ldots, x_n, y)$ y $(\exists y)_{y\leq z} R(x_1, \ldots, x_n, y)$.

Definición 4.12. Una relación número-teórica $r \subseteq \mathbb{N}^n$ se llama relación primitiva recursiva (o recursiva) si y solo si su función característica C_R es una función primitiva recursiva (o recursiva). Como caso particular un conjunto A de números naturales es primitivo recursivo (o recursivo) si y solo si su función característica C_A es primitiva recursiva (o recursiva).

Ejemplos 5. Las siguientes son ejemplos de relaciones recursivas:

1. La relación $x_1 = x_2$ en $\mathbb{N}^2$. La función característica de la igualdad, que llamamos $C_= : \mathbb{N}^2 \to \{0,1\}$ esta dada por:

$$C_=(x_1,x_2) = \begin{cases} 0 & \text{si} \quad x_1 = x_2 \\ 1 & \text{si} \quad x_1 \neq x_2. \end{cases}$$

Podemos definir a $C_=$ de la siguiente manera:

$$C_=(x_1,x_2) = sg(|x_1 - x_2|).$$

De esta manera, $C_=$ se obtuvo por sustitución de las funciones sg y $|x_1 - x_2|$ que son funciones recursivas, así, $C_=$ es recursiva. Por tanto, la igualdad es una relación recursiva.

2. La relación $x_1 < x_2$ en $\mathbb{N}^2$ pues su función característica $C_<$ se puede definir como:

$$C_<(x_1,x_2) = \overline{sg}(x_2 \dot{-} x_1).$$

Observación 4.5. La definición de relación recursiva se puede utilizar para definir cuándo un conjunto es recursivo. Decimos que $A \subseteq \mathbb{N}$ es recursivo si la función característica de A es función recursiva. En este caso, la función característica de un conjunto es la función característica de la relación "$\in A$".

Ejemplo 7. a. $\mathbb{N}$ es un conjunto recursivo pues su función característica es la función cero.

b. $\emptyset$ es recursivo pues su función característica es una función constante.

La siguiente proposición nos permite obtener nuevas relaciones recursivas a partir de relaciones recursivas dadas. No se pondrá la prueba en este texto, pero puede ser consultada en la proposición 3.18 de las páginas 180-181 de [1].

Proposición 4.13. *Las relaciones obtenidas de relaciones primitivas recursivas (o recursivas) a través de los conectivos del calculo proposicional y los cuantificadores acotados también so relaciones primitivas recursivas (o recursivas). Además, las aplicaciones de los μ-operadores acotados nos llevan de relaciones primitivas recursivas (o recursivas) a funciones primitivas recursivas (o recursivas).*

Lema 4.14 (La $\beta-$función de Gödel)**.** *Si $\beta : \mathbb{N}^3 \longrightarrow \mathbb{N}$ es tal que $\beta(a,b,c) = rm(1+(c+1)\cdot b, a)$, entonces β es una función primitiva recursiva y β es fuertemente representable en S por la siguiente fórmula $Bt(x_1,x_2,x_3,y)$:*

$$(\exists w)(x_1 = (\overline{1} + (x_3 + \overline{1}) \cdot x_2) \cdot w + y \ \wedge \ y < \overline{1} + (x_3 + \overline{1}) \cdot x_2).$$

Demostración. Para $x_1, x_2, x_3 \in VAR$, notemos lo siguiente:

i) Por la proposición 3.15, se cumple que
$\vdash_S y_1 \neq 0 \to (\exists y)(\exists w)[x_1 = y_1 \cdot w + y \wedge (y < y_1) \wedge (\forall w_1)(\forall y_2)((x_1 = y_1 \cdot w_1 + y_2 \wedge (y_2 < y_1)) \to w = w_1 \wedge y = y_2)]$. Usando la notación de la Definición 1.5 tenemos que
$\vdash_S y_1 \neq 0 \to (\exists_1 y)(\exists w)[x_1 = y_1 \cdot w + y \wedge (y < y_1) \wedge (\forall w_1)((x_1 = y_1 \cdot w_1 + y_2 \wedge (y_2 < y_1)) \to w = w_1]$.
Así, tenemos que $\vdash_S y_1 \neq 0 \to (\exists_1 y)(\exists w) x_1 = y_1 \cdot w + y \wedge (y < y_1)$.

ii) Por (S3') sabemos que para $t \in \mathcal{TERM}$ $\vdash_S t' \neq 0$ y por la Proposición 3.7 inciso (a) tenemos que $\vdash_S t + 1 = t'$, entonces podemos deducir que $\vdash_S t + 1 \neq 0$. Así, para $t := (x_3 + \overline{1}) \cdot x_2$, se tiene que $\vdash_S (x_3 + \overline{1}) \cdot x_2 + \overline{1} \neq 0$, es decir, $\vdash_S \overline{1} + (x_3 + \overline{1}) \cdot x_2 \neq 0$.

iii) Para $r := \overline{1} + (x_3 + \overline{1}) \cdot x_2$, por ii) tenemos que $\vdash_S r \neq 0$, además r es libre para y_1 en la fórmula $\vdash_S y_1 \neq 0 \rightarrow (\exists_1 y)(\exists w) x_1 = y_1 \cdot w + y \wedge (y < y_1)$. Entonces por la regla (A4) se cumple que $\vdash_S r \neq 0 \rightarrow (\exists_1 y)(\exists w) x_1 = r \cdot w + y \wedge (y < r)$, y usando MP tenemos que $\vdash_S (\exists_1 y)(\exists w) x_1 = r \cdot w + y \wedge (y < r)$, es decir

$$\vdash_S (\exists_1 y)(\exists w)[x_1 = (\overline{1} + (x_3 + \overline{1}) \cdot x_2) \cdot w + y \wedge (y < (\overline{1} + (x_3 + \overline{1}) \cdot x_2)].$$

De iii) concluimos que

$$\vdash_S (\exists_1 y) Bt(x_1, x_2, x_3, y)$$

Como queremos probar que $\beta(a, b, c)$ es fuertemente representable por la fórmula $Bt(x_1, x_2, x_3, y)$, entonces para $k_1, k_2, k_3, m \in \mathbb{N}$ probaremos:

1. Si $\beta(k_1, k_2, k_3) = m$ entonces $\vdash_S Bt(\overline{k_1}, \overline{k_2}, \overline{k_3}, \overline{m})$.

2. $\vdash_S (\exists_1 y) Bt(x_1, x_2, x_3, y)$

Acabamos de demostrar 2. Resta probar 1.
Supongamos que $\beta(k_1, k_2, k_3) = m$. Demostremos que $\vdash_S Bt(\overline{k_1}, \overline{k_2}, \overline{k_3}, \overline{m})$.
Como $\beta(k_1, k_2, k_3) = m$, entonces $rm(1 + (k_3 + 1) \cdot k_2, k_1) = m$, así, por el algoritmo de la división se tiene que existe un único $k \in \mathbb{N}$ tal que $k_1 = (1 + (k_3 + 1) \cdot k_2) \cdot k + m$, además $m < 1 + (k_3 + 1) \cdot k_2$.
Como $k_1 = (1 + (k_3 + 1) \cdot k_2) \cdot k + m$, entonces por la Observación 3.4 se cumple que $\vdash_S \overline{k_1} = \overline{(1 + (k_3 + 1) \cdot k_2) \cdot k + m}$. También, por la Proposición 3.8 inciso a) ii. se cumple que $\vdash_S \overline{(1 + (k_3 + 1) \cdot k_2) \cdot k + m} = (\overline{1} + (\overline{k_3} + \overline{1}) \cdot \overline{k_2}) \cdot \overline{k} + \overline{m}$. Entonces tenemos que

$$\vdash_S \overline{k_1} = (\overline{1} + (\overline{k_3} + \overline{1}) \cdot \overline{k_2}) \cdot \overline{k} + \overline{m}. \tag{4.1}$$

En los Ejemplos 1. inciso 2. vimos que la relación $<$ es expresable en S por la fórmula $\varphi(z_1, z_2) := (z_1 < z_2) := (\exists z)(z \neq 0 \ \wedge \ z + z_1 = z_2)$, así que como $m < 1 + (k_3 + 1) \cdot k_2$, entonces, $\vdash_S \overline{m} < \overline{1 + (k_3 + 1) \cdot k_2}$. También, por la Proposición 3.8 inciso a) ii. se cumple que $\vdash_S \overline{1 + (k_3 + 1) \cdot k_2} = \overline{1} + (\overline{k_3} + \overline{1}) \cdot \overline{k_2}$. Entonces tenemos que

$$\vdash_S \overline{m} < \overline{1} + (\overline{k_3} + \overline{1}) \cdot \overline{k_2}. \tag{4.2}$$

De (4.1) y (4.2) podemos concluir que

$$\vdash_S \overline{k_1} = (\overline{1} + (\overline{k_3} + \overline{1}) \cdot \overline{k_2}) \cdot \overline{k} + \overline{m} \ \wedge \ \overline{m} < \overline{1} + (\overline{k_3} + \overline{1}) \cdot \overline{k_2}$$

Ahora, si $\varphi(w) := \overline{k_1} = (\overline{1} + (\overline{k_3} + \overline{1}) \cdot \overline{k_2}) \cdot w + \overline{m} \ \wedge \ \overline{m} < \overline{1} + (\overline{k_3} + \overline{1}) \cdot \overline{k_2}$, se tiene que $\overline{m}$ es libre para w en $\varphi(w)$, entonces por la regla (E4) se cumple que

$$\varphi(\overline{m}) \vdash_S (\exists w) \varphi(w).$$

Pero $\varphi(\overline{m}) := \overline{k_1} = (\overline{1} + (\overline{k_3} + \overline{1}) \cdot \overline{k_2}) \cdot \overline{k} + \overline{m} \ \wedge \ \overline{m} < \overline{1} + (\overline{k_3} + \overline{1}) \cdot \overline{k_2}$, así que, ocupando MP concluimos que

$$\vdash_S (\exists w)(\overline{k_1} = (\overline{1} + (\overline{k_3} + \overline{1}) \cdot \overline{k_2}) \cdot w + \overline{m} \ \wedge \ \overline{m} < \overline{1} + (\overline{k_3} + \overline{1}) \cdot \overline{k_2}).$$

Es decir:

$$\vdash_S Bt(\overline{k_1}, \overline{k_2}, \overline{k_3}, \overline{m})$$

Por lo tanto, la función recursiva β es fuertemente representable en S por la fórmula Bt. ∎

Lema 4.15. *Para cualquier sucesión de números naturales $k_0, k_1, \ldots, k_n$ existen números naturales b, c tales que, para $0 \leq i \leq n$, $\beta(b, c, i) = k_i$*

Demostración. Sea $j = max(n, k_0, k_1, \ldots, k_n)$ y proponemos $c = j!$. Consideremos para $0 \leq i \leq n$ los números $u_i = 1 + (i+1) \cdot c$. Los números u_i son primos relativos dos a dos, es decir, si $l, m \in \mathbb{N}$ son tales que $0 \leq l < m \leq n$, entonces el máximo común divisor de u_l y u_m es 1. En efecto, si p es un primo tal que $p|u_l$ y $p|u_m$, entonces $p|(u_m - u_l)$. Notemos que $u_m - u_l = (1 + (m+1) \cdot c) - (1 + (l+1) \cdot c) = (m-l) \cdot c$. Entonces se cumple que $p|(m-l) \cdot c$. Ahora, se cumple que $p \nmid c$, pues si ocurriera que $p \mid c$, entonces existe $n_0 \in \mathbb{N}$ tal que $c = n_0 p$, y eso implicaría que $(l+1)c = (l+1)(n_0 p) = ((l+1)n_0)p$, es decir, $p|(1+l)c$. Pero ya sabíamos que $p|1 + (l+1) \cdot c$, así que $p \mid [(1 + (l+1) \cdot c) - ((1+l)c)]$, es decir, $p \mid 1$, lo que es una contradicción, pues p es primo, por tanto $p \nmid c$.
Como $p \mid (m-l) \cdot c$ y $p \nmid c$, entonces se tiene que $p \mid (m-l)$.
Como $0 \leq l < m \leq n$ y $j = max(n, k_0, k_1, \ldots, k_n)$,
entonces tenemos que $0 \leq m - l \leq n \leq j \leq j!$, así, $m - l \in \{0, \ldots, j\}$, es decir, $m - l$ es uno de los factores de $j!$, entonces $c = j! = (m-l)r$ donde r es el producto de los factores de $j!$ a excepción de $m - l$. Así, se tiene que $m - l \mid j!$, es decir, $m - l \mid c$.
Como $p \mid (m-l)$ entonces existe $z \in \mathbb{N}$ tal que $m - l = pz$ y como $c = (m-l)r$, tenemos que $c = (pz)r$, por tanto $p \mid c$ lo cual es una contradicción, pues teníamos que $p \nmid c$.
Por tanto $p \nmid (m-l)$, entonces se cumple que $p \nmid (m-l)c$, que es una contradicción pues sabíamos que $p \mid (m-l)c$, que viene de suponer la existencia del primo p.
Por lo tanto, los números u_i son primos relativos dos a dos.
También, para $0 \leq i \leq n$, $k_i \leq j \leq j! = c < 1 + (i+1)c = u_i$, entonces, $k_i < u_i$.
Ahora, un resultado importante para la teoría de números es el Teorema Chino del Residuo que afirma lo siguiente:

Teorema Chino del Residuo: Si $x_0, \ldots, x_s$ son primos relativos dos a dos y $y_0, \ldots, y_s \in \mathbb{N}$, entonces existe $z \in \mathbb{N}$ tal que para $0 \leq i \leq s$ se cumple que:

$$z \equiv y_i \text{ mód } x_i.$$

No es la intención demostrar este teorema en este trabajo, pero se puede consultar la prueba en la página 21 de [4].

Ahora bien, como $u_0, \ldots, u_n$ son primos relativos y $k_0, \ldots, k_n \in \mathbb{N}$, por el Teorema Chino del residuo tenemos que existe $b \in \mathbb{N}$ tal que, para $0 \leq i \leq n$ se cumple que $b \equiv k_i$ mód u_i, es decir $u_i \mid (b - k_i)$.
Como $u_i \mid (b - k_i)$, entonces existe $q \in \mathbb{N}$ tal que $b - k_i = u_i z$, entonces

$$b = u_i z + k_i \text{ con } k_i < u_i$$

Es decir, k_i es el residuo de dividir b por u_i. Así, $rm(u_i, b) = k_i$, es decir, $rm(1 + (1+i)c, b) = k_i$, pero, $rm(1 + (1+i)c, b) = \beta(b, c, i)$, por lo que $\beta(b, c, i) = k_i$, que es lo que queríamos demostrar. ∎

Proposición 4.16. *Toda función recursiva es representable en S.*

Demostración. Sea f una función recursiva, veamos que es representable en S:

I. Si f es una función inicial, en los Ejemplos 2 incisos a.-c. vimos que las funciones iniciales son fuertemente representables en S, por tanto, son representables.

