Universidad Autónoma del Estado de Hidalgo

Instituto de Ciencias Básicas e Ingenierías
Área Académica de Matemáticas y Física

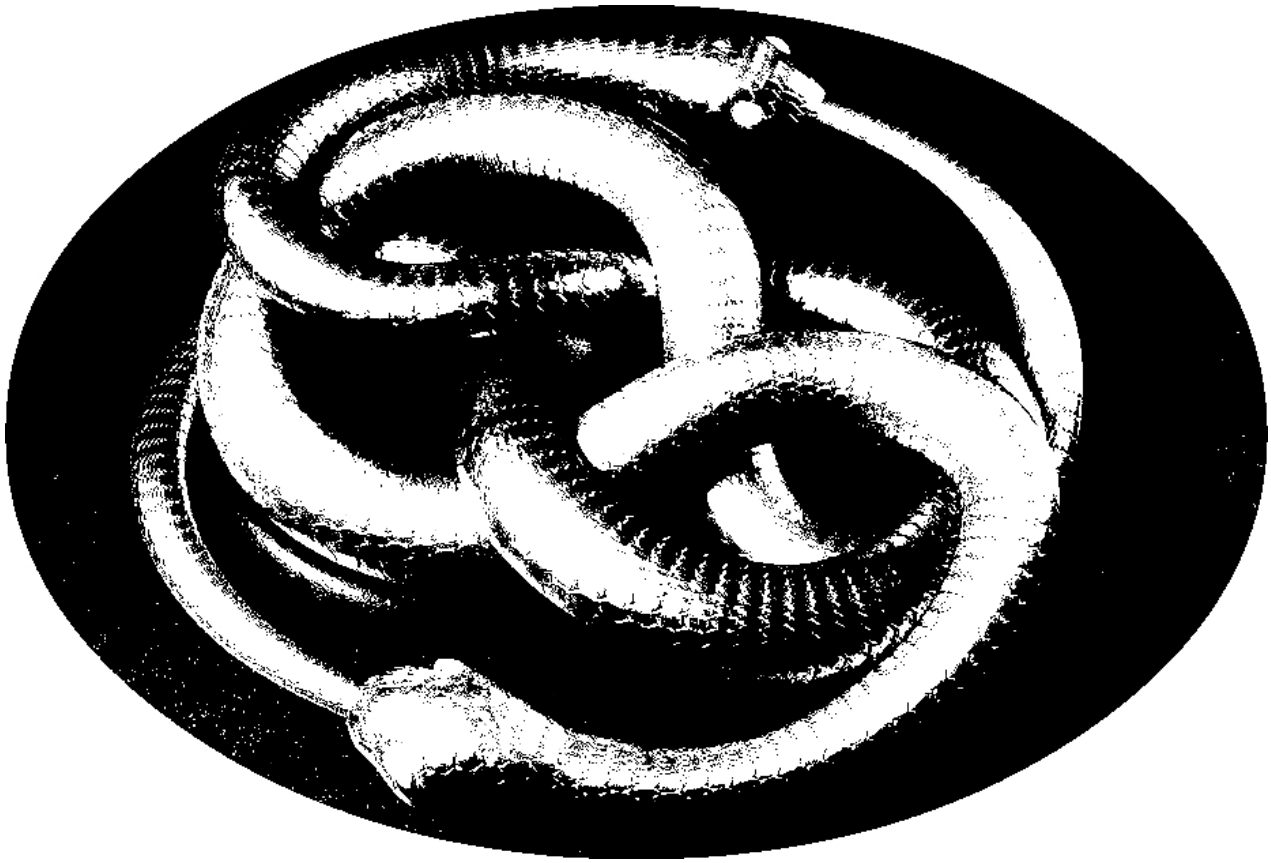
ARITMÉTICA DE PEANO EN LÓGICA DE PRIMER ORDEN Y PROPIEDADES DE SUS MODELOS NUMERABLES

Tesis que para obtener el título de:
Licenciado en Matemáticas Aplicadas

presenta:
Norberto Javier Rivas González

bajo la dirección de:
Ricardo Cruz Castillo

Pachuca de Soto, Hidalgo.
Verano, 2016



ℵ$_{\vee}$r$\beta\exists\mathcal{R}\top\emptyset$ ℶ. R$_{\mathbb{A}}$

Without mathematics one cannot fathom the depths of philosophy,
without philosophy one cannot fathom the depths of mathematics;
without the two, one cannot fathom anything.

(Bordas-Demoulins)

All our knowledge begins with the senses, proceeds
then to the understanding, and ends with reason.
There is nothing higher than reason.

(Kant)

Se puede tener por compañera la fantasía,
pero se debe tener como guía a la razón.

(Dr. Johnson)

Abstract

Starting from the definition of arithmetic model, i.e., a set with two operations which validate each Peano's axiom translated to the first order, this work aims to show that besides the usual arithmetic (that of the natural numbers with their usual addition and multiplication operations), there exist other sets endowed with their own operations which are models to Peano's axioms as well. After proving the existence of them, we will delve in some aspects which are inherent to all arithmetic models, and others that are exclusive to countable ones. Also, the first chapter of preliminaries includes concepts and basic theorems that are considered necessary to better understand the results presented on this thesis.

Resumen

Este trabajo tiene por objetivo partir de la definición de modelo aritmético, esto es, un conjunto y un par de operaciones que validen a cada axiomas de Peano traducido a primer orden y mostrar que, además de la aritmética usual (el conjunto de los números naturales junto a la suma y producto usuales), existen otros conjuntos, dotados de sus propias operaciones, que continúan siendo modelos para estos axiomas. Luego de mostrar su existencia, se ahondará en algunos aspectos que son inherentes a todos los modelos aritméticos y otros exclusivos de los numerables. El texto contiene también un primer capítulo de preliminares a fin de exponer los conceptos y teoremas básicos, considerados necesarios para el buen entendimiento de los resultados presentados en la tesis.

Agradecimientos

En primer lugar quiero agradecer a Ricardo, quien me mostró estos senderos de la matemática y me alentó a caminar en ellos. También a los compañeros, profesores, colegas y amigos que he conocido a lo largo de la licenciatura, pues me han ayudado a crecer no solamente en el aspecto matemático. Agradezco a los miembros del jurado por revisar la tesis y hacer observaciones que ayudaron a mejorarla.

Gracias a la familia, la cual apoyó bastante dejándome ser; en especial a mi padre, quien me habló de libertad. Y gracias a Ahn, por su inefable cariño.

A las circunstancias.

Índice general

Introducción

La lógica, como rama de la matemática, pretende modelar el razonamiento que se ocupa al hacer y estudiar esta ciencia. Así, puede pensarse que la lógica es un intento por formalizar algunos de los conceptos naturales utilizados en cualquiera de sus ramas, tales como la idea intuitiva de *demostración* y la noción de *verdadero*, entre otras.

Es un hecho que el pensamiento humano es lo suficientemente amplio y desconocido como para abarcarlo todo en una sola teoría científica, en particular, la forma de razonar es demasiado compleja para sintetizarla en una única lógica, así, dentro de esta rama aparecen numerosos y diversos tipos de lógica que se enfocan en algún aspecto particular del razonamiento. Uno de los más básicos, y quizá el más cercano a la forma *sencilla* de pensar en la matemática, es la lógica de primer orden (o lógica de predicados) la cual abarca las nociones de *variable*, *constante*, *cuantificador*, *igualdad*, *relación*, *función*, etc. La ventaja de utilizarla como eje de estudio es que gran parte de la matemática se puede trasladar a esta lógica y es, a su vez, no tan compleja como para obtener de ella una rica teoría llena de resultados interesantes. Hay que mencionar la principal gracia (y desgracia) de está lógica; ocurre que este *traslado* de la matemática dentro de la lógica de predicados conlleva cierta pérdida de propiedades, esto debido a su capacidad expresiva pues, si bien puede cuantificar sobre variables (por ejemplo, dentro de ella se puede expresar la frase «para todo número par n mayor que 2 existen números primos p y q tales que $n = p + q$») no puede hacer cuantificación sobre conjuntos o funciones (por ejemplo, no puede reproducir la frase «todo subconjunto no vacío y acotado de números reales tiene un supremo»). Es por ello que, al traducir este tipo de frases (como el *principio de inducción* en los axiomas de Peano, el cual se muestra en el capítulo segundo), aparecen ciertas *irregularidades* que son el punto de partida para la existencia de *estructuras* que seguirán haciendo válidos ciertos axiomas (como los de Peano, por ejemplo) pero que no son *isomorfos* al *modelos* usual (conocido también como *modelos estándar*).

Es importante esclarecer un aspecto de la lógica. No ocurre que la lógica es una rama privilegiada que carga sobre sus hombros a toda la matemática y que de ella depende toda la veracidad de lo que se realiza en las demás; sino que, como ya se ha mencionado, es solo una rama más cuyo objetivo es modelar (no fundamentar) el pensamiento humano que se ocupa dentro de la matemática. Es por ello que se basa en otras teorías para poder presentar y dar sustento a sus resultados, la parte más importante de esto es la teoría de conjuntos clásica denotada por ZFC[1]. Es decir, definiciones importantes para el estudio de la lógica (tales como *proposiciones* o *estructura*) son en sí elementos de ZFC, es decir, conjuntos. Es por ello que la notación utilizada y las nociones de *conjunto*, *relación* y *función*, entre otras, harán referencia a los conceptos dentro de la teoría de conjuntos[2].

[1] En sí, ZFC es el conjunto de axiomas del cuál parte esta teoría, pero suele referirse a ella de esta manera. Estos axiomas se presentan en el apéndice A.

[2] Se pueden consultar las definiciones, notaciones y resultados de ZFC usados a lo largo del texto en el apéndice A.

El objetivo particular de este escrito es lograr un material introductorio[3], formal y a la vez suficientemente completo (un motivo más para la anexión del primer capítulo) que hable sobre los aspectos básicos de la aritmética de Peano en lógica de primer orden, además de ampliar este tema hacia aspectos específicos como el orden (sección 2.3) y la recursión (sección 2.5) sin presentar demasiada notación y resultados que, si bien son importantes para continuar ampliando el estudio, son irrelevantes para lo que esta tesis quiere abarcar. Este deseo nace, en parte, por observar que algunos textos importantes de lógica hacen poca mención del tema (por ejemplo, [18] solo le dedica un par de páginas) y otros, específicos del tema, ahondan tanto que es complicado entender los teoremas importantes de manera sencilla pues su demostración necesita más teoría de la que se pretende mostrar aquí (como en [12], en donde se realiza un estudio profundo y exhaustivo del tema). Algunas demostraciones presentadas a lo largo del trabajo están basadas en las consultadas de la bibliografía, aún así muchas de ellas fueron modificadas o completadas para adaptarse al contexto.

[3]Como en [17], un artículo introductorio del tema donde se mencionan algunos resultados importantes.

Capítulo 1

Preliminares

En este primer capítulo se presentan las nociones, definiciones, teoremas y demás conceptos básicos, elementales y necesarios para el buen entendimiento del desarrollo y objetivo de este texto; por ende, el motivo principal es mostrar un panorama general, amplio y didáctico para poder empaparse con las ideas fundamentales de este estudio, por esta razón se evitarán las partes técnicas y demás contenido que, aunque importante, es irrelevante para lo que aquí se presenta. A fin de lograr esto, se omitirán prácticamente todas las demostraciones de los resultados que se enunciarán, y se presentarán varios ejemplos que ayuden a una mejor comprensión de los conceptos poco conocidos (o quizá desconocidos) de la lógica matemática; además de tener numerosos pies de página que servirán para hacer algunas aclaraciones.

La idea que incitó a la anexión de este capítulo es el hecho de que, a diferencia de otras ramas matemáticas como el cálculo o el álgebra, la lógica no es una asignatura común en la licenciatura de matemáticas y, por tanto, probablemente poco conocida entre la comunidad.

Las secciones y contenido de estos preliminares están fuertemente basados en [18, cap. 2 y cap. 3]. Otro texto donde se pueden consultarse estos temas es [15].

1.1. Lógica proposicional

La lógica proposicional, también llamada lógica de orden cero, es lo que se puede llamar *estudio clásico de la lógica*; se puede decir que en ella se representan algunas oraciones no ambiguas[1] (las llamadas *proposiciones*) que luego se pueden unir a otras mediante conectivos para formar nuevas oraciones más complejas. Por ejemplo, mediante el símbolo «p» se denota a la oración «π es un número trascendente», y mediante el símbolo «q» a la oración «hoy hay luna llena». Una manera de unir estas oraciones es mediante el *conectivo y*, se formaría entonces la oración «π es un número trascendente y hoy hay luna llena», la cual se representará por el símbolo «$p \wedge q$». Otro ejemplo es formar con ellas una oración condicional como «si hoy hay luna llena, entonces π es un número trascendente», representada por «$q \to p$». Además de formar nuevas oraciones interesa el estudio de su veracidad; así, se puede decir que p es verdadera y que la veracidad de q depende del día en cuestión. Uno puede notar que la veracidad de las oraciones complejas (por ejemplo $p \wedge q$ y $q \to p$) dependen de la veracidad de las partes que las constituyen, esto se verá formalmente reflejado más adelante.

Para formalizar estas ideas se procederá en dos niveles, primero se definirá un lenguaje formal, esencial para el estudio de la lógica, para después especificar la manera de decidir cuando una proposición es *válida*.

[1] Un ejemplo de oración no válida es: *Yo miento*.

1.1.1. Sintáctica

Definición 1.1.1. *El* alfabeto *de la lógica proposicional consta de los siguientes símbolos.*

I. *Símbolos proposicionales (numerables):* p_0, p_1, p_2, ...

II. *Conectivos:* $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, $\neg$, $\bot$.

III. *Símbolos auxiliares* (,).

Se ocupó un color de texto diferente para distinguir entre los símbolos que constituirán el lenguaje formal de la lógica y los símbolos que se ocupan en el lenguaje común o informal, el *meta-lenguaje*, necesario para la comunicación humana. Esta diferencia, sutil y aparentemente innecesaria, es un aspecto importante para el entendimiento profundo del estudio. En ocasiones se usará esta distinción en el texto para enfatizar su naturaleza formal, aún así, se puede distinguir entre el lenguaje formal y el meta-lenguaje de acuerdo al contexto.

Se darán algunas aclaraciones de la definición anterior, primero, la cantidad de símbolos proposicionales es, como se indica, numerable[2] y cada uno de ellos está indizado con un número natural (se adoptará la convención, como en ZFC, de que 0 es el primer número natural), los únicos símbolos auxiliares son paréntesis, además, los conectivos poseen nombres tradicionales:

- $\wedge$ - **conjunción**.
- $\vee$ - **disyunción**.
- $\rightarrow$ - **implicación**.
- $\leftrightarrow$ - **doble implicación**.
- $\neg$ - **negación**.
- $\bot$ - **falso**.

Al conectivo $\bot$ y a los símbolos proposicionales (p_i) se les llamará **átomos**.

Se puede pensar que el alfabeto es el conjunto formado por todas las posibles «concatenaciones» (finitas) de los símbolos introducidos en la definición 1.1.1. Más formalmente, si S es el conjunto de estos símbolos (es decir, $S = \{$ (,), $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, $\neg$, $\bot$, p_0, p_1, ... $\}$) entonces el alfabeto para la lógica de orden cero es el conjunto[3] $Alph_0 = S^{<\omega}$ en donde, en lugar de ocupar la notación de sucesión finita (es decir, la notación para $n-$adas de elementos), solo se colocarán en ese orden los símbolos que la conforman (por ejemplo, $(p_0 \vee \neg p_0)$ en lugar de $((, p_0, \vee, \neg, p_0,))$). Ahora bien, este conjunto contiene «palabras basura», en el sentido de que se desea que símbolos como el del ejemplo sí sean parte del lenguaje y símbolos como $p_0)(p_0\neg\vee$ no lo sean (pues estos últimos no representan oraciones matemáticas del meta-lenguaje). Por tal motivo se «depura» al conjunto $Alph_0$ definiendo al conjunto de *proposiciones* (siguiente definición) y se olvidan los demás símbolos del alfabeto. A fin de simplificar la comunicación se usarán letras griegas minúsculas, tales como σ, φ y ψ, como meta-variables para elementos del lenguaje, las cuales no son parte del mismo, sino símbolos del meta-lenguaje utilizados para hacer referencia a elementos del lenguaje formal (así por ejemplo, φ puede ser $p_9 \rightarrow \neg p_9$ o $\bot\bot\bot$). Para este mismo fin se dejará de usar, por ahora, un color diferente para los elementos del lenguaje formal.

[2] En teoría de conjuntos, un conjunto es *numerable* si existe una función biyectiva de éste a $\mathbb{N}$, es decir, «tiene tantos elementos como números naturales».

[3] La notación $X^{<\omega}$ se refiere al conjunto de todas las sucesiones finitas en X, es decir, $X^{<\omega} = \bigcup_{n\in N} X^n$. Ver A.3.7.

Definición 1.1.2. *El conjunto* PROP*, de* proposiciones*, es el conjunto X más pequeño con las siguientes propiedades.*

I. $p_i \in X$ *para cada* $i = 0, 1, 2, \ldots$ *y* $\bot \in X$.

II. *Si* $\varphi, \psi \in X$ *entonces* $(\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \to \psi), (\varphi \leftrightarrow \psi) \in X$.

III. *Si* $\varphi \in X$ *entonces* $(\neg\varphi) \in X$.

La existencia de PROP se sigue de la existencia de $Alph_0$ puesto que éste lo contiene. A manera de ejemplo, se mostrará que $\sigma_1 = (p_0 \wedge p_9) \to \bot$ es una proposición, mientras que $\sigma_2 = \neg\neg\bot$ no lo es.

Por la parte uno de la definición se tiene que p_0, p_9 y $\bot$ están en PROP; así, por la parte dos, se tiene que $(p_0 \wedge p_9)$ también lo está, luego, por el mismo motivo, σ_1 es una proposición. En general, para mostrar que una cierta cadena de símbolos del alfabeto es una proposición (pertenece a PROP), basta verificar si su construcción está basada en la definición 1.1.2.

Por otro lado, mostrar que σ_2 no está en PROP lleva a otro tipo de argumento. Se actúa por contradicción, es decir, se supone que $\neg\neg\bot \in$ PROP. Claim: $X = \text{PROP} \setminus \{\neg\neg\bot\}$ cumple las condiciones de la definición 1.1.2, eso bastará para llegar a una contradicción. Dado que $p_i, \bot \in$ PROP entonces $p_i, \bot \in X$, luego, es claro[4] que $\neg\neg\bot$ no es de la forma $(\varphi\Box\psi)$ para algunos φ y ψ donde $\Box$ representa[5] a cualquiera de los símbolos $\wedge$, $\vee$, $\to$ o $\leftrightarrow$; por esta razón, el conjunto X cumple la condición dos. De la misma manera X satisface la última condición puesto que $\neg\neg\bot$ no es de la forma[6] $(\neg\varphi)$ para alguna φ.

Se puede mostrar que las proposiciones poseen ciertas meta-propiedades, esto es, propiedades que son enunciadas en el meta-lenguaje; por ejemplo, retomando que se pueden pensar como concatenaciones de símbolos, una meta-propiedad es que son finitas y esto es aplicable sin necesidad de definir *finito* en el lenguaje formal. El uso de estas propiedades es bastante útil para la lógica, ya que permite discernir cualidades y características de los objetos en este estudio. Si A es una meta-propiedad se ocupa el símbolo $A(\varphi)$ para cuando φ posea la propiedad descrita por A. Para mostrar que todas las proposiciones poseen cierta meta-propiedad se procede de «manera inductiva», es decir, se mostrará primero que los átomos tienen la propiedad y luego se ocupará esto para mostrar que las más complejas también poseen la propiedad aprovechando el hecho de que están formadas por átomos de acuerdo a las reglas de la definición 1.1.2. Esto se formaliza en el siguiente teorema.

Teorema 1.1.3. Principio de inducción. *Sea* A *una meta-propiedad, si ocurre que*

- $\mathrm{A}(p_i)$ *para cada* $i = 0, 1, 2, \ldots$ *y* $\mathrm{A}(\bot)$,
- *si* $\mathrm{A}(\varphi)$ *y* $\mathrm{A}(\psi)$ *entonces* $\mathrm{A}((\varphi\Box\psi))$, *y*
- *si* $\mathrm{A}(\varphi)$ *entonces* $\mathrm{A}((\neg\varphi))$;

entonces $\mathrm{A}(\varphi)$ *se tiene para toda* $\varphi \in$ PROP.

Demostración. Sea $X = \{\varphi \in \text{PROP} \ : \ \mathrm{A}(\varphi)\}$, por las hipótesis del teorema se tiene que X satisface las condiciones de la definición 1.1.2, así, PROP $\subseteq X$, es decir, $\mathrm{A}(\varphi)$ se tiene para toda $\varphi \in$ PROP. □

Utilizando el principio de inducción se puede mostrar, por ejemplo, que cualquier proposición tiene un número par de paréntesis. A fin de simplificar la notación no se usarán paréntesis en el lenguaje, a menos que sean necesarios para evitar ambigüedad, utilizando la convención de que $\wedge$ y $\vee$ tienen mayor

[4] Es claro si se recuerda que éstos símbolos se pueden tratar como sucesiones finitas.
[5] El símbolo $\Box$ funge como una meta-variable para algunos conectivos del lenguaje.
[6] Es importante el uso de los paréntesis, ya que $\neg\neg\bot$ es diferente a $(\neg(\neg\bot))$, este último sí es un elemento de PROP.

jerarquía que $\to$ y $\leftrightarrow$ (de manera similar al uso de paréntesis con los símbolos $+$ y $\cdot$), y que $\neg$ es más fuerte que los demás. Por ejemplo, en lugar de ocupar la proposición $((\varphi \wedge (\neg\psi)) \to \bot)$ se ocupará el símbolo $\varphi \wedge \neg\psi \to \bot$, y en lugar de $(\varphi \to (\varphi \vee (\psi \to \sigma)))$ se ocupará $\varphi \to \varphi \vee (\psi \to \sigma)$. Las abreviaciones no son, en un sentido estricto, proposiciones.

1.1.2. Semántica

Como se mencionó al principio de este capítulo, interesa tener una forma de decidir cuándo una proposición es verdadera y, como se observó, ésta debe depender de las partes atómicas que la forman. La *semántica* es la parte de la lógica que se encarga de interpretar las proposiciones, a diferencia de la *sintáctica* donde importa la buena formación de éstas sin preocuparse por su significado. En esta sección se estudiará entonces la semántica de la lógica de predicados. Para comenzar se utilizará la idea de las llamadas *tablas de verdad*.

Retomando el ejemplo en el primer párrafo del capítulo, se consideran las oraciones representadas por p y q; además, se adopta la tradicional notación de usar 1 y 0 en lugar de *verdadero* y *falso* respectivamente. A continuación, se muestra la tabla de verdad de algunas oraciones formadas a partir de estas proposiciones.

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \to q$	$p \leftrightarrow q$	$\neg(p \wedge \neg q) \to p$	$(\neg p \vee q) \to ((p \wedge \neg p) \to q)$
0	0	1	0	0	1	1	0	1
0	1	1	0	1	1	0	0	1
1	0	0	0	1	0	0	1	0
1	1	0	1	1	1	1	1	1

Cuadro 1.1: Ejemplo de una tabla de verdad.

Entonces, se puede interpretar la cuarta columna como «π es un número trascendente y hoy hay luna llena» y así las demás, siendo las últimas dos más complicadas, por ejemplo, la penúltima sería «si π no es un número trascendente y hoy no hay luna llena, entonces π es un número trascendente». Como se observa, la veracidad de cada una de éstas depende del valor que tenga cada átomo y se nota que la asignación de valores es acorde a lo que se espera, así, la única manera de que una conjunción sea verdad es que ambas partes los sean, una disyunción es verdad si al menos una de las partes lo es, una implicación es falsa solo cuando el antecedente es verdadero y la conclusión falsa, etc. Estas ideas intuitivas se definen formalmente mediante las llamadas *valuaciones*.

Definición 1.1.4. *Una función* $v : \mathrm{PROP} \to \{0, 1\}$ *es una* valuación *si cumple lo siguiente.*

I. $v(\varphi \wedge \psi) = \mathrm{mín}\{v(\varphi), v(\psi)\}$.

II. $v(\varphi \vee \psi) = \mathrm{máx}\{v(\varphi), v(\psi)\}$.

III. $v(\varphi \to \psi) = \mathrm{máx}\{1 - v(\varphi), v(\psi)\}$.

IV. $v(\varphi \leftrightarrow \psi) = 1 - |v(\varphi) - v(\psi)|$.

V. $v(\neg\varphi) = 1 - v(\varphi)$.

VI. $v(\bot) = 0$.

Dada esta definición, si una valuación está dada solo en los átomos entonces es posible extenderla, de manera única, a todas las proposiciones[7]. Dada una valuación v, se ocupará la notación $[\![\varphi]\!]_v$ en lugar de $v(\varphi)$. Además, se dirá que φ es *verdadera* (resp. *falsa*) bajo v si $[\![\varphi]\!]_v = 1$ (resp. $[\![\varphi]\!]_v = 0$). Ahora se definen dos importantes conceptos, el primero, que se llamará *tautología*, es la propiedad de una proposición de ser verdadera bajo cualquier valuación, se puede decir que es siempre verdadera; la otra es una manera de relacionar conjuntos de proposiciones con proposiciones.