II. Si f se obtiene por sustitución, en los ejemplos 2, inciso d., vimos que f es fuertemente representable en S, por tanto es representable en S.

III. Si f se obtiene por recursión, tenemos que $f : \mathbb{N}^{n+1} \longrightarrow \mathbb{N}$ tal que

$$f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n)$$

$$f(x_1,\ldots,x_n,y+1)=h(x_1,\ldots,x_n,y,f(x_1,\ldots,x_n,y)),$$

donde $g:\mathbb{N}^n\longrightarrow\mathbb{N}$, $h:\mathbb{N}^{n+2}\longrightarrow\mathbb{N}$ son funciones recursivas representables en S por las fórmulas $\mathscr{B}(x_1,\ldots,x_{n+1})$ y $\mathscr{C}(x_1,\ldots,x_{n+3})$ respectivamente.
Ahora notemos que $f(x_1,\ldots,x_n,y)=z$ si y solo si existen $b_0,\ldots,b_y\in\mathbb{N}$ tales que $b_0=g(x_1,\ldots,x_n)$ y para $1\leq w+1\leq y$, $b_{w+1}=h(x_1,\ldots,x_n,w,b_w)$ y $b_y=z$ y esto es cierto, pues podemos proponer que $b_w=f(x_1,\ldots,x_n,w)$, entonces,
$b_{w+1}=f(x_1,\ldots,x_n,w+1)=h(x_1,\ldots,x_n,w,f(x_1,\ldots,x_n,w))$, es decir,
$b_{w+1}=h(x_1,\ldots,x_n,w,b_w)$.
Veamos que $f(x_1,\ldots,x_{n+1})$ es representable en S por la siguiente fórmula $\mathscr{D}(x_1,\ldots,x_{n+2})$:

$$(\exists u)(\exists v)[((\exists w)(Bt(u,v,0,w)\ \wedge\ \mathscr{B}(x_1,\ldots,x_n,w)))\ \wedge\ Bt(u,v,x_{n+1},x_{n+2})$$
$$\wedge(\forall w)(w<x_{n+1}\Rightarrow(\exists y)(\exists z)(Bt(u,v,w,y)\ \wedge\ Bt(u,v,w',z)\ \wedge\ \mathscr{C}(x_1,\ldots,x_n,w,y,z)))].$$

Queremos demostrar que para $k_1,\ldots,k_n,p,m\in\mathbb{N}$ si $f(k_1,\ldots,k_n,p)=m$, entonces $\vdash_S\mathscr{D}(\overline{k_1},\ldots,\overline{k_n},\overline{p},\overline{m})$ y que $\vdash_S(\exists_1 x_{n+2})\mathscr{D}(\overline{k_1},\ldots,\overline{k_n},\overline{p},x_{n+2})$.

i) Supongamos que $f(k_1,\ldots,k_n,p)=m$. Demostremos que $\vdash_S\mathscr{D}(\overline{k_1},\ldots,\overline{k_n},\overline{p},\overline{m})$.
Si $p=0$, entonces como $f(k_1,\ldots,k_n,0)=g(k_1,\ldots,k_n)$, se cumple que $g(k_1,\ldots,k_n)=m$. Si consideramos la sucesión que solo consiste de $m\in\mathbb{N}$, entonces por el Lema 4.15, existen $b,c\in\mathbb{N}$ tales que $\beta(b,c,0)=m$, por el Lema 4.14, β es representable en S por la formula Bt, entonces como $\beta(b,c,0)=m$, se cumple que

$$\vdash_S Bt(\overline{b},\overline{c},\overline{0},\overline{m}).\tag{4.3}$$

También, sabemos que $g(k_1,\ldots,k_n)=m$, y como g es representable en S por $\mathscr{B}$, entonces $\vdash_S\mathscr{B}(\overline{k_1},\ldots,\overline{k_n},\overline{m})$. Así, tenemos que

$$\vdash_S Bt(\overline{b},\overline{c},\overline{0},\overline{m})\ \wedge\ \mathscr{B}(\overline{k_1},\ldots,\overline{k_n},\overline{m}).$$

Como $\overline{m}$ es un termino libre para w, por la regla (E4), tenemos que

$$\vdash_S(\exists w)(Bt(\overline{b},\overline{c},\overline{0},w)\ \wedge\ \mathscr{B}(\overline{k_1},\ldots,\overline{k_n},w)).\tag{4.4}$$

Por la Proposición 3.10 inciso (z) sabemos que
$\vdash_S w\not<0$ y también sabemos que $\vdash_S\varphi\to(\neg\varphi\to\psi)$ para $\varphi,\psi\in\mathcal{FORM}$, entonces tenemos que

$$\vdash_S w\not<0\to(w<0\to((\exists y)(\exists z)(Bt(\overline{b},\overline{c},w,y))\wedge(Bt(\overline{b},\overline{c},w',z)\wedge\mathscr{C}(\overline{k_1},\ldots,\overline{k_n},w,y,z)))).$$

Y ocupando MP se tiene que

$$\vdash_S w<0\to((\exists y)(\exists z)(Bt(\overline{b},\overline{c},w,y))\ \wedge\ (Bt(\overline{b},\overline{c},w',z)\ \wedge\ \mathscr{C}(\overline{k_1},\ldots,\overline{k_n},w,y,z)))$$

Si aplicamos gen tenemos que

$$\vdash_S(\forall w)(w<0\to((\exists y)(\exists z)(Bt(\overline{b},\overline{c},w,y))\ \wedge\ (Bt(\overline{b},\overline{c},w',z)\ \wedge\ \mathscr{C}(\overline{k_1},\ldots,\overline{k_n},w,y,z)))).\tag{4.5}$$

Los términos $\overline{b}$, y $\overline{c}$ son libres para las variables u,v en todas las fórmulas de las ecuaciones (4.3), (4.4) y (4.5); así, si ocupamos la regla de conjunción y la regla (E4) en dichas ecuaciones obtenemos que

$$\vdash_S\mathscr{D}(\overline{k_1},\ldots,\overline{k_n},0,\overline{m}).$$

Ahora, si $p>0$, como f se obtiene por la regla de recursión, se tiene que $f(k_1,\ldots,k_n,p)$ se calcula en un total de $p+1$ pasos.

Sea $r_i = f(k_1, \ldots, k_n, i)$ para $0 \leq i \leq p$, ahora, por el Lema 4.15, para la sucesión de números naturales $r_0, \ldots, r_p \in \mathbb{N}$ existen $b, c \in \mathbb{N}$ tales que para $0 \leq i \leq p$, $\beta(b, c, i) = r_i$. También por el Lema 4.14 se cumple que como $\beta(b, c, i) = r_i$, entonces $\vdash_S Bt(\overline{b}, \overline{c}, \overline{i}, \overline{r_i})$ para $0 \leq i \leq p$. Así, se cumple que como $\beta(b, c, 0) = r_0$, entonces $\vdash_S Bt(\overline{b}, \overline{c}, 0, \overline{r_0})$. También como $r_0 = f(k_1, \ldots, k_n, 0) = g(k_1, \ldots, k_n)$ y como g es representable por $\mathscr{B}$, entonces $\vdash_S \mathscr{B}(\overline{k_1}, \ldots, \overline{k_n}, \overline{r_0})$; si usamos la regla de conjunción, tenemos que

$$\vdash_S Bt(\overline{b}, \overline{c}, 0, \overline{r_0}) \ \wedge \ \mathscr{B}(\overline{k_1}, \ldots, \overline{k_n}, \overline{r_0}). \tag{4.6}$$

Como $\overline{r_0}$ es un término libre para la variable w en la fórmula (4.6), entonces por la regla (E4) se cumple que

$$\vdash_S (\exists w)(Bt(\overline{b}, \overline{c}, 0, w) \ \wedge \ \mathscr{B}(\overline{k_1}, \ldots, \overline{k_n}, w)). \tag{4.7}$$

Sabemos que $r_p = f(k_1, \ldots, k_n, p) = m$ y que $\beta(b, c, p) = r_p$, entonces $\beta(b, c, p) = m$, y por el Lema 4.14 se tiene que

$$\vdash_S Bt(\overline{b}, \overline{c}, \overline{p}, \overline{m}) \tag{4.8}$$

Sabemos que para $0 \leq i \leq p-1$, $\beta(b, c, i) = r_i = f(k_1, \ldots, k_n, i)$, entonces $\vdash_S Bt(\overline{b}, \overline{c}, \overline{i}, \overline{r_i})$. Ahora, por como definimos f, se tiene que
$\beta(b, c, i+1) = r_{i+1} = f(k_1, \ldots, k_n, i+1) = h(k_1, \ldots, k_n, i, f(k_1, \ldots, k_n, i))$
$= h(k_1, \ldots, k_n, i, r_i)$. Es decir
$r_{i+1} = h(k_1, \ldots, k_n, i, r_i)$ y como h es representable por $\mathscr{C}$, se cumple que
$\vdash_S \mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, \overline{i}, \overline{r_i}, \overline{r_{i+1}})$. También, como $\beta(b, c, i+1) = r_{i+1}$ y β representable por Bt, entonces $\vdash_S Bt(\overline{b}, \overline{c}, \overline{i+1}, \overline{r_{i+1}})$, es decir, $\vdash_S Bt(\overline{b}, \overline{c}, \overline{i}', \overline{r_{i+1}})$
Si ocupamos la regla de conjunción, obtenemos que

$$\vdash_S Bt(\overline{b}, \overline{c}, \overline{i}, \overline{r_i}) \ \wedge \ Bt(\overline{b}, \overline{c}, \overline{i}', \overline{r_{i+1}}) \ \wedge \ \mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, \overline{i}, \overline{r_i}, \overline{r_{i+1}}).$$

Ahora, los términos $\overline{r_i}$ y $\overline{r_{i+1}}$ son libres para las variables y, z respectivamente en la fórmula anterior, entonces por la regla (E4) se cumple que

$$\vdash_S (\exists y)(\exists z)(Bt(\overline{b}, \overline{c}, \overline{i}, y) \ \wedge \ Bt(\overline{b}, \overline{c}, \overline{i}', z) \ \wedge \ \mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, \overline{i}, y, z))$$

donde $0 \leq i \leq p-1$. Si denotamos como
$\varphi(\overline{i}) := (\exists y)(\exists z)(Bt(\overline{b}, \overline{c}, \overline{i}, y) \ \wedge \ Bt(\overline{b}, \overline{c}, \overline{i}', z) \ \wedge \ \mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, \overline{i}, y, z))$, entonces tenemos que $\vdash_S \varphi(\overline{i})$ para $0 \leq i \leq p-1$, ocupando la regla de conjunción tenemos que
$\vdash_S \varphi(0) \ \wedge \ldots \ \wedge \ \varphi(\overline{p-1})$. Por la Proposición 3.11 inciso b$'$) se cumple que

$$\vdash_S \varphi(0) \ \wedge \ldots \ \wedge \ \varphi(\overline{p-1}) \rightarrow (\forall w)(w < \overline{p} \rightarrow \varphi(w))$$

Ocupando MP tenemos que

$$\vdash_S (\forall w)(w < \overline{p} \rightarrow \varphi(w)).$$

Es decir

$$\vdash_S (\forall w)(w < \overline{p} \rightarrow (\exists y)(\exists z)(Bt(\overline{b}, \overline{c}, w, y) \wedge Bt(\overline{b}, \overline{c}, w', z) \wedge \mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, w, y, z))) \tag{4.9}$$

Los términos $\overline{b}$, y $\overline{c}$ son libres para las variables u, v en todas las fórmulas de las ecuaciones (4.7), (4.8) y (4.9), así si ocupamos la regla de conjunción y la regla (E4) en dichas ecuaciones obtenemos que

$$\vdash_S \mathscr{D}(\overline{k_1}, \ldots, \overline{k_n}, \overline{p}, \overline{m})$$

Por lo tanto, hemos probado que si $f(k_1, \ldots, k_n, p) = m$, entonces $\vdash_S \mathscr{D}(\overline{k_1}, \ldots, \overline{k_n}, \overline{p}, \overline{m})$

ii) Nos resta probar que $\vdash_S (\exists_1 x_{n+2})\mathscr{D}(\overline{k_1},\ldots,\overline{k_n},\overline{p},x_{n+2})$. Notemos que, por el desarrollo que hicimos en i), solo resta probar la unicidad
Hagamos la prueba por inducción sobre $p \in \mathbb{N}$.

Para $p = 0$. Tenemos que $f(x_1,\ldots,x_n,0) = g(x_1,\ldots,x_n)$. Digamos que $g(x_1,\ldots,x_n) = m$. En i) habíamos visto que $\vdash_S \mathscr{D}(\overline{k}_1,\ldots,\overline{k}_n,0,\overline{m})$. Supongamos que $\vdash_S \mathscr{D}(\overline{k}_1,\ldots,\overline{k}_n,0,x_{n+2})$. Demostremos que $\vdash_S x_{n+2} = \overline{m}$.
Como $\vdash_S \mathscr{D}(\overline{k}_1,\ldots,\overline{k}_n,0,\overline{m})$, entonces se cumple que

$$\begin{aligned}&\vdash_S (\exists u)(\exists v)[((\exists w)(Bt(u,v,0,w)\ \wedge\ \mathscr{B}(\overline{k}_1,\ldots,\overline{k}_n,w)))\ \wedge\ Bt(u,v,0,\overline{m})\\ &\wedge(\forall w)(w<0 \Rightarrow (\exists y)(\exists z)(Bt(u,v,w,y)\ \wedge\ Bt(u,v,w',z)\ \wedge\ \mathscr{C}(\overline{k}_1,\ldots,\overline{k}_n,w,y,z)))].\end{aligned}$$

Ocupando la regla C para las constantes b_1, c_1 y d_1 tenemos que
$\vdash_S (Bt(b_1,c_1,0,d_1)\ \wedge\ \mathscr{B}(\overline{k}_1,\ldots,\overline{k}_n,d_1))\ \wedge\ Bt(b_1,c_1,0,\overline{m})$. Así, tenemos que

$$\vdash_S Bt(b_1,c_1,0,d_1), \vdash_S \mathscr{B}(\overline{k}_1,\ldots,\overline{k}_n,d_1) \text{ y } \vdash_S Bt(b_1,c_1,0,\overline{m}).$$

Sabemos que la función β de Gödel es fuertemente representable en S por la fórmula Bt, entonces se cumple que $\vdash_S (\exists_1 x_4)Bt(x_1,x_2,x_3,x_4)$, donde $x_1,x_2,x_3 \in VAR$. Si aplicamos Gen 3 veces tenemos que

$$\vdash_S (\forall x_1)(\forall x_2)(\forall x_3)(\exists_1 x_4)Bt(x_1,x_2,x_3,x_4).$$

Ahora bien, b_1, c_1 y 0 son términos libres para x_1,x_2,x_3 respectivamente en la fórmula $(\exists_1 x_4)Bt(x_1,x_2,x_3,x_4)$, entonces, si aplicamos la regla de particularización (A4) y MP 3 veces tenemos que

$$\vdash_S (\exists_1 x_4)Bt(b_1,c_1,0,x_4). \tag{1}$$

Como sabíamos que $\vdash_S Bt(b_1,c_1,0,d_1)$ y que $\vdash_S Bt(b_1,c_1,0,\overline{m})$, entonces por (1) se cumple que $\vdash_S d_1 = \overline{m}$.