Definición 1.1.5. *Sea φ una proposición y Γ un conjunto de proposiciones.*

I. *φ es una* tautología *(denotado por $\vDash \varphi$) si $[\![\varphi]\!]_v = 1$ para toda valuación v.*

II. φ es una consecuencia semántica de Γ *(denotado por $\Gamma \vDash \varphi$) si para toda valuación v se cumple que, si $[\![\psi]\!]_v = 1$ para todo $\psi \in \Gamma$, entonces $[\![\varphi]\!]_v = 1$.*

En palabras, $\Gamma \vDash \varphi$ se tiene si y solo si φ es verdadera bajo todas aquellas valuaciones que hacen verdaderas todas las proposiciones de Γ. La notación $\Gamma \nvDash \varphi$ hará referencia a que $\Gamma \vDash \varphi$ no es el caso, es decir, φ no es consecuencia semántica de Γ, lo que significa que existe una valuación v tal que $[\![\psi]\!]_v = 1$ para todo $\psi \in \Gamma$ y $[\![\varphi]\!]_v = 0$.

Algunos ejemplos de tautologías y consecuencias semánticas:

- $\vDash \varphi \to \varphi$
- $\vDash \varphi \vee \psi \leftrightarrow \psi \vee \varphi$
- $\{\varphi, \psi\} \vDash \varphi \wedge \psi$
- $\{\varphi, \varphi \to \psi\} \vDash \psi$

El primero de ellos se puede interpretar en el meta-lenguaje como «siempre es cierto que una proposición se implica a ella misma» o el último como «siempre que las proposiciones φ y $\varphi \to \psi$ sean ciertas, entonces ψ es cierta». Ahora se definirá otro artilugio muy usual en la matemática y es el sustituir proposiciones por átomos dentro de una proposición; esta definición, como aquellas que establecen algo para todas las proposiciones, se hace por recursión.

Definición 1.1.6. *Sean $\varphi, \psi, \varphi_1, \varphi_2$ proposiciones y p_i un átomo.*

I. $\varphi[\psi/p_i] = \begin{cases} \varphi, & \text{si } \varphi \text{ es un átomo y } \varphi \neq \psi; \\ \psi, & \text{si } \varphi = p_i. \end{cases}$

II. $(\varphi_1 \square \varphi_2)[\psi/p_i] = \varphi_1[\psi/p_i] \square \varphi_2[\psi/p_i]$

III. $(\neg\varphi)[\psi/p_i] = \neg\varphi[\psi/p_i]$

Se dirá que las proposiciones φ, ψ son *equivalentes* si $\vDash \varphi \leftrightarrow \psi$. El siguiente teorema establece una propiedad en las sustituciones con relación a las proposiciones equivalentes; el cual, interpretado, dice que se pueden reemplazar partes de una proposición por partes equivalentes. Su demostración se encuentra en [18, pág. 19].

Teorema 1.1.7. Teorema de sustitución. *Sean $\psi, \varphi_1, \varphi_2$ proposiciones y p un átomo, si se tiene que $\vDash \varphi_1 \leftrightarrow \varphi_2$ entonces $\vDash \psi[\varphi_1/p] \leftrightarrow \psi[\varphi_2/p]$*

[7] El sustento de este hecho, y de otros posteriores, es el llamado teorema de definición por recursión, el cual es un resultado técnico que puede consultarse junto con su demostración en [18, pág. 10].

El teorema de sustitución, aunque poderoso, está limitado a realizar sustituciones sobre los átomos; a veces, interesará realizar sustituciones sobre proposiciones más complejas. Por ejemplo, se sabe por un teorema anterior que $\varphi \vee \psi$ es equivalente a $\psi \vee \varphi$, ahora, en $\sigma \to (\varphi \vee \psi)$ se quiere realizar la respectiva sustitución y obtener el mismo valor de verdad; como $\varphi \vee \psi$ no es un átomo el teorema anterior no procede, sin embargo, el resultado se puede extender a uno más general que involucra el caso citado (para hacerlo se necesita, claramente, una nueva definición de sustitución) cuya demostración es análoga a la del anterior. El teorema resultante se enuncia de igual manera salvo la restricción de los átomos, aún así, es demasiado técnico para los propósitos de esta sección. En adelante, cuando se mencione el teorema de sustitución se hará uso de la versión general.

Una manera eficaz, aunque no siempre conveniente, para mostrar que alguna proposición es una tautología es utilizar las tablas de verdad; en este caso, la condición de que en la correspondiente columna haya únicamente símbolos de verdad (unos) es necesaria y suficiente para que ésta sea una tautología. El fundamento de esto se basa en que, dada la definición, el valor de verdad de una proposición depende solamente de las partes que la constituyen.

Teorema 1.1.8. *Sean φ, ψ, σ proposiciones, las siguientes son tautologías.*

- *Asociatividad:*

  $(\varphi \wedge \psi) \wedge \sigma \;\leftrightarrow\; \varphi \wedge (\psi \wedge \sigma)$

  $(\varphi \vee \psi) \vee \sigma \;\leftrightarrow\; \varphi \vee (\psi \vee \sigma)$

- *Conmutatividad:*

  $\varphi \wedge \psi \;\leftrightarrow\; \psi \wedge \varphi$

  $\varphi \vee \psi \;\leftrightarrow\; \psi \vee \varphi$

- *Distribución:*

  $\varphi \wedge (\psi \vee \sigma) \;\leftrightarrow\; (\varphi \wedge \psi) \vee (\varphi \wedge \sigma)$

  $\varphi \vee (\psi \wedge \sigma) \;\leftrightarrow\; (\varphi \vee \psi) \wedge (\varphi \vee \sigma)$

- *Leyes de De Morgan:*

  $\neg(\varphi \wedge \psi) \;\leftrightarrow\; \neg\varphi \vee \neg\psi$

  $\neg(\varphi \vee \psi) \;\leftrightarrow\; \neg\varphi \wedge \neg\psi$

- *Ley de doble negación:*

  $\neg\neg\varphi \;\leftrightarrow\; \varphi$

A manera de ejemplo, se demostrará una de éstas utilizando el método de las tablas de verdad.

φ	ψ	$\neg\varphi$	$\neg\psi$	$\varphi \wedge \psi$	$\neg(\varphi \wedge \psi)$	$\neg\varphi \vee \neg\psi$	$\neg(\varphi \wedge \psi) \leftrightarrow \neg\varphi \vee \neg\psi$
0	0	1	1	0	1	1	1
0	1	1	0	0	1	1	1
1	0	0	1	0	1	1	1
1	1	0	0	1	0	0	1

Cuadro 1.2: Ejemplo de una demostración utilizando tablas de verdad.

El siguiente teorema muestra algunas proposiciones equivalentes, con las cuales se pueden «definir» todos los demás conectivos lógicos en términos de solo dos, ya sea de $\{\vee, \neg\}$, de $\{\to, \neg\}$, de $\{\wedge, \neg\}$ o de $\{\to, \bot\}$.

Teorema 1.1.9. *Sean φ, ψ proposiciones, se cumple lo siguiente.*

a) $\vDash (\varphi \leftrightarrow \psi) \ \leftrightarrow \ (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$

b) $\vDash (\varphi \rightarrow \psi) \ \leftrightarrow \ (\neg\varphi \vee \psi)$

c) $\vDash \varphi \vee \psi \ \leftrightarrow \ (\neg\varphi \rightarrow \psi)$

d) $\vDash \varphi \vee \psi \ \leftrightarrow \ \neg(\neg\varphi \wedge \neg\psi)$

e) $\vDash \varphi \wedge \psi \ \leftrightarrow \ \neg(\neg\varphi \vee \neg\psi)$

f) $\vDash \neg\varphi \ \leftrightarrow \ (\varphi \rightarrow \bot)$

g) $\vDash \bot \ \leftrightarrow \ \varphi \wedge \neg\varphi$

Como se mencionó anteriormente, las tablas de verdad pueden ser una útil ayuda para determinar si una proposición es o no una tautología, sin embargo, como se puede observar, este procedimiento tiene la desventaja de ser amplio en proposiciones complejas (por ejemplo, para $(\varphi_1 \wedge \varphi_2 \rightarrow (\neg\psi \vee \sigma)) \vee (\varphi_1 \vee \varphi_2 \rightarrow \psi) \leftrightarrow \neg\sigma \vee \varphi_3 \vee \varphi_1$ se necesita una tabla con 2^5 renglones, lo cual desemboca en un problema computacional). Luego, se puede actuar por otro tipo de demostración usando cálculos algebraicos, esto es, utilizar los anteriores teoremas (cuya demostración se pude hacer sin problema utilizando tablas de verdad) para establecer una cadena de equivalencias hasta obtener el resultado. La siguiente es una prueba utilizando este método. Por conveniencia, solo en este ejemplo, se escribirá $\varphi \approx \psi$ en lugar de $\vDash \varphi \leftrightarrow \psi$.

Ejemplo 1.1.10. *Se cumple que* $\vDash (\varphi \rightarrow (\psi \rightarrow \sigma)) \leftrightarrow (\varphi \wedge \psi \rightarrow \sigma)$

Demostración. Se tiene la siguiente cadena de equivalencias.

$$\begin{aligned}
&\varphi \rightarrow (\psi \rightarrow \sigma) \approx \neg\varphi \vee (\psi \rightarrow \sigma) && \text{[Teorema anterior]}\\
&\neg\varphi \vee (\psi \rightarrow \sigma) \approx \neg\varphi \vee (\neg\psi \vee \sigma) && \text{[Mismo teorema y sustitución]}\\
&\neg\varphi \vee (\neg\psi \vee \sigma) \approx (\neg\varphi \vee \neg\psi) \vee \sigma && \text{[Teorema anterior, sustitución y asociatividad]}\\
&(\neg\varphi \vee \neg\psi) \vee \sigma \approx \neg(\varphi \wedge \psi) \vee \sigma && \text{[Asociatividad, leyes de De Morgan y sustitución]}\\
&\neg(\varphi \wedge \psi) \vee \sigma \approx (\varphi \wedge \psi \rightarrow \sigma) && \text{[Teorema anterior, leyes de De Morgan y sustitución]}
\end{aligned}$$

Por lo tanto, $\vDash \neg(\varphi \wedge \psi) \vee \sigma \leftrightarrow (\varphi \wedge \psi \rightarrow \sigma)$. □

Existe una buena cantidad de resultados semánticos muy interesantes que son de ayuda para empatar a la lógica con otros estudios de la matemática, sin embargo, están fuera de los propósitos de estos preliminares. Si se desea, se pueden consultar en [18, pág. 20-27].

1.1.3. Deducción natural

Hasta este momento se ha visto a la lógica desde el punto de vista semántico, donde la noción principal es la de verdad. Sin embargo ésta no es la única manera de tratarla, si se piensa en la lógica como una representación simbólica del razonamiento humano, principalmente el matemático, entonces uno puede preguntarse sobre un método de *inferencia* o *derivación*[8] que no utilize la noción de verdad.

Por tal motivo, en esta subsección se mostrará un enfoque no semántico de la lógica creando un conjunto de reglas que permitan concluir proposiciones a partir de otras dadas (llamadas *premisas*). Estas reglas, en su forma actual, fueron propuestas por G. Gentzen en la primera mitad del siglo XX (en [6]

[8] En este contexto, *inferir* es la acción de formular conclusiones a partir de premisas mediante reglas. Es la formalización de la noción matemática de *demostrar*.

y [7]) y representan la manera intuitiva que se ocupa para derivar conclusiones; por ejemplo se puede pensar en el siguiente escenario: la experiencia ha enseñado, y los hechos lo confirman, que siempre que cae una tormenta el cielo está nublado, esto se puede concentrar en la frase «si hay tormenta, entonces el cielo está nublado», ahora, en un típico día de agosto en el cual hay tormenta se tienen dos premisas: «si hay tormenta, entonces el cielo está nublado» y «hay tormenta», así nuestro *sistema natural de razonamiento* concluye que «el cielo está nublado»[9]. Un ejemplo más ahora en el contexto de la matemática: un teorema del cálculo afirma que toda función derivable es continua, esto es, «si una función f es derivable, entonces f es continua», ahora, es sabido que toda función polinomial es derivable, incluso se tiene una fórmula para encontrar dicha derivada, así «si f es un polinomio, entonces f es derivable», por último, $x^{18}+9x^2-2$ es un polinomio; entonces, usando *modus ponens* se tiene que $x^{18}+9x^2-2$ es derivable y, ocupando la misma regla, se concluye que $x^{18}+9x^2-2$ es una función continua.

Otra regla natural de inferencia es la conocida como *demostración por casos*. Se ilustrará esta regla mediante un ejemplo; primero se parte de una disyunción «todo primo p mayor o igual que 5 es congruente a 1 o a 2 módulo 3», se procede a suponer uno de los *casos* y se llega a una cierta conclusión «supongamos que p es congruente con 1 módulo 3, entonces $\cdots$ y así p^2 es congruente a 1 módulo 3», luego se parte del otro caso y se llega a misma conclusión «supongamos ahora que p es congruente con 2 módulo 3, entonces $\cdots$ y por lo tanto p^2 es congruente a 1 módulo 3», al final, se concluye con lo inferido en ambos casos «de todo lo anterior se sigue que p^2 es congruente a 1 módulo 3». De este ejemplo también se extrae algo muy importante en las demostraciones que es el hecho de suponer *temporalmente* algunas proposiciones, así, en cierto punto se supuso que «p es congruente a 1 módulo 3» y en otra parte que «p es congruente a 2 módulo 3», sin embargo, estas hipótesis no aparecen en la conclusión final, a este tipo de hipótesis se les llamará *hipótesis cancelables*. Estos nuevos términos se explicarán con detalle más adelante mediante algunos ejemplos.

Así, la deducción natural no es más que una manera formal y abstracta de representar, mediante reglas, el razonamiento natural que se ocupa para hacer demostraciones. A pesar de que este estudio se abstiene de interpretaciones, puesto que las proposiciones aquí carecen de significado alguno, es recomendable intentar empatar las siguientes definiciones y resultados con lo que se estudian en una licenciatura de matemática o, incluso, en la interacción cotidiana.

Las *derivaciones* se formaran de pequeños pasos consecutivos, que de hecho son las reglas que a continuación se establecerán, las cuales tienen una forma muy simple; a manera de ejemplo se muestra la regla del *modus ponens*:

$$\frac{\varphi \qquad \varphi \to \psi}{\psi}$$

Las proposiciones por arriba de la linea horizontal se conocen como *premisas*, la que está debajo como *conclusión*. Se observa que el *modus ponens* es una regla que «elimina» el conectivo implicación, sin embargo, también se pueden introducir conectivos. A continuación las reglas.

Reglas de conjunción.

$$\frac{\varphi \qquad \psi}{\varphi \wedge \psi}\ (\wedge \text{ I}) \qquad \frac{\varphi \wedge \psi}{\varphi}\ (\wedge \text{ E}) \qquad \frac{\varphi \wedge \psi}{\psi}\ (\wedge \text{ E})$$

[9] A esta *regla natural* de hacer inferencia se le conoce como *modus ponens*.

Reglas de disyunción.

$$\frac{\varphi}{\varphi \vee \psi}\ (\vee \text{ I}) \qquad \frac{\psi}{\varphi \vee \psi}\ (\vee \text{ I}) \qquad \frac{\varphi \vee \psi \qquad \begin{array}{c}[\varphi]\\ \vdots\\ \sigma\end{array} \qquad \begin{array}{c}[\psi]\\ \vdots\\ \sigma\end{array}}{\sigma}\ (\vee \text{ E})$$

Reglas de implicación.

$$\frac{\begin{array}{c}[\varphi]\\ \vdots\\ \psi\end{array}}{\varphi \to \psi}\ (\to \text{ I}) \qquad \frac{\varphi \qquad \varphi \to \psi}{\psi}\ (\to \text{ E})$$

Reglas de doble implicación.

$$\frac{\begin{array}{cc}[\varphi] & [\psi]\\ \vdots & \vdots\\ \psi & \varphi\end{array}}{\varphi \leftrightarrow \psi}\ (\leftrightarrow \text{ I}) \qquad \frac{\varphi \qquad \varphi \leftrightarrow \psi}{\psi}\ (\leftrightarrow \text{ E}) \qquad \frac{\psi \qquad \varphi \leftrightarrow \psi}{\varphi}\ (\leftrightarrow \text{ E})$$

Reglas de negación.

$$\frac{\begin{array}{c}[\varphi]\\ \vdots\\ \bot\end{array}}{\neg\varphi}\ (\neg \text{ I}) \qquad \frac{\varphi \qquad \neg\varphi}{\bot}\ (\neg \text{ E})$$

Reglas del falso.

$$\frac{\bot}{\varphi}\ (\bot) \qquad \frac{\begin{array}{c}[\neg\varphi]\\ \vdots\\ \bot\end{array}}{\varphi}\ (\text{RAA})$$

La etiqueta que se coloca a la derecha de las reglas codifica su nombre, por ejemplo «($\wedge$ I)» representa «(introducción de la conjunción)» y «($\neg$ E)» a «(eliminación de la negación)». Los puntos suspensivos significan que puede haber una derivación entre la proposición de arriba y la de abajo.

Antes de continuar, se darán ejemplos de cómo poder interpretar estas reglas y observaciones sobre éstas. En palabras, la regla de introducción de la conjunción dice que de las proposiciones φ y ψ se puede concluir[10] que $\varphi \wedge \psi$; en la regla de introducción de la implicación la primera premisa está entre corchetes, lo que significa que es una *hipótesis cancelable*, es decir que no cuenta como hipótesis para la conclusión sin importar las veces que se haya usado para la inferencia, lo cual resulta claro si se interpreta lo que quiere decir esta regla: si de φ se puede concluir ψ, entonces de todo ello se concluye que $\varphi \to \psi$

[10]Recordando la diferencia entre el lenguaje y el meta-lenguaje: es diferente «φ y ψ» a «$\varphi \wedge \psi$».

y no es necesario mantener a φ como hipótesis[11]. De manera similar se interpretan las demás reglas de introducción y eliminación. La primer regla del falso, por ejemplo, se puede interpretar como el principio de explosión (*ex falso quodlibet*, «de lo falso se sigue cualquier cosa») y la segunda como el tradicional principio de demostración por contradicción (*Reductio ad absurdum*), la cual se entiende como «si de la negación de φ se llega a lo falso (una contradicción), entonces se concluye a φ».

Para adquirir practica con está nueva técnica y para mostrar las notaciones que se usarán en ella, a continuación se muestran ejemplos de cómo estas reglas se usan para formar derivaciones.

Ejemplos 1 y 2.

$$\dfrac{\dfrac{\dfrac{[\varphi\wedge\psi]^1}{\psi}\wedge \mathrm{E} \qquad \dfrac{[\varphi\wedge\psi]^1}{\varphi}\wedge \mathrm{E}}{\psi\wedge\varphi}\wedge \mathrm{I}}{\varphi\wedge\psi\to\psi\wedge\varphi}\to \mathrm{I}_1 \qquad\qquad \dfrac{\dfrac{[\varphi]^2 \qquad [\neg\varphi]^1}{\bot}\neg \mathrm{E}}{\neg\neg\varphi}\neg \mathrm{I}_1}{\varphi\to\neg\neg\varphi}\to \mathrm{I}_2$$

Estos ejemplos muestran que, sin ninguna hipótesis, se puede inferir a $\varphi\wedge\psi\to\psi\wedge\varphi$ y a $\varphi\to\neg\neg\varphi$. Aquí los super-índices en las hipótesis cancelables se corresponden con los sub-índices de las reglas que indican cual de ellas es la que las están cancelando. Ahora, ejemplos un poco más elaborados.

Ejemplo 3.

$$\dfrac{\dfrac{\dfrac{\dfrac{[\varphi\wedge\psi]^1}{\psi}\wedge \mathrm{E} \qquad \dfrac{\dfrac{[\varphi\wedge\psi]^1}{\varphi}\wedge \mathrm{E} \qquad [\varphi\to(\psi\to\sigma)]^2}{\psi\to\sigma}\to \mathrm{E}}{\sigma}\to \mathrm{E}}{\varphi\wedge\psi\to\sigma}\to \mathrm{I}_1}{(\varphi\to(\psi\to\sigma))\to(\varphi\wedge\psi\to\sigma)}\to \mathrm{I}_2$$

Ejemplo 4.

$$\dfrac{\dfrac{\dfrac{\dfrac{[\varphi]^1}{\varphi\vee\neg\varphi}\vee \mathrm{I} \qquad [\neg(\varphi\vee\neg\varphi)]^2}{\bot}\neg \mathrm{E}}{\neg\varphi}\neg \mathrm{I}_1}{\varphi\vee\neg\varphi}\vee \mathrm{I} \qquad [\neg(\varphi\vee\neg\varphi)]^2}{\bot}\neg \mathrm{E}}{\varphi\vee\neg\varphi}\ \mathrm{RAA}_2$$

Como se muestra en el teorema 1.1.9 todo el lenguaje se puede formular a partir de unos cuantos conectivos, esto es de mucha ayuda dentro de la deducción natural pues ocurre que algunas de las reglas de inferencia son «abreviaciones» de unas pocas y así la demostración de los resultados que involucren derivaciones son mucho menos extensas, pues solo hay que argumentar para un número reducido de casos. Como en estos preliminares se omiten la mayoría de las demostraciones, esta restricción del lenguaje no

[11] Se puede pensar en el teorema del cálculo que se mencionó anteriormente. Para mostrar que una función diferenciable es continua ($\varphi\to\psi$) se comienza suponiendo que f es diferenciable (φ) y de ello se deduce que es continua (ψ), al final el teorema no se enuncia: «si f es diferenciable, entonces si f es diferenciable entonces es continua», sino que se elimina la primera hipótesis ($[\varphi]$) quedando solamente lo deseado ($\varphi\to\psi$).

es necesaria, además, al ocupar su totalidad se puede apreciar más la manera en que se está abstrayendo la forma de demostrar en la matemática.

Retomando las observaciones sobre las reglas, una aclaración sobre las siguientes.

$$\dfrac{\begin{array}{c}[\varphi]\\ \vdots\\ \bot\end{array}}{\neg\varphi}\ \neg\,\mathrm{I} \qquad\qquad \dfrac{\begin{array}{c}[\neg\varphi]\\ \vdots\\ \bot\end{array}}{\varphi}\ \mathrm{RAA}$$

Aunque en el meta-lenguaje éstas sean consideradas iguales, ya que ambas se pueden interpretar como demostraciones por contradicción (pues la primera se puede entender como: si de suponer φ se concluye lo falso, es porque φ *no es el caso*, por lo tanto, se concluye a $\neg\varphi$), lo cierto es que en principio son diferentes, ya que en la segunda se está utilizando el principio de contradicción y no la regla de introducción de la negación; si se aplica esta última a la derivación se concluiría $\neg\neg\varphi$ en lugar de φ y aunque estos sean *intuitivamente equivalentes* no es claro que lo sean en este sentido.

Antes de llegar a la definición principal, se hará mención de la notación que se ocupará. El símbolo $\begin{array}{c}\mathcal{D}\\ \varphi\end{array}$ representará una derivación con conclusión φ ($\mathcal{D}$ puede ser vacía, es decir, la derivación solo consta de la proposición φ), se ocupará $\begin{array}{c}\psi\\ \mathcal{D}\\ \varphi\end{array}$ para hacer énfasis en que ψ es una hipótesis (no cancelable). Si $\begin{array}{c}\mathcal{D}\\ \varphi\end{array}$ es una derivación, entonces $\dfrac{\begin{array}{c}\mathcal{D}\\ \varphi\end{array}}{\psi}$ es una derivación que se obtiene de la primera aplicando una regla de inferencia a φ; similarmente, si $\begin{array}{c}\mathcal{D}\\ \varphi\end{array}$ y $\begin{array}{c}\mathcal{D}'\\ \varphi'\end{array}$ son derivaciones, entonces $\dfrac{\begin{array}{cc}\mathcal{D} & \mathcal{D}'\\ \varphi & \varphi'\end{array}}{\psi}$ es una derivación que se obtiene de las anteriores aplicando alguna regla de inferencia a φ y φ' (existe el caso de hacer inferencia ocupando tres premisas, esto es únicamente cuando se ocupa la regla de eliminación de la disyunción, en cuyo caso la notación es similar). Como se mencionó, la cancelación de hipótesis se indicará con corchetes, esto es, si $\begin{array}{c}\psi\\ \mathcal{D}\\ \varphi\end{array}$ es una derivación con hipótesis ψ, entonces $\dfrac{\begin{array}{c}[\psi]\\ \mathcal{D}\\ \varphi\end{array}}{\sigma}$ es una derivación con ψ cancelada mediante la aplicación de una regla.

Definición 1.1.11. *El* conjunto de derivaciones *es el conjunto X más pequeño tal que:*

I. (ψ)

$\psi \in X$ *para cada* $\psi \in$ PROP.

II. $(\wedge)$

Si $\begin{array}{c}\mathcal{D}\\ \varphi\end{array}$, $\begin{array}{c}\mathcal{D}'\\ \psi\end{array} \in X$ *entonces* $\dfrac{\begin{array}{cc}\mathcal{D} & \mathcal{D}'\\ \varphi & \psi\end{array}}{\varphi\wedge\psi} \in X$.

Si $\begin{array}{c}\mathcal{D}\\ \varphi\wedge\psi\end{array} \in X$ *entonces* $\dfrac{\begin{array}{c}\mathcal{D}\\ \varphi\wedge\psi\end{array}}{\varphi}$, $\dfrac{\begin{array}{c}\mathcal{D}\\ \varphi\wedge\psi\end{array}}{\psi} \in X$.