Como $\vdash_S \mathscr{D}(\overline{k}_1,\ldots,\overline{k}_n,0,x_{n+2})$, entonces se cumple que

$$\begin{aligned}&\vdash_S (\exists u)(\exists v)[((\exists w)(Bt(u,v,0,w)\ \wedge\ \mathscr{B}(\overline{k}_1,\ldots,\overline{k}_n,w)))\ \wedge\ Bt(u,v,0,x_{n+2})\\ &\wedge(\forall w)(w<0 \Rightarrow (\exists y)(\exists z)(Bt(u,v,w,y)\ \wedge\ Bt(u,v,w',z)\ \wedge\ \mathscr{C}(\overline{k}_1,\ldots,\overline{k}_n,w,y,z)))].\end{aligned}$$

Ocupando la regla C para las constantes b_2, c_2 y d_2 tenemos que
$\vdash_S (Bt(b_2,c_2,0,d_2)\ \wedge\ \mathscr{B}(\overline{k}_1,\ldots,\overline{k}_n,d_2))\ \wedge\ Bt(b_2,c_2,0,x_{n+2})$. Así, tenemos que

$$\vdash_S Bt(b_2,c_2,0,d_2), \vdash_S \mathscr{B}(\overline{k}_1,\ldots,\overline{k}_n,d_2) \text{ y } \vdash_S Bt(b_2,c_2,0,x_{n+2}).$$

De manera analoga a lo que hicimos con b_1, c_1 y 0 se cumple que

$$\vdash_S (\exists_1 x_4)Bt(b_2,c_2,0,x_4). \tag{2}$$

Como sabíamos que $\vdash_S Bt(b_2,c_2,0,d_2)$ y que $\vdash_S Bt(b_2,c_2,0,x_{n+2})$, entonces por (2) se cumple que $\vdash_S d_2 = x_{n+2}$.

Ahora, sabemos que g es representable en S por la fórmula $\mathscr{B}$, entonces se cumple que $\vdash_S (\exists_1 x_{n+1})\mathscr{B}(\overline{k}_1,\ldots,\overline{k}_n,x_{n+1})$ y como $\vdash_S \mathscr{B}(\overline{k}_1,\ldots,\overline{k}_n,d_1)$ y que $\vdash_S \mathscr{B}(\overline{k}_1,\ldots,\overline{k}_n,d_2)$ entonces se cumple que $\vdash_S d_1 = d_2$

Por último, como $\vdash_S d_1 = \overline{m}$, $\vdash_S d_2 = x_{n+2}$ y $\vdash_S d_1 = d_2$, podemos concluir que

$$\vdash_S \overline{m} = x_{n+2}.$$

Por lo tanto

$$\vdash_S (\exists_1 x_{n+2})\mathscr{D}(\overline{k}_1, \ldots, \overline{k}_n, 0, x_{n+2}).$$

Ahora supongamos que para $p \in \mathbb{N} \vdash_S (\exists_1 x_{n+2})\mathscr{D}(\overline{k_1}, \ldots, \overline{k_n}, \overline{p}, x_{n+2})$,
Veamos que $\vdash_S (\exists_1 x_{n+2})\mathscr{D}(\overline{k_1}, \ldots, \overline{k_n}, \overline{p+1}, x_{n+2})$.
Sea $g(k_1, \ldots, k_n) = \alpha$, $f(k_1, \ldots, k_n, p) = \beta$ y $f(k_1, \ldots, k_n, p+1) = \gamma = h(k_1, \ldots, k_n, p, \beta)$.
Notemos que se cumple que:

1. $\vdash_S \mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, \overline{p}, \overline{\beta}, \overline{\gamma})$ [Pues $h(k_1, \ldots, k_n, p, \beta) = \gamma$ y $\mathscr{C}$ representa a h]
2. $\vdash_S \mathscr{B}(\overline{k_1}, \ldots, \overline{k_n}, \overline{\alpha})$ [Pues $g(k_1, \ldots, k_n) = \alpha$ y $\mathscr{B}$ representa a g]
3. $\vdash_S \mathscr{D}(\overline{k_1}, \ldots, \overline{k_n}, \overline{p}, \overline{\beta})$ [Igual al desarrollo en i) pues $f(k_1, \ldots, k_n, p) = \beta$]
4. $\vdash_S \mathscr{D}(\overline{k_1}, \ldots, \overline{k_n}, \overline{p+1}, \overline{\gamma})$ [Igual a i) pues $f(k_1, \ldots, k_n, p+1) = \gamma$]
5. $\vdash_S (\exists_1 x_{n+2})\mathscr{D}(\overline{k_1}, \ldots, \overline{k_n}, \overline{p}, x_{n+2})$ [Hipótesis inductiva]

Supongamos que

6. $\mathscr{D}(\overline{k_1}, \ldots, \overline{k_n}, \overline{p+1}, x_{n+2})$

Demostremos que $\overline{\gamma} = x_{n+2}$

Como $\mathscr{D}(\overline{k_1}, \ldots, \overline{k_n}, \overline{p+1}, x_{n+2})$, ocupando la regla C con las constantes b y c se tiene que:

a. $(\exists w)(Bt(b, c, 0, w) \ \wedge \ \mathscr{B}(\overline{k_1}, \ldots, \overline{k_n}))$
b. $Bt(b, c, \overline{p+1}, x_{n+2})$
c. $(\forall w)(w < \overline{p+1} \rightarrow (\exists y)(\exists z)(Bt(b, c, w, y) \ \wedge \ Bt(b, c, w', z) \ \wedge \ \mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, w, y, z)))$

Ahora, si denotamos $\varphi(w) := (\exists y)(\exists z)(Bt(b, c, w, y) \wedge Bt(b, c, w', z) \wedge \mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, w, y, z))$, entonces, tenemos que $\vdash_S (\forall w)(w < \overline{p+1} \rightarrow \varphi(w))$. Por la Proposición 3.11 inciso b$'$) y MP obtenemos que $\vdash_S \varphi(0) \wedge \ldots \wedge \varphi(\overline{p-1}) \wedge \varphi(\overline{p})$, entonces, $\vdash_S \varphi(0) \wedge \ldots \wedge \varphi(\overline{p-1})$, y nuevamente por la Proposición 3.11 inciso b$'$) y MP obtenemos que $\vdash_S (\forall w)(w < \overline{p} \rightarrow \varphi(w))$, es decir,

d. $(\forall w)(w < \overline{p} \rightarrow (\exists y)(\exists z)(Bt(b, c, w, y) \ \wedge \ Bt(b, c, w', z) \ \wedge \ \mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, w, y, z)))$

Ahora, $\overline{p}$ es un término libre para w en la fórmula $\psi := (w < \overline{p+1} \rightarrow \varphi(w))$, entonces por la regla (A4) se tiene que
$\vdash_S \overline{p} < \overline{p+1} \rightarrow (\exists y)(\exists z)(Bt(b, c, \overline{p}, y) \ \wedge \ Bt(b, c, \overline{p}', z) \ \wedge \ \mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, w, y, z))$. Sabemos que $\vdash_S \overline{p} < \overline{p+1}$, entonces por MP
$\vdash_S (\exists y)(\exists z)(Bt(b, c, \overline{p}, y) \ \wedge \ Bt(b, c, \overline{p}', z) \ \wedge \ \mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, \overline{p}, y, z))$. También, sabemos que $\vdash_S \overline{p}' = \overline{p+1}$, así que, ocupando (A7$'$) y MP se tiene que
$\vdash_S (\exists y)(\exists z)(Bt(b, c, \overline{p}, y) \ \wedge \ Bt(b, c, \overline{p+1}, z) \ \wedge \ \mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, \overline{p}, y, z))$. Ocupando la regla C con las constantes d y e tenemos que:

e. $Bt(b, c, \overline{p}, d) \ \wedge \ Bt(b, c, \overline{p+1}, e) \ \wedge \ \mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, \overline{p}, d, e)$.

Ahora, b y c son términos libres para u y v respectivamente en las fórmulas $(a.), (d.)$ y $Bt(b, c, \overline{p}, d)$, entonces, b y c son libres para u y v en la fórmula

$\psi_1 := (a.) \wedge Bt(b,c,\overline{p},d) \wedge (d.)$, entonces por la regla (E4) y MP tenemos que $\vdash_S (\exists u)(\exists v)[((\exists w)(Bt(u,v,0,w) \ \wedge \ \mathscr{B}(\overline{k_1},\ldots,\overline{k_n},w))) \ \wedge \ Bt(u,v,\overline{p},d)$ $\wedge \ (\forall w)(w < \overline{p} \rightarrow (\exists y)(\exists z)(Bt(u,v,w,y) \ \wedge \ Bt(u,v,w',z) \ \wedge \ \mathscr{C}(\overline{k_1},\ldots,\overline{k_n},w,y,z)))]$, es decir,

f. $\mathscr{D}(\overline{k_1},\ldots,\overline{k_n},\overline{p},d)$.

Ahora, por *f.*, 5. y 3. se tiene que

g.	$d = \overline{\beta}$	
h.	$\mathscr{C}(\overline{k_1},\ldots,\overline{k_n},\overline{p},\overline{\beta},e)$	[Pues de *e.* y *h.* utilizamos (A7′) y MP]
i.	$\overline{\gamma} = e$	[Pues $\mathscr{C}$ representa a h y $\vdash_S (h.) \vdash_S (1.)$]
j.	$Bt(b,c,\overline{p+1},\overline{\gamma})$	[Pues de *i.* y *e.* utilizamos (A7′) y MP]

Por el Lema 4.14 la función β de Gödel es fuertemente representable por la fórmula Bt, así que,$\vdash_S (\exists_1 x_{n+2})By(x_1,x_2,x_3,x_{n+2})$. Si ocupamos Gen 3 veces para las variables x_1, x_2 y x_3 y ocupamos la regla (A4) se tiene que $\vdash_S (\exists_1 x_{n+2})Bt(b,c,\overline{p+1},x_{n+2})$. Como por *j.* tenemos que $\vdash_S Bt(b,c,\overline{p+1},\overline{\gamma})$ y por *b.* tenemos que $\vdash_S Bt(b,c,\overline{p+1},x_{n+2})$, así que

$$\vdash_S x_{n+2} = \overline{\gamma}$$

Por lo tanto

$$\vdash_S (\exists_1 x_{n+2})\mathscr{D}(\overline{k_1},\ldots,\overline{k_n},\overline{p+1},x_{n+2}).$$

IV. Si f se obtiene a través del $\mu-$operador:
Supongamos que para $x_1,\ldots,x_n \in \mathbb{N}$ existe $y \in \mathbb{N}$ tal que $g(x_1,\ldots,x_n,y) = 0$ y supongamos que g es representable en S por la fórmula $\mathscr{E}(x_1,\ldots,x_{n+2})$ y supongamos que

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

Veamos que f es representable en S por la fórmula $\mathscr{F}(x_1,\ldots,x_{n+1})$:

$$\mathscr{E}(x_1,\ldots,x_{n+1},0) \ \wedge \ (\forall y)(y < x_{n+1} \rightarrow \neg\mathscr{E}(x_1,\ldots,x_n,y,0)).$$

Sean $k_1,\ldots,k_n,m \in \mathbb{N}$.

i. Supongamos que $f(k_1,\ldots,k_n) = m$, veamos que $\mathscr{F}(\overline{k_1},\ldots,k_n,\overline{m})$.
Como $f(k_1,\ldots,k_n) = \mu y(g(k_1,\ldots,k_n,y) = 0)$, entonces se cumple que $g(k_1,\ldots,k_n,m) = 0$ y para $k \in \mathbb{N}$ tal que $k < n$, $g(k_1,\ldots,k_n,k) \neq 0$.
Como $g(k_1,\ldots,k_n,m) = 0$ y $\mathscr{E}$ representa a g, entonces $\vdash_S \mathscr{E}(\overline{k_1},\ldots,\overline{k_n},\overline{m},0)$.
Notemos que si $k < m$, entonces $\vdash_S \neg\mathscr{E}(\overline{k_1},\ldots,\overline{k_n},\overline{k},0)$, pues como $k < m$, entonces $g(k_1,\ldots,k_n,k) = z \neq 0$. Si ocurriera que $\vdash_S \mathscr{E}(\overline{k_1},\ldots,\overline{k_n},\overline{k},0)$, se tiene que $\vdash_S \mathscr{E}(\overline{k_1},\ldots,\overline{k_n},\overline{k},\overline{z})$ y como $\vdash_S (\exists_1 x_{n+2})\mathscr{E}(\overline{k_1},\ldots,\overline{k_n},\overline{k},x_{n+2})$, entonces se cumple que $\vdash_S \overline{z} = 0$, y así, se cumpliría que $z = 0$, lo cual es una contradicción, por lo que, para $k < n$, $\vdash_S \neg\mathscr{E}(\overline{k_1},\ldots,\overline{k_n},\overline{k},0)$, es decir,

$$\vdash_S \neg\mathscr{E}(\overline{k_1},\ldots,\overline{k_n},0,0) \wedge \ldots \wedge \neg\mathscr{E}(\overline{k_1},\ldots,\overline{k_n},\overline{m-1},0)$$

Así que, por la Proposición 3.11 inciso $b')$ y MP se cumple que

$$\vdash_S (\forall y)(y < \overline{m} \rightarrow \neg\mathscr{E}(\overline{k_1},\ldots,\overline{k_n},y,0))$$

Así, hemos probado que

$$\vdash_S \mathscr{E}(\overline{k_1},\ldots,\overline{k_n},\overline{m},0) \ \wedge \ (\forall y)(y < \overline{m} \rightarrow \neg\mathscr{E}(\overline{k_1},\ldots,\overline{k_n},y,0))$$

Es decir:

$$\vdash_S \mathscr{F}(\overline{k_1}, \dots, \overline{k_n}, \overline{m})$$

ii. Demostremos que $(\exists_1 x_{n+1})\mathscr{F}(\overline{k_1}, \dots, \overline{k_n}, x_{n+1})$.
En i. ya vimos que $\vdash_S \mathscr{F}(\overline{k_1}, \dots, \overline{k_n}, \overline{m})$, así que nos resta probar la unicidad.
Supongamos que para $u \in VAR \vdash_S \mathscr{F}(\overline{k_1}, \dots, \overline{k_n}, u)$, es decir,
$\vdash_S \mathscr{E}(\overline{k_1}, \dots, \overline{k_n}, u, 0) \ \wedge \ (\forall y)(y < u \to \neg\mathscr{E}(\overline{k_1}, \dots, \overline{k_n}, y, 0))$.
Sabemos que $\vdash_S \overline{m} < u \ \vee u < \overline{m} \ \vee \ \overline{m} = u$.
Si ocurriera que $\vdash_S \overline{m} < u$, como $\vdash_S (\forall y)(y < u \to \neg\mathscr{E}(\overline{k_1}, \dots, \overline{k_n}, y, 0))$ y $\overline{m}$ es un término libre para y en la fórmula $\psi := y < u \to \neg\mathscr{E}(\overline{k_1}, \dots, \overline{k_n}, y, 0)$, entonces por MP y la regla (A4) se tiene que $\vdash_S \overline{m} < u \to \neg\mathscr{E}(\overline{k_1}, \dots, \overline{k_n}, \overline{m}, 0)$. Como $\vdash_S \overline{m} < u$, entonces por MP se tiene que $\vdash_S \neg\mathscr{E}(\overline{k_1}, \dots, \overline{k_n}, \overline{m}, 0)$, pero sabíamos que $\vdash_S \mathscr{E}(\overline{k_1}, \dots, \overline{k_n}, \overline{m}, 0)$, por lo que $\vdash_S \overline{m} \not< u$.
Si ocurriera que $\vdash_S u < \overline{m}$, como $\vdash_S \mathscr{F}(\overline{k_1}, \dots, \overline{k_n}, \overline{m})$, entonces
$\vdash_S (\forall y)((y < \overline{m} \to \neg\mathscr{E}(\overline{k_1}, \dots, \overline{k_n}, \overline{m}, 0)))$. Ahora, u es un término libre para la variable y en la fórmula $\psi := y < \overline{m} \to \neg\mathscr{E}(\overline{k_1}, \dots, \overline{k_n}, \overline{m}, 0)$, entonces por (A4) y MP se cumple que $\vdash_S u < \overline{m} \to \neg\mathscr{E}(\overline{k_1}, \dots, \overline{k_n}, \overline{m}, 0)$, y de nuevo por MP, $\vdash_S \neg\mathscr{E}(\overline{k_1}, \dots, \overline{k_n}, \overline{m}, 0)$, lo cual es una contradicción, por lo que $\vdash_S u \not< \overline{m}$.
Así, se tiene que $\vdash_S \overline{m} \not< u \ \wedge \ u \not< \overline{m}$, es decir, $\vdash_S \neg(\overline{m} < u \ \vee \ u < \overline{m})$.
Recordando que para $\alpha, \gamma \in \mathcal{FORM}$ se tiene que $\vdash_S \gamma \vee \alpha \to (\neg\alpha \to \gamma)$ y como
$\vdash_S \overline{m} < u \ \vee u < \overline{m} \ \vee \ \overline{m} = u$, ocupando lo anterior y MP concluimos que $\vdash_S \overline{m} = u$.
Así, hemos probado que

$$(\exists_1 x_{n+1})\mathscr{F}(\overline{k_1}, \dots, \overline{k_n}, x_{n+1}).$$

Así, f es representable en S por $\mathscr{F}$ cuando f se obtiene a través del $\mu-$operador.

Por lo tanto, de I., II., III. y IV., concluimos que toda función recursiva es representable en S. ■

Corolario 3. *Toda relación recursiva es expresable en S.*

Demostración. Sea $R \subseteq \mathbb{N}^n$ una relación recursiva, entonces su función característica C_R es una función recursiva, entonces por la Proposición 4.16 se cumple que C_R es representable en S, así que, por la proposición 4.7 se cumple que R es expresable en S. ■

Capítulo 5

Teoremas de incompletitud de Gödel

5.1. Números de Gödel

Hasta ahora hemos visto que S es lo suficientemente fuerte para construir interpretaciones en donde la aritmética de los números naturales sea válida; más aún hemos visto que una amplia cantidad de funciones número-teóricas tienen representación en S. Nuestro objetivo en este capítulo será ver que no hay manera de probar la completitud de S siempre que asumamos su consistencia.
El proceso que Gödel utilizó para mostrar la incompletitud de S ha sido utilizado en distintos procedimientos tanto de la lógica como de distintas áreas matemáticas. De manera resumida, Gödel buscaba poder trasladar información sobre el lenguaje $\mathscr{L}$ a una forma numérica particular con el objetivo de que fuera más fácil de asimilar. Es decir, que a cada símbolo, término, fórmula y sucesiones de símbolos en $\mathscr{L}$ se les asignara un número en específico, a los que llamamos los números de Gödel. Con esta idea en mente, seremos capaces de probar la incompletitud de S.

Definición 5.1. Para una teoría de primer orden K, relacionamos cada símbolo u de K con un número natural $g_1(u)$ al que llamaremos número de Gödel de u, de la siguiente manera:

a) $g_1(()=3,\ g_1())=5,\ g_1(,)=7,\ g_1(\neg)=9,\ g_1(\rightarrow)=11,\ g_1(\forall)=13.$

b) Para cada $x_k \in VAR$, $g_1(x_k)=13+8k$, donde $k \geq 1$.

c) Para cada $a_k \in C$, $g_1(a_k)=7+8k$, donde $k \geq 1$.

d) Para cada símbolo funcional de aridad n f_k^n, $g_1(f_k^n)=1+8(2^n3^k)$, donde $n,k \geq 1$.

e) Para cada símbolo predicativo de aridad n A_k^n, $g_1(A_k^n)=3+8(2^n3^k)$, donde $n,k \geq 1$.

Observación 5.1. Notemos que para $x_k \in VAR$, $g_1(x_k)=13+8k=2(4k+6)+1$, para $a_k \in C$, $g_1(a_k)=7+8k=2(4k+3)+1$, para el símbolo funcional f_k^n, $g_1(f_k^n)=1+8(2^n3^k)=2(4)(2^n3^k)+1$ y para el símbolo predicativo A_k^n, $g_1(A_k^n)=3+8(2^n3^k)=2((4)(2^n3^k)+1)+1$. Así que, cada símbolo de K es un número impar.
También cuando dividimos por 8, $g_1(u)$ deja un residuo de 5 si u es una variable, un residuo de 7 si u es una constante, un residuo de 1 si u es un símbolo funcional y un residuo de 3 si u es un símbolo predicativo, así que, a símbolos distintos, se les asignan números de Gödel distintos.

Ejemplos 6. a. $g_1(x_2)=13+8(2)=29$.

b. El número 1944 no es el número de Gödel de algún símbolo, pues $2 \mid 1944$, es decir, 1944 no es impar.

c. ¿49 es el número de Gödel de algún símbolo?.
Notemos que $49=8(6)+1=8(2^13^1)+1$. Por lo tanto 49 es el número de Gödel del símbolo f_1^1.

Definición 5.2. Para una teoría de primer orden K, y una expresión $u_0u_1 \dots u_r$ donde para $0 \leq j \leq r$ u_j es un símbolo de K, definimos el número de Gödel $g_2(u_0u_1 \dots u_r)$ con la ecuación:

$$g_2(u_0u_1 \dots u_r) = 2^{g_1(u_0)}3^{g_1(u_1)} \dots p_r^{g_1(u_r)},$$

donde para $0 \leq j \leq r$ u_j, p_j es el j-ésimo número primo y $p_0 = 2$, y $g_1(u_j)$ es el número de Gödel de u_j como símbolo.

Ejemplo 8. Si K es una teoría de primer orden K con el símbolo predicativo A_1^2, entonces el número de Gödel de la expresión $A_1^2(x_1, x_2)$ es:

$$\begin{aligned} g_2(A_1^2(x_1, x_2)) &= 2^{g_1(A_1^2)}3^{g_1(()}5^{g_1(x_1)}7^{g_1(,)}11^{g_1(x_2)}13^{g_1())} \\ &= 2^{99}3^3 5^{21}7^7 11^{29}13^5 \end{aligned}$$

Observación 5.2. Los números de Gödel de una expresión son naturales expresados con factorizaciones de productos de números primos, así que, dadas expresiones distintas de una teoría K, su número de Gödel como expresión será distinto.
También, las expresiones en K tienen distintos números de Gödel que los símbolos, pues el número de Gödel de un símbolo siempre es un número impar, mientras que el número de Gödel de una expresión siempre es un número par, ya que es un producto de una potencia 2^m con $m \neq 0$.

Observación 5.3. Si consideramos a un solo símbolo u_0 como expresión, tendrá distinto número de Gödel como expresión y como símbolo.

Ejemplo 9. Si consideramos la variable x_1, su número de Gödel como símbolo es $g(x_1) = 13 + 8(1) = 21$ y como expresión, su número de Gödel es $g(x_1) = 2^{g(x_1)} = 2^{21}$.

Definición 5.3. Dada una teoría de primer orden K, si $e_0, e_1, \dots e_r$ es una sucesión finita de expresiones de K, definimos el número de Gödel $g_3(e_0, \dots, e_r)$ de la sucesión con la siguiente ecuación:

$$g_3(e_0, \dots, e_r) = 2^{g_2(e_0)}3^{g_2(e_1)} \dots p_r^{g_2(e_r)},$$

donde para $0 \leq j \leq r$, $g_2(e_j)$ es el número de Gödel de la expresión e_j.

Observación 5.4. Dos sucesiones de expresiones de K diferentes tienen número de Gödel distinto, pues su número de Gödel es una descomposición de un natural en un producto de números primos.
Tambíen como el número de Gödel de una sucesión es un número par y el número de Gödel de un símbolo es impar, entonces las sucesiones tienen diferente número de Gödel que los símbolos en K.
Además, para una sucesión, el exponente $g_2(e_0)$ del 2 en su factorizacion de productos de números primos es un número par, por lo que las sucesiones tienen diferente número de Gödel que las expresiones en K pues el exponente $g_1(u_0)$ del 2 en la factorización de producto de números primos es un número impar.

Definición 5.4. Para una teoría de primer orden K, definimos la función número de Gödel g, del conjunto $\mathscr{S}$ de símbolos de K, expresiones de K y sucesiones finitas de expresiones de K a $\mathbb{N}$ de la siguiente manera: $g : \mathscr{S} \longrightarrow \mathbb{N}$ tal que :

$$g(A) = \begin{cases} g_1(A) & \text{si } A \text{ es un símbolo de } K \\ g_2(A) & \text{si } A \text{ es una expresión de } K \\ g_3(A) & \text{si } A \text{ es una sucesión finita de expresiones de } K \end{cases}$$

Observación 5.5. Por el desarrollo que hicimos en las observaciones 5.1, 5.2 y 5.4, tenemos que g es una función inyectiva.

A este proceso de construir la función g se le conoce como aritmetización, pues a cualquier teoría de primer orden y a su conjunto $\mathscr{S}$, la función g nos permite reemplazar cualquier tipo de afirmación dentro de la teoría por enunciados numéricos equivalentes. Este fue el método que ideó Gödel en 1930 para poder demostrar la incompletitud de S.

Definición 5.5. Decimos que una teoría K es una teoría con vocabulario primitivo recursivo (o vocabulario recursivo) si las siguientes propiedades son primitivas recursivas (o recursivas):

a. $IC(x)$: x es el número de Gödel de una constante de K.

b. $FL(x)$: x es el número de Gödel de una letra funcional de K.

c. $PL(x)$: x es el número de Gödel de un símbolo predicativo de K.

Observación 5.6. Si una teoría K tiene un número finito de constantes, de letras funcionales y de símbolos predicativos, entonces K tiene un vocabulario primitivo recursivo. En efecto, digamos que K tiene a las constantes $a_{j_1}, \ldots, a_{j_n}$.Ahora, $x \in IC(x)$ si y solo si x es el número de Gödel de alguna constante a_{j_i}, eso si y solo si $x = 7 + 8j_1 \ \vee \ldots \vee x = 7 + 8j_n$. Podemos definir la función característica $C_{IC(x)}$ de la siguiente manera:

$$C_{IC(x)}(x) = sg(|x - (7 + 8j_i)|)$$

Así, $C_{IC(x)}$ es recursiva, y por tanto $IC(x)$ es primitiva recursiva.
De manera análoga $FL(x)$ y $PL(x)$ son primitivas recursivas, y por tanto, K tiene un vocabulario primitivo recursivo.
Como consecuencia de esto como S tiene a la constante 0, las letras funcionales f_1^1, f_1^2 y f_2^2 y el símbolo predicativo A_1^2, entonces se cumple que S tiene un vocabulario recursivo primitivo.

A continuación enunciaremos una lista de relaciones y funciones número-teóricas que son recursivas en teorías con ciertas condiciones, además S cumple dichas condiciones, por lo que estas funciones y relaciones son recursivas en S. No se pondrá la prueba en este texto, pero puede ser consultada en las páginas 194-199 de [1].

Proposición 5.6. *Sea K una teoría con un vocabulario primitivo recursivo (o recursivo). Entonces, las siguientes relaciones y funciones son primitivas recursivas (o recursivas):*

1. i. *$EVbl(x)$: x es el número de Gödel de una expresión que consiste de una variable.*
   ii. *$EIC(x)$: x es el número de Gödel de una expresión que consiste de una constante.*
   iii. *$EFL(x)$: x es el número de Gödel de una expresión que consiste de una letra funcional.*
   iv. *$EPL(x)$: x es el número de Gödel de una expresión que consiste de un símbolo predicativo.*

2. i. *La función Arg_T, donde si x es el número de Gödel de la letra funcional f_j^n, entonces $Arg_T(x) = n$.*
   ii. *La función Arg_P, donde si x es el número de Gödel del símbolo predicativo A_j^n, entonces $Arg_P(x) = n$.*

3. *$Gd(x)$: x es el número de Gödel de una expresión de K.*

4. *$MP(x, y, z)$: La expresión con número de Gödel z es una consecuencia directa de las expresiones con número de Gödel x e y por Modus Ponens.*

5. *$Gen(x, y)$: La expresión con número de Gödel y es una consecuencia directa de la expresión con número de Gödel x por Gen.*

6. *$Trm(x)$: x es el número de Gödel de un término de K.*

7. *$Atfml(x)$: x es el número de Gödel de una fórmula atómica de K.*

8. *$Fml(y)$: y es el número de Gödel de una fórmula de K.*

9. *$Subst(x, y, u, v)$: x es el número de Gödel del resultado de sustituir en la expresión con número de Gödel y el término con número de Gödel u por todas las ocurrencias libres de la variable con número de Gödel v.*

10. *$Sub(y, u, v)$: El número de Gödel del resultado de sustituir el término con número de Gödel u por todas las ocurrencias libres de la expresión con número de Gödel y de la variable con número de Gödel v.*

11. *$Fr(y, v)$: y es el número de Gödel de una fórmula o de un término de K que contiene ocurrencias libres de la variable con número de Gödel v.*

12. *$Ff(u, v, w)$: u es el número de Gödel de un término que es libre para la variable con número de Gödel v en la fórmula con número de Gödel w.*

13. a. *$Ax_1(x)$: x es el número de Gödel de una instancia del esquema de axioma (A1).*
    b. *$Ax_2(x)$: x es el número de Gödel de una instancia del esquema de axioma (A2).*
    c. *$Ax_3(x)$: x es el número de Gödel de una instancia del esquema de axioma (A3).*
    d. *$Ax_4(x)$: x es el número de Gödel de una instancia del esquema de axioma (A4).*
    e. *$Ax_5(x)$: x es el número de Gödel de una instancia del esquema de axioma (A5).*
    f. *$LAX(y)$: y es el número de Gödel de un axioma lógico de K.*

14. *La siguiente función **negación** es primitiva recursiva. $Neg(x)$: el número de Gödel de $(\neg\varphi)$ si x es el número de Gödel de φ*

15. *La siguiente función **implicación** es primitiva recursiva. $Cond(x, y)$: el número de Gödel de $(\varphi \to \psi)$ si x es el número de Gödel de φ e y es el número de Gödel de ψ.*

16. *$Clos(u)$: El número de Gödel de la clausura de φ si u es el número de Gödel de φ.*

Proposición 5.7. *Si K es una teoría con un vocabulario primitivo recursivo (o recursivo) y cuyo lenguaje contenga la constante 0 y la letra funcional f_1^1 de $\mathscr{L}_A$, entonces las siguientes funciones y relación son primitivas recursivas (o recursivas).*

17. *$Num(y)$: el numero de Gödel de la expresión $\overline{y}$.*

18. *$Nu(x)$: x es el número de Gödel de un numeral.*

19. *$D(u)$: El número de Gödel de $\varphi(\overline{u})$ si u es el número de Gödel de la fórmula $\varphi(x_1)$. A D se le llama la función diagonal.*

Definición 5.8. Decimos que una teoría K tiene un conjunto de axiomas primitivo recursivo (o recursivo) si la siguiente propiedad $PrAx$ es primitiva recursiva (o recursiva)

$$PrAx(y) : y \text{ es el número de Gödel de un axioma propio de } K.$$

Observación 5.7. S tiene un conjunto de axiomas primitivo recursivo. Se puede consultar la prueba de por qué $PrAx(y)$ es primitiva recursiva en [1], páginas 199-200.