III. $(\vee)$

$$Si \quad \begin{matrix}\mathcal{D}\\ \varphi\end{matrix} \in X \text{ entonces } \frac{\begin{matrix}\mathcal{D}\\ \varphi\end{matrix}}{\varphi \vee \psi}, \quad \frac{\begin{matrix}\mathcal{D}\\ \varphi\end{matrix}}{\psi \vee \varphi} \in X.$$

$$Si \quad \begin{matrix}\mathcal{D}\\ \varphi \vee \psi\end{matrix}, \begin{matrix}\varphi\\ \mathcal{D}'\\ \sigma\end{matrix}, \begin{matrix}\psi\\ \mathcal{D}''\\ \sigma\end{matrix} \in X \text{ entonces } \frac{\begin{matrix}\mathcal{D} & [\varphi] & [\psi]\\ \varphi \vee \psi & \mathcal{D}' & \mathcal{D}''\\ & \sigma & \sigma\end{matrix}}{\sigma} \in X.$$

IV. $(\rightarrow)$

$$Si \quad \begin{matrix}\varphi\\ \mathcal{D}\\ \psi\end{matrix} \in X \text{ entonces } \frac{\begin{matrix}[\varphi]\\ \mathcal{D}\\ \psi\end{matrix}}{\varphi \rightarrow \psi} \in X.$$

$$Si \quad \begin{matrix}\mathcal{D}\\ \varphi\end{matrix}, \begin{matrix}\mathcal{D}'\\ \varphi \rightarrow \psi\end{matrix} \in X \text{ entonces } \frac{\begin{matrix}\mathcal{D} & \mathcal{D}'\\ \varphi & \varphi \rightarrow \psi\end{matrix}}{\psi} \in X.$$

V. $(\leftrightarrow)$

$$Si \quad \begin{matrix}\varphi\\ \mathcal{D}\\ \psi\end{matrix}, \begin{matrix}\psi\\ \mathcal{D}'\\ \varphi\end{matrix} \in X \text{ entonces } \frac{\begin{matrix}[\varphi] & [\psi]\\ \mathcal{D} & \mathcal{D}'\\ \psi & \varphi\end{matrix}}{\varphi \leftrightarrow \psi} \in X.$$

$$Si \quad \begin{matrix}\mathcal{D}\\ \varphi\end{matrix}, \begin{matrix}\mathcal{D}'\\ \psi\end{matrix}, \begin{matrix}\mathcal{D}''\\ \varphi \leftrightarrow \psi\end{matrix} \in X \text{ entonces } \frac{\begin{matrix}\mathcal{D} & \mathcal{D}''\\ \varphi & \varphi \leftrightarrow \psi\end{matrix}}{\psi}, \quad \frac{\begin{matrix}\mathcal{D}' & \mathcal{D}''\\ \psi & \varphi \leftrightarrow \psi\end{matrix}}{\varphi} \in X.$$

VI. $(\neg)$

$$Si \quad \begin{matrix}\varphi\\ \mathcal{D}\\ \bot\end{matrix} \in X \text{ entonces } \frac{\begin{matrix}[\varphi]\\ \mathcal{D}\\ \bot\end{matrix}}{\neg\varphi} \in X.$$

$$Si \quad \begin{matrix}\mathcal{D}\\ \varphi\end{matrix}, \begin{matrix}\mathcal{D}'\\ \neg\varphi\end{matrix} \in X \text{ entonces } \frac{\begin{matrix}\mathcal{D} & \mathcal{D}'\\ \varphi & \neg\varphi\end{matrix}}{\bot} \in X.$$

VII. $(\bot)$

$$Si \quad \begin{matrix}\mathcal{D}\\ \bot\end{matrix} \in X \text{ entonces } \frac{\begin{matrix}\mathcal{D}\\ \bot\end{matrix}}{\varphi} \in X.$$

$$Si \quad \begin{matrix}\neg\varphi\\ \mathcal{D}\\ \bot\end{matrix} \in X \text{ entonces } \frac{\begin{matrix}[\neg\varphi]\\ \mathcal{D}\\ \bot\end{matrix}}{\varphi} \in X.$$

Se puede mostrar que el conjunto de derivaciones existe de manera análoga a la utilizada para mostrar la existencia de PROP. A los elementos de X se les llamará **derivaciones**, la última proposición en una derivación se llama **conclusión**. Puesto que las derivaciones tienen una definición recursiva se pueden trasladar los resultados de la subsección 1.1.1, en particular el principio de inducción. La anterior definición no es más que la formalización dentro del estudio de la lógica de todo lo anterior mencionado en esta subsección, es decir, a la manera que se utiliza para demostrar resultados en la matemática.

Definición 1.1.12. *Sea* Γ *un subconjunto de* PROP *y* φ *una proposición. La relación* $\Gamma \vdash \varphi$ *se tiene si existe una derivación cuya conclusión es* φ *y todas las hipótesis no canceladas son elementos del conjunto* Γ. *Si* $\Gamma \vdash \varphi$ *es el caso, se dirá que* φ *es* derivable *(*demostrable*) de* Γ.

Se nota que, por definición, si $\Gamma \vdash \varphi$ entonces Γ puede tener elementos innecesarios, esto es, no todos los elementos de Γ tienen que ser hipótesis de la derivación. Otra observación importante es que toda derivación tiene finitas hipótesis.

Definición 1.1.13. *Si* $\Gamma \vdash \varphi$ *y* $\Gamma = \emptyset$ *entonces se ocupará la notación* $\vdash \varphi$ *y se dirá que* φ *es un* teorema.

La definición de teorema[12] se interpreta como una proposición que puede ser demostrada (en el sentido formal que se acaba de definir) sin necesidad de hipótesis alguna. Para terminar esta sección, se darán ejemplos de teoremas y proposiciones derivables.

Lema 1.1.14. *Sean* Γ *un conjunto de proposiciones y* φ, ψ, σ *proposiciones. Se cumple lo siguiente.*

a) Si $\Gamma \cup \{\varphi\} \vdash \psi$, *entonces* $\Gamma \vdash \varphi \to \psi$.

b) Si $\Gamma \vdash \varphi$ *y* $\Gamma' \vdash \varphi \to \psi$, *entonces* $\Gamma \cup \Gamma' \vdash \psi$.

c) $\Gamma \cup \{\varphi, \neg\varphi\} \vdash \bot$.

d) Si $\Gamma \cup \{\varphi\} \vdash \bot$, *entonces* $\Gamma \vdash \neg\varphi$.

e) Si $\Gamma \vdash \bot$, *entonces* $\Gamma \vdash \varphi$ *para cualquier* $\varphi \in$ PROP.

f) $\vdash \varphi \to (\psi \to \varphi)$

g) $\vdash \varphi \to (\neg\varphi \to \psi)$

h) $\vdash (\varphi \to \psi) \leftrightarrow (\neg\psi \to \neg\varphi)$

A la parte a) del lema se le conoce como el *meta-teorema de deducción*, y éste afirma que para demostrar que una implicación se deriva de un conjunto de oraciones Γ, basta con suponer al antecedente como hipótesis adicional para probar al consecuente[13]. En principio demostrar el lema anterior, y en general mostrar que $\Gamma \vdash \varphi$ para casos particulares, es una ardua tarea ya que, por el momento, se necesita exhibir una derivación cuya conclusión sea φ y las hipótesis no cancelables sean elementos de Γ. Procediendo así, se mostrará la parte h), las demás son demostraciones similares.

$$\dfrac{\dfrac{\dfrac{\dfrac{[\varphi]^1 \qquad [\varphi \to \psi]^5}{\psi} \to \mathrm{E} \qquad [\neg\psi]^2}{\bot} \neg \mathrm{E}}{\neg\varphi} \neg \mathrm{I}_1}{\neg\psi \to \neg\varphi} \to \mathrm{I}_2 \qquad \dfrac{\dfrac{\dfrac{\dfrac{[\varphi]^4 \qquad \dfrac{[\neg\psi]^3 \qquad [\neg\psi \to \neg\varphi]^6}{\neg\varphi} \to \mathrm{E}}{\bot} \neg \mathrm{E}}{\psi} \mathrm{RAA}_3}{\varphi \to \psi} \to \mathrm{I}_4}{(\varphi \to \psi) \leftrightarrow (\neg\psi \to \neg\varphi)} \leftrightarrow \mathrm{I}_{5,6}$$

Se puede, si así se quiere, omitir las etiquetas izquierdas en cada paso de la derivación y los super-índices en las hipótesis para obtener una forma más presentable, el precio a pagar es que se pierde información directa sobre la misma, pero uno puede prescindir de esto si posee cierta experiencia con derivaciones. A continuación, se muestra la anterior omitiendo las etiquetas.

[12] Una vez más, una aclaración sobre el lenguaje y el meta-lenguaje. Aquí la palabra *teorema* tiene un significado preciso dentro del estudio y, formalmente, carece de interpretación alguna; un *teorema* en el meta-lenguaje es lo que comúnmente se entiende por ello en la comunidad matemática.

[13] Esto último es lo que se realiza en la matemática siempre que se quiere mostrar una implicación.

$$\dfrac{\dfrac{\dfrac{[\varphi] \quad [\varphi \to \psi]}{\psi} \quad [\neg\psi]}{\dfrac{\bot}{\neg\varphi}}}{\dfrac{\neg\psi \to \neg\varphi}{(\varphi \to \psi) \leftrightarrow (\neg\psi \to \neg\varphi)}} \qquad \dfrac{\dfrac{[\varphi] \quad \dfrac{[\neg\psi] \quad [\neg\psi \to \neg\varphi]}{\neg\varphi}}{\bot}}{\dfrac{\psi}{\varphi \to \psi}}$$

1.1.4. Completitud

Hasta este momento se han estudiado dos importantes relaciones entre proposiciones, la noción de *verdad* (consecuencia semántica) y la noción de *demostrable* (derivación); éstas, formalmente, son muy diferentes, sin embargo no es complicado (aunque si un tanto laborioso) demostrar lo siguiente.

Lema 1.1.15. LEMA DE SUFICIENCIA. *Si* $\Gamma \vdash \varphi$*, entonces* $\Gamma \vDash \varphi$

Para mostrar este lema es suficiente, por definición de $\Gamma \vdash \varphi$, mostrar que para toda derivación $\mathcal{D}$ con conclusión φ e hipótesis en Γ se tiene que $\Gamma \vDash \varphi$, lo cual se realiza por inducción sobre las derivaciones[14]. Este lema tiene una consecuencia importante, provee una manera alternativa de mostrar que una proposición no es un teorema, basta mostrar que no es una tautología, es decir, en lugar de mostrar que no existe ninguna derivación sin hipótesis con conclusión φ solo hay que encontrar una valuación que haga falsa a φ. A manera de ejemplo, se ocupará este método para mostrar que ni $\bot$ ni $(\varphi \to \psi) \to \varphi \wedge \psi$ son teoremas.

Ejemplo 1.1.16. *Se cumple que:*

a) $\nvdash \bot$

b) $\nvdash (\varphi \to \psi) \to \varphi \wedge \psi$

Demostración. Mostrar que $\bot$ no es un teorema es muy sencillo ya que, por definición, para cualquier valuación v se tiene que $[\![\bot]\!]_v = 0$, es decir, $\bot$ no es una tautología, luego, no es un teorema. El otro ejemplo no es, estrictamente hablando, una proposición, si no un *esquema de proposiciones*[15], por lo que basta demostrar que una instancia[16] de éste no es una tautología; sea entonces $\varphi \equiv \bot$ y $\psi \equiv p_0$, entonces la proposición $(\bot \to p_0) \to \bot \wedge p_0$ no es una tautología, ya que bajo la valuación cero ($[\![p_i]\!]_v = 0$ para todo átomo p_i) su valor de verdad es cero; por lo tanto $\nvdash (\varphi \to \psi) \to \varphi \wedge \psi$. □

Se puede esperar que, más que una condición suficiente, el lema 1.1.15 sea también una condición necesaria. Para mostrar ello, se requiere una serie de nuevas definiciones y lemas previos.

Definición 1.1.17. *Un conjunto* Γ *de proposiciones es* consistente *si* $\Gamma \nvdash \bot$*. Un conjunto* Γ *de proposiciones es* inconsistente *si no es consistente.*

Lema 1.1.18. *Sea* Γ *un conjunto de proposiciones, las siguientes condiciones son equivalentes.*

- Γ *es consistente.*
- *Para ningún* φ*,* $\Gamma \vdash \varphi$ *y* $\Gamma \vdash \neg\varphi$*.*
- *Existe una proposición* φ *tal que* $\Gamma \nvdash \varphi$*.*

[14] La prueba de los lemas y del teorema de completitud en esta subsección se encuentran en [18, cap. 2.5].
[15] Una abreviación dentro del meta-lenguaje para referirse a un conjunto de proposiciones.
[16] Debería nombrarse meta-instancia ya que más adelante se ocupa la palabra *instancia* dentro del lenguaje formal.

Su prueba se sigue directamente de las propiedades de la derivación. La segunda condición del lema dice que un conjunto consistente no puede demostrar algo y su negación a la vez, y la tercera afirma que un conjunto consistente *no puede demostrarlo todo*. El siguiente lema muestra una condición suficiente para que Γ sea consistente.

Lema 1.1.19. *Si existe una valuación v tal que $[\![\psi]\!]_v = 1$ para cada $\psi \in \Gamma$, entonces Γ es consistente.*

Ahora se define un tipo especial de conjuntos consistentes, que son los *más grandes* en el sentido de la contención, esto es, los maximales.