A continuación enunciaremos las últimas relaciones recursivas que necesitamos, se puede consultar el por qué son recursivas en [1], página 200.

Proposición 5.9. *Sea K una teoría con un vocabulario primitivo recursivo (o recursivo) y un conjunto de axiomas primitivo recursivo (o recursivo) entonces las siguientes relaciones son primitivas recursivas:*

20. *$Ax(y)$: y es el número de Gödel de un axioma de K.*

21. *$Prf(y)$: y es el número de Gödel de una prueba en K.*

22. *$Pf(y,x)$: y es el número de Gödel de una prueba de una fórmula con número de Gödel x.*

Proposición 5.10. *Sea K una teoría de primer orden con igualdad que contenga a la constante 0 y a la letra funcional f_1^1 del lenguaje $\mathscr{L}_A$ y tal que K tenga un vocabulario y conjunto de axiomas primitivo recursivo (o recursivo). También supongase que:*

$$\textit{Para cualesquiera } r,s \in \mathbb{N}, \textit{ si } \vdash_K \overline{r} = \overline{s}, \textit{ entonces } r = s.$$

Entonces cualquier función número-teórica $f(k_1,\ldots,k_n)$ que es representable en K es recursiva.

Demostración. Supongamos que f es representable en K por la fórmula $\varphi(x_1,\ldots,x_n,x_{n+1})$. Ahora, consideremos la relación $P_\varphi(u_1,\ldots,u_n,u_{n+1},y)$ como aquella que ocurre si y es el número de Gödel de una prueba en K de la fórmula $\varphi(\overline{u}_1,\ldots,\overline{u}_n,\overline{u}_{n+1})$.
Notemos que

$$\text{Si } P_\varphi(u_1,\ldots,u_n,u_{n+1},y), \text{ entonces } f(u_1,\ldots,u_n) = u_{n+1}. \tag{a}$$

En efecto, si $f(u_1,\ldots,u_n) = r$, como φ representa a f en K se cumple que $\vdash_K \varphi(\overline{u}_1,\ldots,\overline{u}_n,\overline{r})$ y también $\vdash_K (\exists_1 y)\varphi(\overline{u}_1,\ldots,\overline{u}_n,y)$. Como $P_\varphi(u_1,\ldots,u_n,u_{n+1},y)$, entonces $\vdash_K \varphi(\overline{u}_1,\ldots,\overline{u}_n,\overline{u}_{n+1})$, así, tenemos que $\vdash_K \overline{r} = \overline{u}_{n+1}$. Ahora, por la hipótesis se cumple que $r = u_{n+1}$, es decir, $f(u_1,\ldots,u_n) = u_{n+1}$.
Ahora, sea m el número de Gödel de $\varphi(x_1,\ldots,x_n,x_{n+1})$. Entonces, $P_\varphi(u_1,\ldots,u_n,u_{n+1},y)$ es equivalente a:

$$Pf(y, Sub(\ldots Sub(Sub(m, Num(u_1), 21), Num(u_2), 29)\ldots Num(u_{n+1}), 21+8n))$$

Son equivalentes pues para $1 \leq i \leq n+1$, $Num(u_i)$ es el número de Gödel del término $\overline{u}_i$, así que:

i. $Sub(m, Num(u_1), 21)$: El número de Gödel de sustituir el termino con número de Gödel $Num(u_1)$ (es decir, sustituiremos por el término $\overline{u}_1$) todas las ocurrencias libres en la expresión con número de Gödel m (es decir se sustituirán en la fórmula $\varphi(x_1,\ldots,x_n,x_{n+1})$) de la variable con número de Gödel 21 (es decir las ocurrencias libres de la variable x_1 pues $g(x_1) = 13+8 = 21$. Así, $Sub(m, Num(u_1), 21)$ es el número de Gödel de la fórmula $\varphi(\overline{u}_1,\ldots,x_n.x_{n+1})$.

ii. $Sub(Sub(m, Num(u_1), 21), Num(u_2), 29)$: El número de Gödel de sustituir el termino con número de Gödel $Num(u_2)$ (es decir, sustituiremos por el término $\overline{u}_2$) todas las ocurrencias libres en la expresión con número de Gödel $Sub(m, Num(u_1), 21)$ (es decir se sustituirán en la fórmula $\varphi(\overline{u}_1,\ldots,x_n.x_{n+1})$) de la variable con número de Gödel 29 (es decir las ocurrencias libres de la variable x_2 pues $g(x_2) = 13+8(2) = 29$. Así, $Sub(Sub(m, Num(u_1), 21), Num(u_2), 29)$ es el número de Gödel de la fórmula $\varphi(\overline{u}_1,\overline{u}_2\ldots,x_n,x_{n+1})$.

iii. $Sub(Sub(Sub(m, Num(u_1), 21), Num(u_2), 29), Num(u_3), 37)$ es el número de Gödel de la fórmula $\varphi(\overline{u}_1,\overline{u}_2,\overline{u}_3\ldots,x_n,x_{n+1})$

iv. Seguimos construyendo y obtenemos que $Sub(\ldots Sub(Sub(m, Num(u_1), 21), Num(u_2), 29)\ldots, Num(u_{n+1}), 21+8n)$ es el número de Gödel de la fórmula $\varphi(\overline{u}_1,\ldots,\overline{u}_n,\overline{u}_{n+1})$

v. Entonces, $Pf(y, Sub(\ldots Sub(Sub(m, Num(u_1), 21), Num(u_2), 29)\ldots, Num(u_{n+1}), 21{+}8n))$: y es el número de Gödel de una prueba de una fórmula con número de Gödel $Sub(\ldots Sub(Sub(m, Num(u_1), 21), Num(u_2), 29)\ldots, Num(u_{n+1}), 21+8n)$ (es decir y es el número de Gödel de una prueba de la fórmula $\varphi(\overline{u}_1, \ldots, \overline{u}_n, \overline{u}_{n+1})$)

Así, $P_\varphi(u_1, \ldots, u_n, u_{n+1}, y)$ es equivalente a
$Pf(y, Sub(\ldots Sub(Sub(m, Num(u_1), 21), Num(u_2), 29)\ldots Num(u_{n+1}), 21 + 8n))$.

Ahora, por las proposiciones 5.6, 5.7 y 5.9, $P_\varphi(u_1, \ldots, u_n, u_{n+1}, y)$ es una relación primitiva recursiva (o recursiva).

Notemos que lo siguiente se cumple: Si $R(x_1, \ldots, x_n, z)$ es primitiva recursiva (o recursiva) y si para toda $x_1, \ldots, x_n \in \mathbb{N}$ existe $z \in \mathbb{N}$ tal que $R(x_1, \ldots, x_n, z)$, entonces la función $g(x_1, \ldots, x_n) = \mu z(R(x_1, \ldots, x_n, z))$ es una función recursiva.
En efecto, como R es recursiva, entonces C_R es una función recursiva. Como existe $z \in \mathbb{N}$ tal que $R(x_1, \ldots, x_n, z)$, entonces se cumple que $C_R(x_1, \ldots, x_n, z) = 0$, así, se tiene que existe $z \in \mathbb{N}$ tal que $C_R(x_1, \ldots, x_n, z) = 0$, entonces existe el mínimo $z_0 \in \mathbb{N}$ tal que $C_R(x_1, \ldots, x_n, z_0) = 0$. Entonces podemos definir la función $h : \mathbb{N}^n \longrightarrow \mathbb{N}$ tal que

$$h(x_1, \ldots, x_n) = \mu z(C_R(x_1, \ldots, x_n, z) = 0).$$

Como C_R es recursiva, tenemos que h es una función recursiva. Ahora bien, $h(x_1, \ldots, x_n) = z_0$ donde z_0 es el menor natural tal que $C_R(x_1, \ldots, x_n, z_0) = 0$, es decir, z_0 es el menor natural tal que $R(x_1, \ldots, x_n, z_0)$. Como existe $z \in \mathbb{N}$ tal que $R(x_1, \ldots, x_n, z)$, entonces, existe el menor natural z_1 tal que $R(x_1, \ldots, x_n, z_1)$,entonces,$z_0 = z_1$.
Así que $g(x_1, \ldots, x_n) = \mu z(R(x_1, \ldots, x_n, z)) = z_1 = z_0 = h(x_1, \ldots, x_n)$. Por lo tanto, $h = g$, así que, g es una función recursiva.

Ahora, si $k_1, \ldots, k_n \in \mathbb{N}$, entonces existe $y \in \mathbb{N}$ tal que $f(k_1, \ldots, k_n) = y$, entonces se cumple que $\vdash_K \varphi(\overline{k_1}, \ldots, \overline{k_n}, \overline{y})$, así, si j es el número de Gödel de una prueba en K de $\varphi(\overline{k_1}, \ldots, \overline{k_n}, \overline{y})$, tenemos que $P_\varphi(k_1, \ldots, k_n, y, j)$. Notemos que la existencia del j depende del $y \in \mathbb{N}$ tal que $f(k_1 \ldots, k_n) = y$. Así, denotemos por $y_0 = y$ y a j como $y_1 = j$ para tener presente la dependencia de j. Así tenemos que,para $k_1, \ldots, k_n \in \mathbb{N}$, existe $y_0 \in \mathbb{N}$ tal que $P_\varphi(k_1, \ldots, k_n, y_0, y_1)$. Por lo anterior, tenemos que si definimos $g : \mathbb{N}^n \longrightarrow \mathbb{N}$ tal que

$$g(k_1, \ldots, k_n) = \mu y_0(P_\varphi(k_1, \ldots, k_n, y_0, y_1)),$$

entonces g es recursiva. Veamos que $f = g$. Sean $k_1, \ldots, k_n \in \mathbb{N}$, ahora, por definición, $g(k_1, \ldots, k_n) = y_0$ donde y_0 es el mínimo natural tal que $P_\varphi(k_1, \ldots, k_n, y_0, y_1)$, y por (a) tenemos que $f(k_1, \ldots, k_n) = y_0$. Por lo tanto $f(k_1, \ldots, k_n) = g(k_1, \ldots, k_n)$. Así, concluimos que f es recursiva.
Por lo tanto, toda función representable en K es una función recursiva. ■

Corolario 4. *Supongase que S es consistente, entonces la clase de funciones recursivas es idéntica a la clase de funciones representables en S.*

Demostración. Ya sabemos que S tiene un vocabulario y conjunto de axiomas primitivo recursivo. También, sabemos que S incluye a la constante 0 y a la letra funcional f_1^1. Veamos que en S se cumple que para $r, s \in \mathbb{N}$ si $\vdash_S \overline{r} = \overline{s}$, entonces $r = s$.
Supongamos que $r \neq s$ entonces por la Proposición 3.8 inciso $a) - i.$ se cumple que $\vdash_S \overline{r} \neq \overline{s}$, entonces tenemos que $\vdash_S (\overline{r} = \overline{s}) \ \wedge \ (\overline{r} \neq \overline{s})$ lo cual es una contradicción, pues S es consistente, por lo tanto se cumple que $r = s$.
Así que siempre que $\vdash_S \overline{r} = \overline{s}$, entonces $r = s$.
Entonces por la Proposición 5.10, si f es representable entonces f es recursiva.

Y por la proposición 4.16, si f es recursiva, entonces S es representable. Por lo tanto la clase de funciones representables es la clase de las funciones recursivas. ∎

Corolario 5. *Si S es consistente, entonces una relación número-teórica $R(x_1, \ldots, x_n)$ es recursiva si y solo si es expresable en S.*

Demostración. R es recursiva si y solo si C_R es una función recursiva, por el corolario anterior C_R es recursiva si y solo si C_R es representable en S. Por ultimo, por la Proposición 4.7 C_R es representable en S si y solo si R es expresable en S. Por lo tanto, $R(x_1, \ldots, x_n)$ es recursiva si y solo si es expresable en S. ∎

5.2. Teoremas de incompletitud

Es momento de que analicemos el teorema de incompletitud que Gödel demostró en sus trabajos, pese a que es un solo teorema, este necesita de resultados igual de importantes para la lógica matemática que demostraremos a continuación.

Recordemos que si K es una teoría en el lenguaje $\mathscr{L}_A$, la función diagonal D tiene la propiedad que, si u es el número de Gödel de una fórmula $\varphi(x_1)$, entonces $D(u)$ es el número de Gödel de la fórmula $\varphi(\bar{u})$.

Notación. Cuando $\mathscr{C}$ es una expresión de una teoría y el número de Gödel de $\mathscr{C}$ es q, denotaremos al numeral $\bar{q}$ por $\ulcorner \mathscr{C} \urcorner$. Podemos pensar que $\ulcorner \mathscr{C} \urcorner$ es un "nombre" para la expresión $\mathscr{C}$ dentro del lenguaje $\mathscr{L}_A$.

Comencemos con un resultado que implica el uso de la función D.

Proposición 5.11 (Lema de la diagonalización)**.** *Supongase que D es una función representable en una teoría con igualdad K en el lenguaje $\mathscr{L}_A$. Entonces, para cualquier $\psi(x_1) \in \mathcal{FORM}$ en donde x_1 es la única variable libre, existe $\varphi \in \mathcal{FORM}$ sentencia tal que*

$$\vdash_K \varphi \Leftrightarrow \psi(\ulcorner \varphi \urcorner)$$

Demostración. Como D es representable en K, digamos que es representada en K por la fórmula $\gamma(x_1, x_2)$. Ahora construyamos la fórmula $(\triangledown)$ siguiente:

$$(\forall x_2)(\gamma(x_1, x_2) \to \psi(x_2)) \tag{$\triangledown$}$$

Sea m el número de Gödel de $(\triangledown)$. Ahora, sustituyamos a x_1 por $\overline{m}$ en $(\triangledown)$ y obtengamos la fórmula φ:

$$(\forall x_2)(\gamma(\overline{m}, x_2) \to \psi(x_2)) \tag{φ}$$

Sea q el número de Gödel de φ, entonces $\overline{q}$ es $\ulcorner \varphi \urcorner$. Se tiene que, como m es el número de Gödel de la fórmula $(\triangledown)$ entonces $D(m)$ es el número de Gödel de la fórmula $\triangledown(\overline{m})$, pero $\triangledown(\overline{m})$ es la fórmula φ, así que $D(m) = q$. Como γ representa a D en K y como $D(m) = q$, se cumple que

$$\vdash_K \gamma(\overline{m}, \overline{q}) \tag{∂}$$

Vamos a demostrar que $\vdash_K \varphi \Leftrightarrow \psi(\overline{q})$.

a. Veamos que $\vdash_K \varphi \to \psi(\overline{q})$.

1.	φ	[Hipótesis]
2.	$(\forall x_2)(\gamma(\overline{m}, x_2) \to \psi(x_2))$	[1. es la abreviación de 2.]

$\overline{q}$ es un término libre para x_2 en la fórmula $(\gamma(\overline{m}, x_2) \rightarrow \psi(x_2))$, entonces por la regla (A4) se tiene que $\vdash_K (\forall x_2)(\gamma(\overline{m}, x_2) \rightarrow \psi(x_2)) \rightarrow (\gamma(\overline{m}, \overline{q}) \rightarrow \psi(\overline{q}))$, entonces ocupando MP con 2. tenemos:

3.	$\gamma(\overline{m}, \overline{q}) \rightarrow \psi(\overline{q})$	
4.	$\gamma(\overline{m}, \overline{q})$	[Se cumple (∂)]
5.	$\psi(\overline{q})$	[MP 3 y 4]
6.	$\varphi \vdash_K \psi(\overline{q})$	[Prueba 1-5]
7.	$\vdash_K \varphi \rightarrow \psi(\overline{q})$	[Teorema de la deducción]

b. Probemos ahora que $\vdash_K \psi(\overline{q}) \rightarrow \varphi$.

1.	$\psi(\overline{q})$	[Hipótesis]
2.	$\gamma(\overline{m}, x_2)$	[Hipótesis]
3.	$(\exists_1 x_2)\gamma(\overline{m}, x_2)$	[Pues γ representa a D]
4.	$\gamma(\overline{m}, \overline{q})$	[Se cumple (∂)]
5.	$x_2 = \overline{q}$	[Usando la unicidad descrita en 3 con 1 y 2]
6.	$\psi(x_2)$	[Usamos (A7$'$) y MP dos veces usando 5 y 1]
7.	$\psi(\overline{q}), \gamma(\overline{m}, x_2) \vdash_K \psi(x_2)$	[Prueba 1-6]
8.	$\psi(\overline{q}) \vdash_K \gamma(\overline{m}, x_2) \rightarrow \psi(x_2)$	[Teorema de la deducción en 7.]
9.	$\psi(\overline{q}) \vdash_K (\forall x_2)(\gamma(\overline{m}, x_2) \rightarrow \psi(x_2))$	[Gen en 8.]
10.	$\psi(\overline{q}) \vdash_K \varphi$	[10. es la abreviación de 9.]
11.	$\vdash_K \psi(\overline{q}) \rightarrow \varphi$	[Teorema de la deducción en 10.]

De a. y b. tenemos que $\vdash_S \varphi \rightarrow \psi(\overline{q})$ y $\vdash_K \psi(\overline{q}) \rightarrow \varphi$, así que $\vdash_K (\varphi \rightarrow \psi(\overline{q})) \wedge (\psi(\overline{q}) \rightarrow \varphi)$, es decir:

$$\vdash_K \varphi \Leftrightarrow \psi(\overline{q})$$

Por lo tanto, hemos probado que existe $\varphi \in \mathcal{FORM}$ tal que

$$\vdash_K \varphi \Leftrightarrow \psi(\ulcorner \varphi \urcorner)$$

■

Proposición 5.12 (Teorema del punto fijo)**.** *Supongamos que todas las funciones recursivas son representables en una teoría con igualdad K en el lenguaje $\mathscr{L}_A$. Entonces, para cualquier $\psi(x_1) \in \mathcal{FORM}$ en donde x_1 es la única variable libre, existe una sentencia $\varphi \in \mathcal{FORM}$ tal que*

$$\vdash_K \varphi \Leftrightarrow \psi(\ulcorner \varphi \urcorner)$$

Demostración. Como K es una teoría con igualdad en el lenguaje $\mathscr{L}_A$, solo tiene a la constante 0, las letras funcionales f_1^1, f_1^2 y f_2^2 y el símbolo predicativo A_1^2, entonces por la Observación 5.6 se tiene que K tiene un vocabulario primitivo recursivo.
Como K tiene un vocabulario primitivo recursivo, entonces, por la Proposición 5.7 inciso 19, se tiene que la función D es recursiva, así por hipótesis D es representable en K, por lo que, por la Proposición 5.11 se cumple que para cualquier $\psi(x_1) \in \mathcal{FORM}$ en donde x_1 es la única variable libre, existe $\varphi \in \mathcal{FORM}$ sentencia tal que

$$\vdash_K \varphi \Leftrightarrow \psi(\ulcorner \varphi \urcorner)$$

■

Observación 5.8. Ya vimos que S es una teoría con igualdad en el lenguaje $\mathscr{L}_A$ y que todas las funciones recursivas son representables en S, por lo tanto tanto el Lema de la diagonalización como el Teorema del punto fijo, son aplicables en S. Estos resultados son de vital importancia en la demostración del teorema de incompletitud.

Definición 5.13. 1. Sea K una teoría cuyo lenguaje contenga la constante 0 y la letra funcional f_1^1. Decimos que K es $\omega-$consistente si, para toda $\varphi(x) \in \mathcal{FORM}$ donde $x \in VAR$ es la única variable libre, si $\vdash_K \neg\varphi(\overline{n})$, entonces no ocurre que $\vdash_K (\exists x)\varphi(x)$.

2. Sea K una teoría en el lenguaje $\mathscr{L}_A$. Decimos que K es una teoría verdadera si todos los axiomas propios de K son verdaderos en el modelo estándar.

Observación 5.9. 1. Si K es una teoría verdadera, entonces sus axiomas propios son verdaderos en el modelo estándar; también se sabe que los axiomas lógicos son válidos en cualquier modelo y MP y Gen conducen de fórmulas verdaderas en un modelo a fórmulas verdaderas en ese modelo, así todos los teoremas de la teoría serán verdaderos en el modelo estándar.

2. Toda teoría verdadera es $\omega-$ consistente, si $\vdash_K \neg\varphi(\overline{n})$ para cada número natural, entonces bajo la interpretación del modelo estándar tendríamos que para todo número natural, es falso que $\varphi(x)$; así la fórmula $(\exists x)\varphi(x)$ no puede ser verdadera en el modelo estándar, pues si lo fuera, tendríamos que existe un número natural x_0 tal que $\varphi(x_0)$ es verdadera, por lo que no puede ocurrir entonces que $\vdash_K (\exists x)\varphi(x)$

Proposición 5.14. *Si K es $\omega-$consistente, entonces K es consistente.*

Demostración. Sea $\psi(x)$ una fórmula donde x es la única variable libre. Consideremos ahora la fórmula $\varphi(x) := \neg\psi(x) \ \wedge \ \psi(x)$. Para $n \in \mathbb{N}$ se cumple lo siguiente:

1.	$\psi(x) \to \neg\neg\psi(x)$	[Pues $\vdash_K \gamma \leftrightarrow \neg\neg\gamma$]
2.	$\psi(x) \ \vee \ \neg\psi(x)$	[Pues $\vdash_K \gamma \vee \neg\gamma$]
3.	$\psi(x) \ \vee \ \neg\psi(x) \to \neg\neg\psi(x) \ \vee \ \neg\psi(x)$	[Pues $\vdash_K (\alpha \to \beta) \to ((\alpha \vee \gamma) \to (\beta \vee \gamma))$, MP 1]
4.	$\neg\neg\psi(x) \ \vee \ \neg\psi(x)$	[MP (2,3)]
5.	$\neg\neg\psi(x) \ \vee \ \neg\psi \to \neg(\neg\psi(x) \ \wedge \ \psi(x))$	[Pues $\vdash_K \neg(\alpha \wedge \beta) \leftrightarrow (\neg\alpha \vee \neg\beta)$]
6.	$\neg(\neg\psi(x) \ \wedge \ \psi(x))$	[MP (4,5)]
7.	$(\forall x)\neg(\neg\psi(x) \ \wedge \ \psi(x))$	[Gen 6]
8.	$\neg(\neg\psi(\overline{n}) \ \wedge \ \psi(\overline{n}))$	[Pues $\overline{n}$ es libre para x y se aplica (A4)]
9.	$\neg\varphi(\overline{n})$	[Pues 9 es la abreviación de 8]

Por lo tanto para todo $n \in \mathbb{N}$, $\vdash_K \neg\varphi(\overline{n})$. Como K es $\omega-$consistente, entonces no ocurre que $\vdash_K (\exists x)\varphi(x)$.
Si K fuera inconsistente, entonces existe $\alpha \in \mathcal{FORM}$ tal que $\vdash_K \alpha$ y $\vdash_K \neg\alpha$. También, sabemos que para $\beta, \gamma \in \mathcal{FORM}$ $\vdash_K \neg\gamma \to (\gamma \to \beta)$, entonces para $\gamma := \alpha$ y $\beta := (\exists x)\varphi(x)$ se cumple que $\vdash_K \neg\alpha \to (\alpha \to ((\exists x)\varphi(x)))$, si ocupamos MP dos veces tenemos que $\vdash_K (\exists x)\varphi(x)$ lo cual es una contradicción pues teníamos que no ocurre que $\vdash_K (\exists x)\varphi(x)$. Por lo tanto K es consistente. ∎

Definición 5.15. Para una teoría K decimos que una sentencia $\varphi \in \mathcal{FORM}$ es una sentencia indecidible si φ ni $\neg\varphi$ son teoremas de K, es decir, no ocurre que $\vdash_K \varphi$ y no ocurre $\vdash_K \neg\varphi$.

5.2.1. El primer Teorema de incompletitud de Gödel.

Construyendo las sentencias de Gödel.

Sea K una teoría con igualdad en el lenguaje $\mathscr{L}_A$ que satisfaga las siguientes 3 condiciones:

1. K tiene un conjunto de axiomas recursivo (es decir, $PrAx(y)$ es recursiva).

2. $\vdash_K 0 \neq \overline{1}$.

3. Toda función recursiva es representable en K.

Como K es una teoría con igualdad en el lenguaje $\mathscr{L}_A$, por la Observación 5.6, K tiene un vocabulario primitivo recursivo, entonces las 16 relaciones y funciones de la Proposición 5.6 son recursivas. De igual manera, las funciones y relación de la Proposición 5.7 son recursivas. Y, por la condición 1., las 3 relaciones de la proposición 5.9 son recursivas. Así, tenemos una lista de 22 funciones y relaciones recursivas.
Ahora, si R es una relación recursiva, entonces C_R es una función recursiva, y así, por la condición 3., C_R es representable en K. Como tenemos que $\vdash_K 0 \neq \overline{1}$ y que C_R es representable en K, por la Proposición 4.7 se cumple que R es expresable en K. Por tanto, toda relación recursiva es expresable en K.
Como toda función recursiva es representable en K, el Teorema del punto fijo es aplicable en K.

Recordemos que $Pf(y, x)$ significa que y es el número de Gödel de una prueba en K de una fórmula con número de Gödel x. Por la Proposición 5.9, $Pf(y, x)$ es una relación recursiva, así que es expresable en K. Digamos que es expresable por $\mathscr{PF}(x_2, x_1) \in \mathcal{FORM}$.

Sea $\varphi(x_1) := (\forall x_2)\neg\mathscr{PF}(x_2, x_1)$. $\varphi(x_1)$ es una fórmula cuya única variable libre es x_1, entonces, por el teorema del punto fijo, existe $\mathscr{G} \in \mathcal{FORM}$ sentencia tal que

$$\vdash_K \mathscr{G} \Leftrightarrow \varphi(\ulcorner\mathscr{G}\urcorner),$$

es decir

$$\vdash_K \mathscr{G} \Leftrightarrow (\forall x_2)\neg\mathscr{PF}(x_2, \ulcorner\mathscr{G}\urcorner) \qquad (\diamond)$$

Recordemos que $\ulcorner\mathscr{G}\urcorner$ es $\overline{q}$ donde q es el número de Gödel de $\mathscr{G}$. Si nos fijamos en lo que nos dice la fórmula $(\forall x_2)\neg\mathscr{PF}(x_2, \ulcorner\mathscr{G}\urcorner)$ en términos de la interpretación estándar, es que no existe número natural que sea el número de Gödel de una prueba en K de la fórmula $\mathscr{G}$, es decir, estamos diciendo que no hay una prueba en K de la fórmula $\mathscr{G}$. Y por $(\diamond)$, bajo la interpretación del modelo estándar, estamos diciendo que la fórmula $\mathscr{G}$ es equivalente a una afirmación que nos indica que $\mathscr{G}$ no es demostrable en K, es como si $\mathscr{G}$ nos dijera "no soy demostrable en K". Así parece que esta afirmación nos está llevando a contradicciones, pero lo que veremos a continuación es que el primer teorema de incompletitud nos demuestra que no es que hayamos construido una contradicción en la teoría, sino que $\mathscr{G}$ es una sentencia indecidible de K.
Nos referiremos a $\mathscr{G}$ como una *sentencia de Gödel* para K.

Proposición 5.16 (Teorema de incompletitud de Gödel)**.** *Sea K una teoría con igualdad en el lenguaje $\mathscr{L}_A$. Suponga que K satisface las condiciones 1-3. Entonces:*

a. Si K es consistente, entonces no ocurre que $\vdash_K \mathscr{G}$.

b. Si K es $\omega-$consistente, entonces no ocurre que $\vdash_K \neg\mathscr{G}$.