Definición 1.1.20. *Un conjunto Γ es* maximalmente consistente *si cumple las siguientes condiciones.*

I. *Γ es consistente.*

II. *Si $\Gamma \subseteq \Gamma'$ y Γ' es consistente, entonces $\Gamma = \Gamma'$.*

O de manera equivalente, Γ es maximalmente consistente si y solo si es consistente y para cada $\Gamma' \subseteq \text{PROP}$ tal que $\Gamma \subsetneq \Gamma'$ se cumple que Γ' es inconsistente. Un ejemplo de un conjunto maximalmente consistente es, como se muestra en la proposición C.0.23, $\Gamma_v = \{\varphi \in \text{PROP} \mid [\![\varphi]\!]_v = 1\}$ para alguna valuación v fija.

Lema 1.1.21. *Cualquier conjunto consistente Γ está contenido en uno maximalmente consistente Γ^*.*

El lema anterior es importante puesto que se tiene una variedad de resultados interesantes para conjuntos maximalmente consistentes.

Lema 1.1.22. *Si Γ es maximalmente consistente, entonces Γ es cerrado bajo derivabilidad, es decir, si $\Gamma \vdash \varphi$ entonces $\varphi \in \Gamma$.*

Lema 1.1.23. *Si Γ es consistente, entonces existe una valuación v tal que $[\![\psi]\!]_v = 1$ para cada $\psi \in \Gamma$.*

Teorema 1.1.24. DE COMPLETITUD. *$\Gamma \vdash \varphi$ si y solo si $\Gamma \vDash \varphi$*

Para terminar con esta sección, se darán algunas definiciones más que se pueden formular con todo lo que se ha visto hasta ahora y corresponden a la idea intuitiva que se tiene de ellas. Se dice que un conjunto Γ es **completo** si para cada proposición φ ocurre que $\Gamma \vdash \varphi$ o $\Gamma \vdash \neg\varphi$ (para cualquier proposición φ, el conjunto Γ puede demostrar φ o su negación). Se dice que φ es **independiente de** Γ si $\Gamma \nvdash \varphi$ y $\Gamma \nvdash \neg\varphi$ (de Γ no se puede demostrar ni ella ni su negación). Un conjunto Γ es **independiente** si para toda $\varphi \in \Gamma$ ocurre que $\Gamma \setminus \{\varphi\} \nvdash \varphi$ (cada elemento de φ es independiente de los demás).

Estas propiedades (consistencia, independencia y completitud) fueron estudiadas por D. Hilbert y, a la vez, fundamentales para el desarrollo del llamado *Programa de Hilbert* (ver [11], principalmente la sección titulada *El pensamiento axiomático*). Hasta el siglo XX se tenía la idea de que el conjunto de axiomas de las ramas matemáticas (que se puede pensar como un conjunto de proposiciones) debería poseer dichas propiedades, es decir, no tenían que producir contradicciones, tenía que ser independiente entre sí[17] y ser capaz de demostrar cualquier enunciado de la teoría o su negación. A partir del programa de Hilbert se comienzan a estudiar con más formalidad buscando una prueba rigurosa de este deseo, sin embargo, los teoremas de Gödel, de alguna manera, lo destruyen (ver *Hilbert y los fundamentos de las matemáticas* de Carlos Torres Alcaraz en [11]).

[17] El ejemplo más antiguo e ilustrativo de este hecho es el quinto postulado de Euclides.

1.2. Lógica de predicados

En la sección anterior se mostró el alcance (semántico y de inferencia) que tiene la lógica de orden cero la cual, retomando, abstrae la idea de formar enunciados complejos (mediante conectivos) partiendo de las unidades llamadas átomos. Sin embargo, es demasiado general y abstracta como para expresar la forma de razonar en la ciencia matemática. Para entender esto se dará un ejemplo. En teoría de números se puede formular la oración «todo número primo mayor que 2 es impar», además se sabe que «19 es un número primo mayor que 2», de lo que se concluye que «19 es impar»; en la lógica proposicional esto se representa con, por ejemplo, $p_2 \wedge p_{15} \to p_8$ y aunque se acepta que el ejemplo es *verdadero* no existe ninguna razón para concluir que $p_2 \wedge p_{15} \to p_8$ lo sea. El motivo de esto es que la lógica de orden cero no es lo bastante expresiva como para abarcar la noción de, por ejemplo, el *para todo*. Es por ello que se desea enriquecer a la lógica agregando nuevos elementos, uno de ellos debe ser aquel que permita interpretarse como el *cuantificador universal* en el mundo de discurso, así, se desea poder tener una manera de representar oraciones tales como «todo número par es igual a la suma de dos números primos impares»; además, se desea introducir la noción dual, conocida como el *cuantificador existencial*, para poder trabajar con, por ejemplo, «existe un número real tal que su cuadrado es igual a 2».

El ejemplo del párrafo anterior también muestra una deficiencia crucial en la lógica proposicional que es el no poder representar, de una manera conveniente, las *propiedades* y *relaciones* que poseen los objetos de estudio. Por ejemplo, la oración «19 es un número primo» se puede representar con el átomo p_5, sin embargo, se pierde mucha información; otro ejemplo es la oración «19 es mayor que 2» que, de nuevo, es pobre en su representación por un átomo. Entonces, se desea ampliar la lógica con la noción de relación en el sentido de la teoría de conjuntos[18]. Se desea también poder abarcar la idea de función, por ejemplo a $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ conocida como la suma de los naturales[19]. Más aún, queda el hecho de poder usar *variables* en nuestro nuevo lenguaje que, puesto que antes no se podían formular oraciones como «$x+4 \leq 0$», en donde el símbolo x representa a un (unos o ningún) objeto dentro del estudio.

Sabiendo la idea principal de la lógica de primer orden, como también se le llama a la lógica de predicados, se está preparado para entrar en las definiciones principales.

1.2.1. Estructuras

La noción de *estructura* está presente en el estudio de la matemática, en álgebra un *grupo* es un conjunto no vacío equipado con dos operaciones, una binaria y una unaria, que satisfacen ciertas reglas; en teoría de conjuntos un *conjunto ordenado* es un conjunto con una relación binaria que satisface otras reglas. Por el momento solo importará extraer la definición abstracta que abarque la idea de estructura, dejando para después las *ciertas reglas*.

Definición 1.2.1. *A un conjunto ordenado de la forma* $\langle A;\ R_1, \ldots, R_n;\ F_1, \ldots, F_m;\ \{c_i \mid i \in I\}\rangle$ *se le llamará* estructura. *Donde* A *es un conjunto no vacío,* $R_1, \ldots, R_n$ *son relaciones en* A *(es decir,* $R_i \subseteq A^{r_i}$ *para algún* r_i *natural),* $F_1, \ldots, F_m$ *son funciones en* A *(es decir,* $F_j : A^{a_j} \to A$ *para algún* a_i *natural) y* $\{c_i \mid i \in I\}$ *es un subconjunto de elementos de* A *indizado con* I.

[18] En dicha teoría se define una *relación* R en un conjunto X como un subconjunto de alguna potencia natural de X, es decir, $R \subseteq X^n$ para algún n natural; en el caso $n = 1$ éstas se pueden llamar *propiedades*. Por ejemplo, en el conjunto de los números naturales ($\mathbb{N}$) la *propiedad* de ser un número par se puede cambiar por el hecho de pertenecer al conjunto $P = \{n \in \mathbb{N} :$ 2 divide a $n\}$ y la *relación* menor o igual se puede concebir como el conjunto $\leq = \{(n, m) \in \mathbb{N}^2 \mid$ existe $k \in \mathbb{N}$ tal que $n = m + k\}$. Véase definición A.1.5 y [10, págs. 45-47 y 66-70].

[19] Véase definición A.1.6 y [10, págs. 51-52].

Se ocuparán letras góticas ($\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$) para denotar estructuras. Si una estructura carece de relaciones, funciones o constantes se omite su escritura entre los puntos y comas correspondientes.

Ejemplos de estructuras son los siguientes[20].

- $\mathfrak{A} = \langle \mathbb{Q};\ ;\ +, -;\ \{0\} \rangle$.
- $\mathfrak{B} = \langle \mathbb{R};\ ;\ +, \times, -;\ \{0, 1\} \rangle$.
- $\mathfrak{C} = \langle \mathbb{Z};\ \leq;\ ;\ \rangle$.

Si $\mathfrak{A}$ es una estructura, se denotará con el símbolo $|\mathfrak{A}|$ al conjunto A de la definición 1.2.1 al cual se le llamará **universo** de $\mathfrak{A}$; además, se dirá que $\mathfrak{A}$ es finito (resp. infinito) si su universo es finito (resp infinito).

Existen estructuras diferentes que comparten cierta similitud, por ejemplo todos los grupos que, aunque son de diferente naturaleza, pues sus universos pueden ser conjuntos diferentes, comparten la misma esencia en cuanto poseer solo un par de funciones (una binaria y una unaria) y una sola constante. Por ello interesa clasificar las estructuras en la siguiente definición.

Definición 1.2.2. *Sea* $\mathfrak{A} = \langle A;\ R_1, \ldots, R_n;\ F_1, \ldots, F_m;\ \{c_i \mid i \in I\} \rangle$ *una estructura, el* tipo de similitud *(o simplemente* tipo*) de* $\mathfrak{A}$ *es el conjunto* $\langle r_1, \ldots, r_n;\ a_1, \ldots, a_m;\ \kappa \rangle$ *donde* $R_i \subseteq A^{r_i}$, $F_j : A^{a_j} \to A$ *y* $\kappa = |\{c_i \mid i \in I\}|$.

Los tipos de $\mathfrak{A}, \mathfrak{B}$ y $\mathfrak{C}$ del ejemplo anterior son, respectivamente, $\langle -;\ 2, 1;\ 1 \rangle$, $\langle -;\ 2, 2, 1;\ 2 \rangle$ y $\langle 2;\ -;\ 0 \rangle$ en donde el símbolo «$-$» indica que no existen relaciones o funciones según sea el caso. Así, $\langle -;\ 2, 1;\ 1 \rangle$ indica que no hay relaciones, que hay dos funciones (una binaria y una unaria) y una constante; y $\langle 2;\ -;\ 0 \rangle$ que hay una relación (binaria), no hay funciones y no hay constantes.

Hay que notar que en los ejemplos no se hace mención de la relación binaria *igualdad* ($I = \{(x, y) \in X^2 \mid x = y\}$), esto es porque se supondrá que todas las estructuras la poseen (a menos que se indique lo contrario) y no se escribirá explícitamente.

Los «casos extremos» en las relaciones son relaciones de aridad 0 (0-arias), esto es, conjuntos R tales que $R \subseteq X^0 = \{\emptyset\}$, así una relación de aridad 0 solo puede ser $\emptyset$ o $\{\emptyset\}$ las cuales pueden ser consideradas como los ordinales 0 y 1 respectivamente. Éstas son, en la práctica de la lógica de predicados, innecesarias, sin embargo son convenientes e importantes para otros fines. Por otro lado, una función f de aridad 0 ($f : \{\emptyset\} \to A$) puede considerarse como una constante (en A), pero como la definición de estructura las considera de manera independiente, no será necesario hacer uso de estas funciones. Este párrafo se puede concluir con lo siguiente: Sea $\langle r_1, \ldots, r_n;\ a_1, \ldots, a_m;\ \kappa \rangle$ el tipo de la estructura $\mathfrak{A}$, entonces $r_i, a_j > 0$ para $i = 1, \ldots, n$ y $j = 1, \ldots, m$, y $\kappa \geq 0$.

1.2.2. Lenguaje

El lenguaje en la lógica de primer orden, así como en cualquier otra lógica, no es más que una representación simbólica y formal del lenguaje natural que se utiliza en los razonamientos. Así, un lenguaje se compone de un alfabeto (conjunto de símbolos sin significado alguno) que se unen o concatenan[21] bajo ciertas reglas para formar *términos* (los cuales representarán objetos del universo) y *formulas* (las cuales representarán expresiones sobre dichos términos).

[20] Aunque con nombre propio, estos ejemplos son, por ahora, solamente estructuras. En la subsección 1.2.6 se dan las definiciones necesarias para llamar *grupo* a, por ejemplo, $\mathfrak{A} = \langle \mathbb{Q};\ ;\ +, -;\ \{0\} \rangle$.

[21] Idea similar a la realizada en lógica de primer orden; es decir, sucesiones finitas de los símbolos de este lenguaje.

Para construir un lenguaje se necesita que este sea de algún tipo; en esta sección se asumirá que el tipo de lenguaje está fijo y es $\langle r_1, \ldots, r_n;\ a_1, \ldots, a_m;\ \kappa\rangle$ con $r_i, a_i > 0$.

Definición 1.2.3. *El* alfabeto *consiste de los siguientes símbolos.*

I. *Símbolos predicados:* $P_1, \ldots, P_n, \doteq$.

II. *Símbolos funcionales:* $F_1, \ldots, F_m$.

III. *Símbolos constantes:* $\bar{c}_i$ *para cada* $i \in \kappa$.

IV. *Variables:* $x_0, x_1, \ldots$ *(numerables)*

V. *Conectivos:* $\wedge, \vee, \to, \leftrightarrow, \neg, \bot, \forall, \exists$.

VI. *Símbolos auxiliares:* $(,)$.

Los símbolos $\forall$, $\exists$ son llamados *cuantificador universal* y *cuantificador existencial*, respectivamente. Los símbolos predicados, funcionales y constantes presentados en la definición, en sí, son meta-variables para representar símbolos; esto es porque, dado un lenguaje, éste tendrá sus propios símbolos.

Un comentario respecto al símbolo de igualdad ($=$); hay, de hecho, varios símbolos de igualdad que se ocuparán, uno de ellos es el usado en el meta-lenguaje, está también la introducida en la definición anterior (la *igualdad sintáctica*), además de otras igualdades que fungen dentro de las meta-variables, como por ejemplo al decir que la estructura $\mathfrak{A}$ es igual a la estructura $\mathfrak{B}$ ($\mathfrak{A} = \mathfrak{B}$). En principio debe haber diferentes símbolos para la igualdad, sin embargo, a veces se abusará del lenguaje y se ocupará el mismo símbolo ($=$) para todas siendo el contexto quien dicte el tipo usado.

Hay algo más que aclarar antes de continuar y es sobre el uso de las variables (*variables sintácticas*). Ocurre que éstas son *de primer orden*, esto significa que solo se pueden ocupar para representar elementos del universo y no otras cosas; por ejemplo, en la estructura de los reales presentada para la definición 1.2.1, las variables solo hacen referencia a números reales (en $x + 4 = 5$, a x se le interpreta como un real) y solo se puede cuantificar sobre éstos ($\forall x(x \cdot x \geq 0)$), dejando fuera la posibilidad de usarlas sobre relaciones o funciones, así no hay manera de representar la oración «todo subconjunto no vacío acotado superiormente tiene una cota mínima superior» pues esta cuantifica sobre subconjuntos, los cuales no son elementos del universo. Para combatir esta *deficiencia* se define la *lógica de segundo orden*. Para un mayor entendimiento de este comentario, ver [18, cap. 5].

A diferencia de la lógica proposicional, en donde solo se definió a PROP, aquí se definirán dos tipos de *categorías sintácticas*, las cuales son TERM (el conjunto de **términos**) y FORM (el conjunto de **fórmulas**)[22]. Esto debido a que en la matemática hay una diferencia esencial entre elementos tales como x^{-1}, $y + x$, 0 y 1 y otros como $x^{-1} \leq 1$, $\forall x \exists y(y + x = 0)$ y $0 \neq 1$, pues las primeras representan a un objeto (u objetos, como $y + x$) dentro del universo y las segundas expresan propiedades de estos objetos, así 0 representa solo un elemento del universo y $0 \neq 1$ es una oración que expresa una propiedad[23].

Definición 1.2.4. *Se define a* TERM *como el conjunto* X *más pequeño con las siguientes propiedades.*

I. $\bar{c}_i \in X$ *para cada* $i \in I$.

II. $x_i \in X$ *para* $i = 0, 1, \ldots$

III. *Si* $t_1, \ldots, t_{a_i} \in X$, *entonces* $F_i(t_1, \ldots, t_{a_i}) \in X$ *para* $1 \leq i \leq m$.

[22] Estos conjuntos existen por motivos similares a los usados en la prueba para la existencia de PROP.

[23] Dentro de los números reales, por ejemplo, ocurre que 0 es un elemento del universo y la oración $0 \neq 1$ no lo es.

En la definición anterior, para hacer referencia a elementos del alfabeto, se ocupan meta-variables, así $\overline{c}_i$ no es parte del lenguaje, es una manera genérica de representar a una constante, lo mismo con x_i y t_j. El conjunto de términos contiene a los símbolos constantes, a las variables y a los símbolos que resultan al *aplicar*[24] las funciones a términos.

Definición 1.2.5. *Se define a* FORM *como el conjunto X más pequeño con las siguientes propiedades.*

I. $\bot \in X$.
   Si $t_1, \ldots, t_{r_i} \in X$ *entonces* $P_i(t_1, \ldots, t_{r_i}) \in X$.
   Si $t_1, t_2 \in X$ *entonces* $t_1 = t_2 \in X$.

II. *Si* $\varphi, \psi \in X$ *entonces* $(\varphi \square \psi) \in X$, *donde* $\square \in \{\wedge, \vee, \to, \leftrightarrow\}$.

III. *Si* $\varphi \in X$, *entonces* $(\neg\varphi) \in X$.

IV. *Si* $\varphi \in X$, *entonces para cada* $i \in I$, $((\forall x_i)\varphi), ((\exists x_i)\varphi) \in X$.

Las fórmulas introducidas en la parte I. de la definición 1.2.5 se llamarán **átomos**. Los átomos de un lenguaje constan entonces del falso y de las relaciones aplicadas a términos, haciendo énfasis en la relación de igualdad que, como se mencionó, se tomará siempre en cuenta a menos que se indique lo contrario. Estos átomos y sus negaciones pueden ser considerados como los átomos de la lógica proposicional, pues son éstos las *unidades mínimas* que expresan algo y pueden formar *expresiones más complejas* al combinarlos apropiadamente con los conectivos.

Se adoptarán las abreviaciones de la sección anterior para simplificar la escritura en el lenguaje omitiendo cierto uso de paréntesis, además se suprimirán los paréntesis externos que se encuentran en las fórmulas que involucran cuantificadores y a veces todos los paréntesis de éstas, teniendo $\forall$ y $\exists$ mayor jerarquía que los demás conectivos; así, se ocupará el símbolo $\forall x_0 \exists x_9(\bot \to x_0 = x_9 \wedge \neg\neg\bot)$ para simplificar la escritura de la fórmula $((\forall x_0)((\exists x_9)(\bot \to ((x_0 = x_9) \wedge (\neg(\neg\bot))))))$. Más aún, se unirán los cuantificadores del mismo tipo cuando éstos sean consecutivos dentro de la misma fórmula, por ejemplo, se ocupará el símbolo $\forall x_1 x_2 \exists x_3 x_4 \forall x_5 \varphi$ para simplificar a $\forall x_1 \forall x_2 \exists x_3 \exists x_4 \forall x_5 \varphi$. Por último, a fin de hacer más amena la escritura, se asumirá que el sub-índice n tanto en $P(t_1, \ldots, t_n)$ como en $F(t_1, \ldots, t_n)$ siempre es el número del argumento correspondiente a cada símbolo predicado P y símbolo funcional F.

Al igual que antes, al ser las definiciones de TERM y FORM recursivas, se tendrá un teorema del principio de inducción para cada una y su demostración es similar a la de su homóloga de la sección anterior.

Teorema 1.2.6. PRINCIPIO DE INDUCCIÓN PARA TÉRMINOS. *Sea* $\mathrm{A}(t)$ *una meta-propiedad aplicable a los términos del lenguaje. Si ocurre que*

- $\mathrm{A}(t)$ *se cumple cuando t es una variable o una constante, y*
- *siempre que* $t_1, \ldots, t_n$ *tienen la propiedad* A *entonces* $F(t_1, \ldots, t_n)$ *tiene la propiedad para todo símbolo funcional F;*

entonces se cumple $\mathrm{A}(t)$ *para todo* $t \in$ TERM.

[24] El lenguaje formal está constituido por símbolos sin significado alguno, así, *aplicar* equivale a concatenar (sucesiones finitas de) símbolos sin necesidad de definir el significado de esto.

Teorema 1.2.7. Principio de inducción para fórmulas. *Sea* $\mathrm{A}(\varphi)$ *una (meta-)propiedad aplicable a las fórmulas del lenguaje. Si ocurre que*

- $\mathrm{A}(\varphi)$ *para todo átomo* φ*,*
- *si* $\mathrm{A}(\varphi)$ *y* $\mathrm{A}(\psi)$ *entonces* $A(\varphi \square \psi)$*,*
- *si* $\mathrm{A}(\varphi)$ *entonces* $\mathrm{A}(\neg\varphi)$*, y*
- *si* $\mathrm{A}(\varphi)$ *entonces* $\mathrm{A}(\forall x_i \varphi)$ *y* $\mathrm{A}(\exists x_i \varphi)$ *para todo* $i = 0, 1, \ldots$*;*

entonces toda $\varphi \in \mathrm{FORM}$ *tiene la propiedad* A.

A continuación, un ejemplo de un lenguaje del tipo $\langle 2;\ 2, 1;\ 1\rangle$. Se usará en éste el color de texto distinto para diferenciar al lenguaje formal. Primero el alfabeto a utilizar.

- Símbolos predicados: m, $\doteq$.
- Símbolos funcionales: p, i.
- Símbolos constantes: $\overline{e}$.

Es importante el orden en el cual se presentan los símbolos (predicados y funcionales), ya que, dado el tipo de similitud de la estructura, el orden coincide con el número de su aridad. Así, en este ejemplo p es un símbolo funcional binario y i es unario. Como se mencionó, no se hace referencia a la relación de igualdad en el tipo.

Algunos términos en este lenguaje son: $t_1 \equiv \overline{e}$, $t_2 \equiv x_0$, $t_3 \equiv p(x_0, \overline{e})$, $t_4 \equiv p(p(x_0, \overline{e}), \overline{e})$, $t_5 \equiv i(x_1)$, $t_6 \equiv p(i(x_1), p(x_0, \overline{e}))$. Algunas fórmulas en este lenguaje son las siguientes.

- $\varphi_1 \equiv x_0 \doteq \overline{e}$
- $\varphi_2 \equiv \neg(x_0 \doteq p(x_0, \overline{e}))$
- $\varphi_3 \equiv m(i(x_1), x_1)$
- $\varphi_4 \equiv i(x_1) \doteq x_1 \to x_1 \doteq \overline{e}$
- $\varphi_5 \equiv \forall x_0 \exists x_1 (p(x_0, x_1) \doteq \overline{e})$
- $\varphi_6 \equiv \forall x_0 \exists x_0 \forall x_0 (x_1 \doteq x_2)$
- $\varphi_7 \equiv \exists x_0 \left(\forall x_1 \left(p(x_0, x_1) \doteq x_1 \wedge \forall x_2 \left(p(x_2, x_1) \doteq x_1 \to x_2 \doteq x_0\right)\right)\right)$

El lenguaje formal de la lógica es un conjunto de símbolos sin ningún significado *a priori*, sin embargo, se utiliza para representar el lenguaje que se ocupa en la matemática. Por tal motivo se utilizo una notación sugestiva en el anterior ejemplo, se puede interpretar el símbolo predicado m como «menor que», los símbolos funcionales p y i como «producto» e «inverso» respectivamente y el símbolo constante $\overline{e}$ como «neutro». Siendo entonces el lenguaje de un *grupo multiplicativo* dotado además de un *orden*. Así, aún cuando solamente son símbolos sin significado, se puede interpretar al termino t_3 como «el producto de x_0 con el neutro» y a la fórmula φ_7 como la condición de existencia y unicidad del neutro.

Al igual que en la lógica de orden cero, en la lógica de predicados existen teoremas que permiten hacer definiciones por recursión sobre los términos y sobre las fórmulas, dichos teoremas son demasiado técnicos para estos preliminares y simplemente se ocuparán como sustento en las definiciones posteriores. Si se desea ver los enunciados de estos teoremas véase [18, pág. 59]

Paso siguiente es definir un curioso y común uso dado a las variables dentro del estudio de la matemática. En la integral $\int_a^b e^{x^2} \partial x$ y en la oración $\forall x \in \mathbb{R}$ la variable x tiene un significado diferente, ya que en estos no varía ni tampoco se puede, a menos que resulte algo sin sentido, sustituir a x por algún

número real; a pesar de todo ello, se sigue conociendo como variable. La razón es que que son simples etiquetas dentro de la notación las cuales, para cobrar sentido, están *ligadas* a otro símbolo (en la integral, x tendría otro sentido si no estuviese junto al símbolo ∂). Por otro lado, el uso de x en expresiones como $x + 4 \leq 0$ o $x^2 = -1$ es completamente diferente, aquí sí se puede pensar que x toma diversos valores y se puede sustituir por algún objeto del estudio (se puede formular a $1^2 = -1$ pues está bien escrito, su veracidad es parte de otro estudio), aquí las variables están *libres* de los otros símbolos.

Definición 1.2.8. *Sea t un término. Se define recursivamente al conjunto $FV(t)$, el* conjunto de variables libres de *t, como sigue.*

I. $FV(x_i) = \{x_i\}$.

II. $FV(\bar{c}_i) = \emptyset$.

III. $FV(F(t_1, \ldots, t_n)) = FV(t_1) \cup \cdots \cup FV(t_n)$.

Definición 1.2.9. *Sea φ una fórmula. Se define recursivamente al conjunto $FV(\varphi)$, el* conjunto de variables libres de *φ, como sigue.*

I. $FV(\bot) = \emptyset$.

II. $FV(t_1 = t_2) = FV(t_1) \cup FV(t_2)$.

III. $FV(P(t_1, \ldots, t_p)) = FV(t_1) \cup \cdots \cup FV(t_p)$.

IV. $FV(\varphi \square \psi) = FV(\varphi) \cup FV(\psi)$.

V. $FV(\neg\varphi) = FV(\varphi)$.

VI. $FV(\forall x_i \varphi) = FV(\varphi) \setminus \{x_i\}$.

VII. $FV(\exists x_i \varphi) = FV(\varphi) \setminus \{x_i\}$.

Lo que dice este par de definiciones es que toda variable (sola) está libre y las unidas a algún cuantificador no lo están, las constantes no tiene variables libres y las variables libres de una fórmula o término compuesto son las variables libres de sus partes. Por ejemplo, $FV(\bar{c}_j = \bar{c}_i \to \bot) = \emptyset$, $FV(x_0 = x_1) = \{x_0, x_1\}$, $FV(\exists x_1 \neg(x_0 = x_1)) = \{x_0\}$ y $FV(\forall x_0 \exists x_1 \neg(x_0 = x_1)) = \emptyset$.