Así, si K es $\omega-$consistente, entonces $\mathscr{G}$ es una sentencia indecidible en K, es decir, K no es una teoría completa.

Demostración. Sea q el número de Gödel de la sentencia de Gödel $\mathscr{G}$.

a. Supongamos que K es consistente y supongamos que $\vdash_K \mathscr{G}$.
Como $\vdash_K \mathscr{G}$, sea r el número de Gödel de una prueba para $\mathscr{G}$ en K. Se cumple entonces que $Pf(r, q)$ y como Pf es expresable en K por la fórmula $\mathscr{PF}$, $\vdash_K \mathscr{PF}(\overline{r}, \overline{q})$, es decir, $\vdash_K \mathscr{PF}(\overline{r}, \ulcorner\mathscr{G}\urcorner)$.
Por $(\diamond)$ tenemos que $\vdash_K \mathscr{G} \Leftrightarrow (\forall x_2)\neg\mathscr{PF}(x_2, \ulcorner\mathscr{G}\urcorner)$ y como $\vdash_K \mathscr{G}$, entonces se cumple que $\vdash_K (\forall x_2)\neg\mathscr{PF}(x_2, \ulcorner\mathscr{G}\urcorner)$. Además, se tiene que $\overline{r}$ es un término libre para la variable x_2 en la fórmula $\neg\mathscr{PF}(x_2, \ulcorner\mathscr{G}\urcorner)$, entonces por la regla (A4) se tiene que $\vdash_K \neg\mathscr{PF}(\overline{r}, \ulcorner\mathscr{G}\urcorner)$.
Por tanto, tenemos que $\vdash_K \neg\mathscr{PF}(\overline{r}, \ulcorner\mathscr{G}\urcorner)$ y que $\vdash_K \mathscr{PF}(\overline{r}, \ulcorner\mathscr{G}\urcorner)$, así que, K es inconsistente, lo cual es una contradicción.
Por lo tanto no ocurre que $\vdash_K \mathscr{G}$.

b. Supongamos que K es $\omega-$consistente y que $\vdash_K \neg\mathscr{G}$.
De ($\diamond$) tenemos que $\vdash_K \mathscr{G} \Leftrightarrow (\forall x_2)\neg\mathscr{P}\mathscr{F}(x_2, \ulcorner\mathscr{G}\urcorner)$, por lo que $\vdash_K \neg\mathscr{G} \Leftrightarrow \neg((\forall x_2)\neg\mathscr{P}\mathscr{F}(x_2, \ulcorner\mathscr{G}\urcorner))$. Como $\vdash_K \neg\mathscr{G}$, entonces $\vdash_K \neg((\forall x_2)\neg\mathscr{P}\mathscr{F}(x_2, \ulcorner\mathscr{G}\urcorner))$ cuya abreviación es

$$\vdash_K (\exists x_2)\mathscr{P}\mathscr{F}(x_2, \ulcorner\mathscr{G}\urcorner). \tag{*}$$

También, como K es $\omega-$consistente, por la Proposición 5.14, se tiene que K es consistente y como $\vdash_K \neg\mathscr{G}$, entonces no ocurre que $\vdash_K \mathscr{G}$, es decir, no existe una prueba en K de $\mathscr{G}$. Entonces $Pf(n, q)$ es falso para todo numero natural n y como $\mathscr{P}\mathscr{F}$ expresa a Pf en K, se cumple que $\vdash_K \neg\mathscr{P}\mathscr{F}(\overline{n}, \overline{q})$, es decir, para $n \in \mathbb{N}$ $\vdash_K \neg\mathscr{P}\mathscr{F}(\overline{n}, \ulcorner\mathscr{G}\urcorner)$. Como K es $\omega-$consistente entonces no ocurre que $\vdash_K (\exists x_2)\mathscr{P}\mathscr{F}(x_2, \ulcorner\mathscr{G}\urcorner)$ lo que contradice a (*). Por lo tanto no ocurre que $\vdash_K \neg\mathscr{G}$.

Por último, si K es $\omega-$consistente, por b. no ocurre que $\vdash_K \neg\mathscr{G}$. También, por la Proposición 5.14, K es consistente, y por a. no ocurre que $\vdash_K \mathscr{G}$. Así, $\mathscr{G}$ es una sentencia indecidible, y por lo tanto, K es incompleta. ■

Observación 5.10. El teorema de incompletitud de Gödel se estableció para teorías que satisfacen las 3 condiciones dadas; ahora, si asumimos que una teoría K también satisface que K es una teoría verdadera, entonces también podemos probar la indecibilidad de $\mathscr{G}$:

i. Supongamos que ocurre que $\vdash_K \mathscr{G}$. Ya sabemos que $\vdash_K \mathscr{G} \Leftrightarrow (\forall x_2)\neg\mathscr{P}\mathscr{F}(x_2, \ulcorner\mathscr{G}\urcorner)$, así que $\vdash_K (\forall x_2)\neg\mathscr{P}\mathscr{F}(x_2, \ulcorner\mathscr{G}\urcorner)$. Como K es una teoría verdadera, entonces la fórmula $(\forall x_2)\neg\mathscr{P}\mathscr{F}(x_2, \ulcorner\mathscr{G}\urcorner)$ es verdadera bajo la interpretación del modelo estándar, pero bajo esta interpretación, la fórmula nos dice que $\mathscr{G}$ no es demostrable en K, lo cual es una contradicción. Así que no ocurre que $\vdash_K \mathscr{G}$.

ii. Supongamos que $\vdash_K \neg\mathscr{G}$. Como $\vdash_K \mathscr{G} \Leftrightarrow (\forall x_2)\neg\mathscr{P}\mathscr{F}(x_2, \ulcorner\mathscr{G}\urcorner)$ y $\vdash_K \neg\mathscr{G}$, entonces se cumple que $\vdash_K \neg((\forall x_2)\neg\mathscr{P}\mathscr{F}(x_2, \ulcorner\mathscr{G}\urcorner))$, es decir $\vdash_K (\exists x_2)\mathscr{P}\mathscr{F}(x_2, \ulcorner\mathscr{G}\urcorner)$. Como K es una teoría verdadera, entonces la fórmula $(\exists x_2)\mathscr{P}\mathscr{F}(x_2, \ulcorner\mathscr{G}\urcorner)$ es verdadera bajo la interpretación del modelo estándar, pero bajo esta interpretación, la fórmula nos dice que $\mathscr{G}$ es demostrable en K, es decir $\vdash_K \mathscr{G}$, lo cual es una contradicción, pues en i. ya habíamos visto que no ocurre que $\vdash_K \mathscr{G}$. Por tanto, no ocurre que $\vdash_K \neg\mathscr{G}$

De i. y ii., concluimos que $\mathscr{G}$ es una sentencia indecidible para K

Ahora, nos podemos preguntar, ¿qué ocurre con S?. Ya sabemos que S cumple con las 3 condiciones del Teorema de incompletitud. No es la intención de este trabajo entrar en debate acerca de la $\omega-$consistencia de S, pues necesitaríamos utilizar metateorías como ZFC para analizarlo. Así, que si nosotros asumimos que S es $\omega-$consistente, hemos probado que la aritmética de Peano S no puede ser una teoría completa, sin importar todo el desarrollo que hemos hecho con esta. De ahí la importancia del primer Teorema de incompletitud, pues hemos encontrado un sistema basado en los números naturales, en los que no todas las afirmaciones pueden ser demostrables.
Con todo esto, es natural que nos preguntemos: ¿Es posible demostrar con todo lo desarrollado en S la consistencia de S? El segundo teorema de incompletitud nos resuelve esta duda.

5.2.2. El segundo teorema de incompletitud de Gödel

Sea K una extensión de S (en este trabajo nos enfocaremos en S) en el lenguaje $\mathscr{L}_A$ tal que K tenga un conjunto de axiomas recursivo. Recordemos que $Neg(x)$ significa que si x es el número de Gödel de γ, entonces $Neg(x)$ es el número de Gödel de $\neg\gamma$. Por la Proposición 5.6, Neg es una función recursiva, así que es representable en K. Digamos que es representable por

$\mathscr{NEG}(x,y) \in \mathcal{FORM}$.
Sea $\mathscr{CON}_K$ la siguiente sentencia:

$$\mathscr{CON}_K := (\forall x_1)(\forall x_2)(\forall x_3)(\forall x_4)\neg(\mathscr{PF}(x_1,x_3) \ \wedge \ \mathscr{PF}(x_2,x_4) \ \wedge \ \mathscr{NEG}(x_3,x_4)).$$

En la interpretación estándar, $\mathscr{CON}_K$ afirma que no hay pruebas en K de una fórmula y de su negación, es decir, afirma que K es consistente.
Consideremos la siguiente sentencia:

$$\mathscr{CON}_k \to \mathscr{G} \tag{$\mathbb{G}$}$$

Donde $\mathscr{G}$ es una sentencia de Gödel. Recordemos que bajo la interpretación estándar, $\mathscr{G}$ afirma que no se puede probar $\mathscr{G}$ en K. Así, ($\mathbb{G}$) bajo la interpretación estándar afirma que si K es consistente, entonces no se puede probar $\mathscr{G}$, que es el primer teorema de incompletitud. Si se cumpliera que $\vdash_K \mathscr{CON}_k \to \mathscr{G}$ y que K es consistente, entonces no puede ocurrir que $\vdash_K \mathscr{CON}_k$, porque en caso contrario, se cumpliría que $\vdash_K \mathscr{G}$, que es imposible, pues al ser K consistente no ocurre que $\vdash_K \mathscr{G}$. Así, si K es consistente, entonces $\mathscr{CON}_K$ es una sentencia indecidible. Esto es lo que conocemos como el segundo teorema de incompletitud de Gödel. Podemos resumirlo de la siguiente manera: Si K es una teoría consistente, entonces la consistencia de K no puede ser probada dentro de K.

Nos centraremos en trabajar en S, que es una teoría ya bien conocida por nosotros y en la que es válido el primer teorema de incompletitud. Analizaremos la prueba del segundo teorema de incompletitud de Gödel que trabajaron Hilbert y Bernays en 1939. Esta prueba está basada en tres condiciones que conocemos como las condiciones de derivabilidad. Para entenderlas, veamos la siguiente definición:

Definición 5.17. En S definimos la fórmula $\mathscr{BEW}(x_1)$ como sigue:

$$\mathscr{BEW}(x_1) := (\exists x_2)\mathscr{PF}(x_2,x_1).$$

Bajo la interpretación estándar $\mathscr{BEW}(x_1)$ nos dice que existe una prueba para una fórmula que tiene número de Gödel x_1, es decir, la fórmula con número de Gödel x_1 es demostrable en S.

Observación 5.11. Notemos que para la fórmula $\varphi(x_1) := (\forall x_2)\neg\mathscr{PF}(x_2,x_1)$, por el Teorema del punto fijo, existe una sentencia de Gödel $\mathscr{G}$ tal que $\vdash_S \mathscr{G} \Leftrightarrow (\forall x_2)\neg\mathscr{PF}(x_2,x_1)$, además $\vdash_S (\forall x_2)\neg\mathscr{PF}(x_2,x_1) \Leftrightarrow \neg((\exists x_2)\mathscr{PF}(x_2,\ulcorner\mathscr{G}\urcorner))$, así que $\vdash_S \mathscr{G} \Leftrightarrow \neg\mathscr{BEW}(\ulcorner\mathscr{G}\urcorner)$.

A continuación enunciaremos las condiciones de derivabilidad de Hilbert-Bernays. Las que enunciaremos son unas simplificaciones del trabajo de Hilbert y Bernays dadas por Löb en 1955. No haremos la prueba de las condiciones en este trabajo, pero pueden ser consultadas en el Capítulo 2 de [5]

Proposición 5.18 (La condiciones de derivabilidad de Hilbert-Bernays)**.** *Si $\varphi,\psi \in \mathcal{FORM}$ son sentencias en S, entonces:*

HB1 Si $\vdash_S \varphi$, entonces $\vdash_S \mathscr{BEW}(\ulcorner\varphi\urcorner)$

HB2 $\vdash_S \mathscr{BEW}(\ulcorner\varphi \to \psi\urcorner) \to (\mathscr{BEW}(\ulcorner\varphi\urcorner) \to \mathscr{BEW}(\ulcorner\psi\urcorner))$

HB3 $\vdash_S \mathscr{BEW}(\ulcorner\varphi\urcorner) \to \mathscr{BEW}(\ulcorner\mathscr{BEW}(\ulcorner\varphi\urcorner)\urcorner)$

Ya sabemos que una sentencia de Gödel $\mathscr{G}$ en S afirma que no puede ser demostrada en S, es decir $\vdash_S \mathscr{G} \Leftrightarrow \neg\mathscr{BEW}(\ulcorner\mathscr{G}\urcorner)$.
Ahora, $\mathscr{BEW}(x_1)$, es una fórmula cuya única variable libre es x_1, entonces por el Teorema del punto fijo, existe una sentencia $\mathscr{H}$ tal que

$$\vdash_S \mathscr{H} \Leftrightarrow \mathscr{BEW}(\ulcorner\mathscr{H}\urcorner)$$

A la sentencia $\mathscr{H}$ la llamamos *sentencia de Henkin*. En la interpretación estándar, la sentencia de Henkin, afirma que existe una prueba en S de ella. A continuación veremos cuándo $\mathscr{H}$ es demostrable, no demostrable, indecidible en S o verdadera para el modelo estándar.

Notación 5.1. Si $\varphi \in \mathcal{FORM}$, denotaremos por $\Box\varphi$ a la fórmula $\mathscr{BEW}(\ulcorner\varphi\urcorner)$. Usando esta notación, las condiciones de derivabilidad de Hilbert-Bernays quedan como:

HB1 Si $\vdash_S \varphi$, entonces $\vdash_S \Box\varphi$.

HB2 $\vdash_S \Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi)$.

HB3 $\vdash_S \Box\varphi \to \Box\Box\varphi$.

También $\mathscr{G}$ y $\mathscr{H}$ satisfacen las equivalencias $\vdash_S \mathscr{G} \Leftrightarrow \neg\Box\mathscr{G}$ y $\vdash_S \mathscr{H} \Leftrightarrow \Box\mathscr{H}$

Proposición 5.19 (Teorema de Löb)**.** *Si φ es una sentencia de S, entonces si $\vdash_S \Box\varphi \to \varphi$, entonces $\vdash_S \varphi$.*

Demostración. Sea $\varphi \in \mathcal{FORM}$ una sentencia y supongamos que $\vdash_S \Box\varphi \to \varphi$. La fórmula $\mathscr{BEW}(x_1) \to \varphi$ es una fórmula cuya única variable libre es x_1, entonces, por el Teorema del punto fijo (Proposición 5.12) se cumple que existe una sentencia ψ tal que
$\vdash_S \psi \Leftrightarrow (\mathscr{BEW}(\ulcorner\psi\urcorner) \to \varphi)$, es decir,

$$\vdash_S \psi \Leftrightarrow (\Box\psi \to \varphi). \tag{5.1}$$

Ahora, se tiene que:

1.	$\psi \Leftrightarrow (\Box\psi \to \varphi)$	[Por 5.1]
2.	$\psi \to (\Box\psi \to \varphi)$	[$\vdash_S (\alpha \leftrightarrow \beta) \to (\alpha \to \beta)$ y MP con 1]
3.	$\Box(\psi \to (\Box\psi \to \varphi))$	[HB1 con 2]
4.	$\Box\psi \to \Box(\Box\psi \to \varphi)$	[HB2 con 3 y MP con 3]
5.	$\Box(\Box\psi \to \varphi) \to (\Box\Box\psi \to \Box\varphi)$	[HB2]
6.	$\Box\psi \to (\Box\Box\psi \to \Box\varphi)$	[$\vdash_S (\alpha \to \beta) \to ((\beta \to \gamma) \to (\alpha \to \gamma))$ y MP con 4 y 5]
7.	$\Box\psi \to \Box\Box\psi$	[HB3]

Sabemos que $\vdash_S (\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$, así que ocupando esto con 6 y 7 y aplicando MP dos veces tenemos que:

8.	$\Box\psi \to \Box\varphi$	
9.	$\Box\varphi \to \varphi$	[Hipótesis]
10.	$\Box\psi \to \varphi$	[$\vdash_S (\alpha \to \beta) \to ((\beta \to \gamma) \to (\alpha \to \gamma))$ y MP con 8 y 9]
11.	$(\Box\psi \to \varphi) \to \psi$	[$\vdash_S (\alpha \leftrightarrow \beta) \to (\beta \to \alpha)$ y MP con 1]
12.	ψ	[MP(10,11)]
13.	$\Box\psi$	[HB1 con 12]
14.	φ	[MP(10,12)]

Por lo tanto, hemos probado que si $\vdash_S \Box\varphi \to \varphi$, entonces $\vdash_S \varphi$. ■

Corolario 6. *Si $\mathscr{H}$ es una sentencia de Henkin para S, entonces $\vdash_S \mathscr{H}$ y $\mathscr{H}$ es verdadera para el modelo estándar.*

Demostración. Sabemos que $\vdash_S \mathscr{H} \Leftrightarrow \Box\mathscr{H}$. Así que $\vdash_S \Box\mathscr{H} \to \mathscr{H}$, entonces, por el Teorema de Löb, se cumple que $\vdash_S \mathscr{H}$.
Ahora, bajo la interpretación estándar, $\mathscr{H}$ afirma que $\mathscr{H}$ es demostrable en S lo cual es cierto, por lo tanto $\mathscr{H}$ es verdadera en el modelo estándar. ■

Es momento de demostrar el segundo teorema de incompletitud.

Proposición 5.20 (Segundo Teorema de incompletitud de Gödel)**.** *Si S es consistente, entonces no ocurre que* $\vdash_S \mathscr{CON}_S$*, es decir, si S es consistente, es imposible probar la consistencia usando los axiomas de S.*

Demostración. Supongamos que S es consistente.
Ya sabemos que $\vdash_S 0 \neq \overline{1}$. Como S es consistente, entonces no ocurre que $\vdash_S 0 = \overline{1}$.
La fórmula $0 = \overline{1}$ no tiene variables libres, así que es una sentencia en S. Si ocurriera que $\vdash_S \Box(0 = \overline{1}) \rightarrow (0 = \overline{1})$, entonces por el Teorema de Löb (Proposición 5.19), se cumpliría que $\vdash_S 0 = \overline{1}$, lo cual es una contradicción, por lo que no ocurre que $\vdash_S \Box(0 = \overline{1}) \rightarrow (0 = \overline{1})$.
Sabemos que para $\alpha, \beta \in \mathcal{FORM}$, $\vdash_S \neg\alpha \rightarrow (\alpha \rightarrow \beta)$, entonces para $\alpha := \neg\Box(0 = \overline{1})$ y $\beta := 0 = \overline{1}$, se cumple que
$\vdash_S \neg\Box(0 = \overline{1}) \rightarrow (\Box(0 = \overline{1}) \rightarrow 0 = \overline{1})$. Si ocurriera que $\vdash_S \neg\Box(0 = \overline{1})$, entonces ocupando MP tendríamos que $\vdash_S \Box(0 = \overline{1}) \rightarrow 0 = \overline{1}$ lo cual es una contradicción. Por lo tanto

$$\text{No ocurre que } \vdash_S \neg\Box(0 = \overline{1}). \tag{$\circ$}$$

Como $\vdash_S 0 \neq \overline{1}$, por (HB1) $\vdash_S \Box(0 \neq \overline{1})$.
Ahora, vamos a demostrar que $\vdash_S \mathscr{CON}_S \rightarrow \neg\Box(0 = \overline{1})$. Supongamos que $\vdash_S \mathscr{CON}_S$ y que $\vdash_S \Box(0 = \overline{1})$.
Sea q el número de Gödel de la fórmula $0 = \overline{1}$ y sea r el número de Gödel de la fórmula $0 \neq \overline{1}$, entonces se cumple que $Neg(q) = r$ y como Neg es representable por $\mathscr{NEG}$, entonces $\vdash_S \mathscr{NEG}(\overline{q}, \overline{r})$, es decir,

$$\vdash_S \mathscr{NEG}(\ulcorner 0 = \overline{1}\urcorner, \ulcorner 0 \neq \overline{1}\urcorner). \tag{i}$$

Como $\vdash_S \Box(0 \neq \overline{1})$, entonces $\vdash_S (\exists x_2)\mathscr{PF}(x_2, \ulcorner 0 \neq \overline{1}\urcorner)$, por regla C, para la constante a, tenemos que

$$\vdash_S \mathscr{PF}(a, \ulcorner 0 \neq \overline{1}\urcorner). \tag{ii}$$

Como $\vdash_S \Box(0 = \overline{1})$, entonces $\vdash_S (\exists x_2)\mathscr{PF}(x_2, \ulcorner 0 = \overline{1}\urcorner)$, por regla C, para la constante b, tenemos que

$$\vdash_S \mathscr{PF}(b, \ulcorner 0 = \overline{1}\urcorner). \tag{iii}$$

Así, de (i), (ii) y tenemos que

$$\vdash_S \mathscr{PF}(b, \ulcorner 0 = \overline{1}\urcorner) \ \wedge\ \mathscr{PF}(a, \ulcorner 0 \neq \overline{1}\urcorner) \ \wedge\ \mathscr{NEG}(\ulcorner 0 = \overline{1}\urcorner, \ulcorner 0 \neq \overline{1}\urcorner). \tag{iv}$$

Como $\vdash_S \mathscr{CON}_S$ se tiene que
$\vdash_S (\forall x_1)(\forall x_2)(\forall x_3)(\forall x_4)\neg(\mathscr{PF}(x_1, x_3) \ \wedge\ \mathscr{PF}(x_2, x_4) \ \wedge\ \mathscr{NEG}(x_3, x_4))$. Ahora, $\ulcorner 0 = \overline{1}\urcorner$ y $\ulcorner 0 \neq \overline{1}\urcorner$ son términos libres para las variables x_3 y x_4 respectivamente en la fórmula $\neg(\mathscr{PF}(x_1, x_3) \wedge \mathscr{PF}(x_2, x_4) \wedge \mathscr{NEG}(x_3, x_4))$, entonces por la regla (A4) y MP tenemos que

$$\vdash_S (\forall x_1)(\forall x_2)\neg(\mathscr{PF}(x_1, \ulcorner 0 = \overline{1}\urcorner) \ \wedge\ \mathscr{PF}(x_2, \ulcorner 0 \neq \overline{1}\urcorner) \ \wedge\ \mathscr{NEG}(\ulcorner 0 = \overline{1}\urcorner, \ulcorner 0 \neq \overline{1}\urcorner)).$$

De igual manera, b y a son términos libres para las variables x_1 y x_2 respectivamente en la fórmula $\neg(\mathscr{PF}(x_1, \ulcorner 0 = \overline{1}\urcorner) \ \wedge\ \mathscr{PF}(x_2, \ulcorner 0 \neq \overline{1}\urcorner) \ \wedge\ \mathscr{NEG}(\ulcorner 0 = \overline{1}\urcorner, \ulcorner 0 \neq \overline{1}\urcorner))$, entonces por la regla (A4) y MP se tiene que

$$\vdash_S \neg(\mathscr{PF}(b, \ulcorner 0 = \overline{1}\urcorner) \ \wedge\ \mathscr{PF}(a, \ulcorner 0 \neq \overline{1}\urcorner) \ \wedge\ \mathscr{NEG}(\ulcorner 0 = \overline{1}\urcorner, \ulcorner 0 \neq \overline{1}\urcorner)). \tag{v}$$

Entonces por (iv) y (v) tenemos que
$\vdash_S \mathscr{PF}(b, \ulcorner 0 = \overline{1}\urcorner) \ \wedge\ \mathscr{PF}(a, \ulcorner 0 \neq \overline{1}\urcorner) \ \wedge\ \mathscr{NEG}(\ulcorner 0 = \overline{1}\urcorner, \ulcorner 0 \neq \overline{1}\urcorner)$ y que
$\vdash_S \neg(\mathscr{PF}(b, \ulcorner 0 = \overline{1}\urcorner) \ \wedge\ \mathscr{PF}(a, \ulcorner 0 \neq \overline{1}\urcorner) \ \wedge\ \mathscr{NEG}(\ulcorner 0 = \overline{1}\urcorner, \ulcorner 0 \neq \overline{1}\urcorner))$ lo cual es una contradicción. Dicha contradicción viene de suponer que $\vdash_S \mathscr{CON}_S$ y que $\vdash_S \Box(0 = \overline{1})$. Por lo tanto, $\vdash_S \mathscr{CON}_S \rightarrow \neg\Box(0 = \overline{1})$.

Si ocurriera que $\vdash_S \mathscr{CON}_S$, entonces como $\vdash_S \mathscr{CON}_S \to \neg\Box(0 = \overline{1})$, por MP tenemos que $\vdash_S \neg\Box(0 = \overline{1})$, pero por $(\circ)$ tenemos que no ocurre que $\vdash_S \neg\Box(0 = \overline{1})$. Por lo tanto, no puede ocurrir que $\vdash_S \mathscr{CON}_S$.
Hemos probado que siempre que S sea consistente, no podemos probar la consistencia de S dentro de la teoría. ∎

Conclusiones

A lo largo de la realización de este trabajo fuimos capaces de visualizar la importancia que han tenido los Teoremas de Incompletitud para las matemáticas, pues fueron un parteaguas en cómo se concebían y estudiaban. Hasta 1930 muchos pensadores coexistían con la idea de que la ciencia matemática siempre sería exacta y que, a pesar de que no se conocía la veracidad de ciertas afirmaciones, la matemática sería capaz de resolverlo con tiempo y paciencia. Los dos teoremas de incompletitud, que demostramos en las Proposiciones 5.16 y 5.20 nos hacen ver que no es así, que hay teorías en las que encontraremos fórmulas que no son decidibles.

A lo largo del Capítulo 3 estudiamos la aritmética de Peano, S y pudimos concluir que en S se puede axiomatizar todos los conceptos que conocemos de los números naturales $\mathbb{N}$ en la metateoría. Así como definimos dentro de S conceptos como $a < b$ o $a \mid b$ relacionándolos con objetos dentro del lenguaje $\mathscr{L}_A$ de S, se pueden seguir definiendo y encontrando distintas propiedades de los naturales, como la exponenciación. Así podemos ir construyendo teorías que tomen como base a S. En el Corolario 2 vimos que S es una teoría con igualdad.

La mayoría del desarrollo del Capítulo 4 estuvo enfocado en llegar a la Proposición 4.16, así todas las funciones recursivas son representables en S, es decir, que fue un resultado muy importante para poder realizar las pruebas de incompletitud. También por el Corolario 3 vimos que toda relación recursiva es expresable en S.

El objetivo del Capítulo 5 era poder demostrar que una teoría como S, en la que la aritmética de los números naturales es válida, no es una teoría completa, y así lo probamos. Las observaciones 5.6 y 5.7 nos permitieron observar que S tiene un lenguaje primitivo recursivo y un conjunto de axiomas primitivo recursivo. Gracias a esto en S tenemos una larga lista de funciones y relaciones recursivas dadas por las proposiciones 5.6, 5.7 y 5.9, que más aún, son representables y expresables dentro de S. También son resultados muy importantes los Corolarios 4 y 5 pues gracias al primero observamos que en S, si asumimos su consistencia, la clase de las funciones recursivas coincide con la clase de las funciones representables, es decir, encontramos una caracterización de las funciones recursivas. Resaltamos la importancia tanto del lema de diagonalización (Proposición 5.11) como del Teorema del punto fijo (Proposición 5.12), pues estos nos sirven como preámbulo para la construcción de las sentencias de Gödel que son fundamentales en la prueba del primer Teorema.

Por último, sabiendo que hay pruebas de la $\omega-$ consistencia de S, la Proposición 5.14 nos implicaría que S es consistente. Así, gracias al Primer Teorema de incompletitud (Proposición 5.16) ya sabemos que es imposible que S sea una teoría completa pese al esfuerzo que se hizo por axiomatizarla de manera precisa. El Segundo Teorema de incompletitud (Proposición 5.20) nos asegura que por más que se intente, no podemos probar la consistencia de S dentro de la teoría, así, las pruebas que haya de su consistencia u $\omega-$consistencia tienen que emplear herramientas de la metateoría.

Pese a que se han demostrado los teoremas de incompletitud de Gödel, no debemos de alarmarnos y pensar que las matemáticas siempre han estado equivocadas. Simplemente estos teoremas nos han abierto los ojos para dejar de pensar en que es necesario que las matemáticas son completas, y nos han abierto las puertas a seguir valiéndonos de otras herramientas y conocimientos para resolver las problemáticas que nos vengan en el futuro.

Bibliografía

[1] Elliott Mendelson. *Introduction to mathematical logic.* Chapman y Hall/CRC, 2015.

[2] Alan G Hamilton. *Logic for mathematicians.* Cambridge University Press, 1988.

[3] Víctor López Martínez y Carlos Gómez Ambrosi. "El Teorema de Incompletitud de Gödel". Tesis de fin de Grado. Zaragoza, España: Universidad Zaragoza, jun. de 2016.

[4] Neal Koblitz. *A course in number theory and cryptography.* Vol. 114. Springer Science & Business Media, 1994.

[5] George Boolos. *The logic of provability.* Cambridge University Press, 1995.

[6] Claudio Gutiérrez. "El Teorema de Incompletitud de Gödel (Versión para no iniciados)". En: *Revista Cubo Mat. Educ.* 1 (1999), págs. 68-75.

[7] Matthias Baaz, Christos H Papadimitriou, Hilary W Putnam, Dana S Scott y Charles L Harper Jr. *Kurt Gödel and the foundations of mathematics: Horizons of truth.* Cambridge University Press, 2011.