La definición del conjunto de **variables ligadas** ($BV(\varphi)$) se hace similar y conserva la idea intuitiva que se presentó. Se observa que no necesariamente $FV(\varphi) \cap BV(\varphi)$ es vacío.

Saber si un término o una fórmula tiene variables libres es importante en el estudio. Por ejemplo, dentro de los números reales, se entiende plenamente el significado de $0 + 1$, $0 + 1 = 0$ y $\exists x_0(x_0 \cdot x_0 = 2)$ en el sentido que expresan un término o predicado concreto, pero, ¿que significaría $x + y$, $0 + x = 0$ o $\exists x_0(x_0 \cdot x_1 = 2)$?

Definición 1.2.10. *Se dice que el término t (resp. la fórmula φ) es* cerrado *(resp.* cerrada*) si $FV(t) = \emptyset$ (resp. $FV(\varphi) = \emptyset$). Una fórmula cerrada también es llamada* oración*. Una fórmula sin cuantificadores es llamada* abierta*. Se denotará con* TERM_C *al conjunto de términos cerrados y con* SENT *al conjunto de oraciones.*

Se definirá ahora la manera de sustituir variables por términos y sustituciones de fórmulas dentro de otras fórmulas.

Definición 1.2.11. *Sean s, t términos y x una variable, entonces $s[t/x]$ es definido por:*

I. $s[t/x] = \begin{cases} s, & si\ s \not\equiv x \\ t, & si\ s \equiv x \end{cases}$

II. $c[t/x] = c$

III. $F(t_1, \ldots, t_n)[t/x] = F(t_1[t/x], \ldots, t_n[t/x])$ *para todo símbolo funcional F.*

Definición 1.2.12. *Sea t un término, x una variable y φ una fórmula, se define $\varphi[t/x]$ mediante:*

I. $\bot[t/x] = \bot$
$P(t_1, \ldots, t_p)[t/x] = P(t_1[t/x], \ldots, t_p[t/x])$ *para todo símbolo predicado P.*
$(t_1 = t_2)[t/x] = (t_1[t/x] = t_2[t/x])$[25]

II. $(\varphi \square \psi)[t/x] = \varphi[t/x] \square \psi[t/x]$
$(\neg\varphi)[t/x] = \neg\varphi[t/x]$

III. $(\forall y\varphi)[t/x] = \begin{cases} \forall y\varphi[t/x], & si\ x \not\equiv y \\ \forall y\varphi, & si\ x \equiv y \end{cases}$
$(\exists y\varphi)[t/x] = \begin{cases} \exists y\varphi[t/x], & si\ x \not\equiv y \\ \exists y\varphi, & si\ x \equiv y \end{cases}$

Las definiciones de sustitución parecen naturales salvo, quizá, las que involucran cuantificadores. Esto queda más claro con un ejemplo, sea $\varphi \equiv \exists x_0(x_0 = x_1)$, no hay problema en sustituir dentro de φ a x_1 por cualquier otro término, por ejemplo una constante $\overline{c}_i$, lo cual da como resultado a $\varphi[\overline{c}_i/x_1] \equiv \exists x_0(x_0 = \overline{c}_i)$; en cambio, si se pretendiera sustituir a x_0 por un termino puede ocurrir que lo resultante ni siquiera esté bien definido, por ejemplo al querer sustituirlo por una constante; es por ello que ese tipo de sustitución no se permite por definición.

Para la siguiente definición se ocupará $\sharp$ como símbolo para representar un átomo, el cual actuará como *parámetro de sustitución*. Como en el caso de la definición 1.1.6, la siguiente solo permite hacer algunos tipos de sustituciones muy sencillos, pero se puede formular una más general donde se permita que el *parámetro de sustitución* sea cualquier fórmula; por ser este último mucho más conveniente, en lo venidero se hará referencia a él.

Definición 1.2.13. *Sean $\varphi, \sigma, \sigma_1, \sigma_2$ fórmulas, se define a $\sigma[\varphi/\sharp]$ de la siguiente manera.*

I. *Si σ es un átomo,* $\sigma[\varphi/\sharp] = \begin{cases} \sigma, & si\ \sigma \not\equiv \sharp \\ \varphi, & si\ \sigma \equiv \sharp \end{cases}$

II. $(\sigma_1 \square \sigma_2)[\varphi/\sharp] = \sigma_1[\varphi/\sharp] \square \sigma_2[\varphi/\sharp]$

III. $(\neg\sigma)[\varphi/\sharp] = \neg\sigma[\varphi/\sharp]$

IV. $(\forall x\sigma)[\varphi/\sharp] = \forall x\sigma[\varphi/\sharp]$

V. $(\exists x\sigma)[\varphi/\sharp] = \exists x\sigma[\varphi/\sharp]$

[25] Aquí la diferencia entre dos tipos de igualdad.

Por último, se tratará otro problema con las sustituciones que involucran a los cuantificadores. Por definición, no se puede realizar una sustitución en una fórmula que involucre un cuantificador utilizando la variable que está ligada a éste, pero puede ocurrir que se realice una sustitución permitida y en lo resultante haya un término ligado *de más*. Por ejemplo en $\forall x(x < y)$, la cual es una fórmula con y como variable libre y x como variable ligada, la definición permite hacer la sustitución $\forall x(x < y)[x/y]$ la cual resulta ser $\forall x(x < x)$, razón por la cual se necesita algún otro tipo de restricción. El problema de esto radica en que cuando se sustituye una variable libre por otra, ésta última puede convertirse en ligada. Para manejar esta prohibición se recurre a lo siguiente.

Definición 1.2.14. *Sea t un término, x una variable y φ una fórmula. Se dice que t es* libre por x en φ *si se cumple alguna de las siguientes condiciones.*

I. *φ es un átomo.*

II. *$\varphi = \varphi_1 \square \varphi_2$ (o $\varphi = \neg\varphi_1$) y t es libre por x en φ_1 y en φ_2 (resp. en φ_1).*

III. *$\varphi = \forall y\psi$ (o $\varphi = \exists y\psi$), si t es libre por x en ψ y además se cumple que si $x \in FV(\varphi)$ entonces $y \notin FV(t)$.*

Algunos ejemplos:

- x_1 es libre por x_0 en $x_0 = x_1$.
- $F(x_0)$ es libre por x_0 en $\neg\exists x_0(P(x_0, x_1, x_2) \to \bot)$.
- $F(x_0)$ no es libre por x_0 en $\neg\exists x_0(P(x_0, x_1, x_2) \to \bot)$.

Esta definición puede parecer engorrosa y poco entendible, pero estas son, como lo demuestra el siguiente lema, exactamente las condiciones que se deben pedir para evitar los problemas mencionados. Su prueba se encuentra en [18, pág. 62].

Lema 1.2.15. *t es libre por x en φ si y solo si las variables de t no están ligadas por algún cuantificador en $\varphi[t/x]$.*

Esto es en el caso de los términos, pero como también se puede sustituir por fórmulas se tiene la definición y lema correspondientes.

Definición 1.2.16. *Sean φ, σ fórmulas. Se dice que σ es* libre por $\sharp$ en φ *si se cumple alguna de las siguientes condiciones.*

I. *φ es un átomo.*

II. *$\varphi = \varphi_1 \square \varphi_2$ (o $\varphi = \neg\varphi_1$) y σ es libre por $\sharp$ en φ_1 y en φ_2 (resp. en φ_1).*

III. *$\varphi = \forall y\psi$ (o $\varphi = \exists y\psi$), si φ es libre por $\sharp$ en ψ y además se cumple que si $\sharp$ ocurre[26] en φ entonces $y \notin FV(\sigma)$.*

Lema 1.2.17. *σ es libre por $\sharp$ en φ si y solo si las variables libres de σ no están ligadas por algún cuantificador en $\varphi[\sigma/\sharp]$.*

[26]Entiéndase «φ (resp. t) *ocurre en* ψ» como el hecho de que la fórmula ψ se creó a partir de φ (resp. t) siguiendo de las reglas de la definición 1.2.5.

A partir de ahora se supondrá, de manera implícita, que en las sustituciones se ocuparán términos y fórmulas «libres por».

A fin de simplificar la notación y de ocupar una más tradicional, se escribirán expresiones de la forma $\varphi(x, y, z), \psi(x)$, etc. Lo cual no significa que las variables listadas sean necesariamente libres y, en caso de serlo, sean las únicas; es simplemente una notación que permitirá presentar las sustituciones de manera más compacta, así, $\psi(t)$ es el resultado de reemplazar t en lugar de x en $\psi(x)$ (es decir, una abreviación de $\psi[t/x]$); a $\psi(t)$ se le llamará *instancia* de $\psi(x)$.

Algunas veces será necesario, en alguna estructura $\mathfrak{A}$, tener un *nombre* para cada elemento de su universo, esto es, se querrá que cada elemento de $|\mathfrak{A}|$ sea una constate (principalmente como un recurso auxiliar). Es por ello que se introduce la siguiente definición.

Definición 1.2.18. *Sea $\mathfrak{A}$ una estructura y L su lenguaje. El* lenguaje extendido *de $\mathfrak{A}$, denotado por $L(\mathfrak{A})$, es el lenguaje que se obtiene de agregar a L símbolos constantes por cada elemento de $|\mathfrak{A}|$. Se denotará con $\bar{a}$ al símbolo constante correspondiente con $a \in |\mathfrak{A}|$.*

1.2.3. Semántica

Debe ser claro que los objetos del estudio de la lógica son símbolos sin significado alguno que representan entes matemáticos (*v. g.* números, gráficas, funciones, conjuntos, figuras geométricas, etc.). El objetivo de la semántica es poder *interpretar* los primeros (objetos sintácticos) utilizando los segundos (objetos *reales*) para después decidir cuándo una oración es verdadera, para ello, se basará en la idea que tuvo Tarski sobre la verdad[27]: «una oración σ será verdadera en una estructura si realmente σ ocurre en ella»[28]. Un ejemplo dentro de la matemática: Dentro de la estructura de los enteros como grupo aditivo, la fórmula del lenguaje formal $\bar{1}\dot{+}\bar{0} \doteq \bar{0}\dot{+}\bar{1}$ es verdadera pues su interpretación (es decir, $1 + 0 = 0 + 1$) sí ocurre en ella.

Para lograr un mayor entendimiento de este sutil concepto, antes de presentar las definiciones formales se trabajará empíricamente con un ejemplo. Sea[29] $\mathfrak{A} = \langle \mathbb{Z}, <, +, -, 0 \rangle$ el grupo aditivo de los números enteros con su orden usual, cuyo tipo de similitud es $\langle 2;\ 2, 1;\ 1 \rangle$; sea L el lenguaje de este tipo cuyo alfabeto es el siguiente.

- Símbolos predicados: M, $\doteq$.
- Símbolos funcionales: S, I.
- Símbolos constantes: $\bar{0}$.

Y sea $L(\mathfrak{A})$ el lenguaje extendido, esto es, para cada $m \in \mathbb{Z}$ se tiene un nuevo símbolo constante para el lenguaje, a saber, $\overline{m}$. Primero se interpretarán algunos términos cerrados del lenguaje $L(\mathfrak{A})$, la interpretación de t en $\mathfrak{A}$, denotada por $t^{\mathfrak{A}}$, es un elemento de su universo, es decir, $t^{\mathfrak{A}} \in \mathbb{Z}$.

[27] Una discusión amplia de este tema puede encontrarse en *Stanford Encyclopedia of Philosophy*, en su entrada llamada *Tarski's Truth Definitions*.

[28] El enunciado «el agua es líquida» es verdadero puesto que realmente el agua es líquida. El enunciado «el número π es algebraico» es falso porque realmente no lo es.

[29] A veces, cuando la escritura no se preste a confusión, se omitirá el uso de las llaves en el conjunto de las constantes y se cambiarán los puntos y comas que separan a los integrantes de la estructura por simples comas.

Termino cerrado (t)	Interpretación ($t^{\mathfrak{A}}$)
$I(I(\overline{0}))$	$-(-0)$ $[=0]$
$S(\overline{9},\overline{14})$	$9+14$ $[=23]$
$S(t,\overline{0})$	$t^{\mathfrak{A}}+0$
$I(S(t_1,t_2))$	$-(t_1^{\mathfrak{A}}+t_2^{\mathfrak{A}})$

Cuadro 1.3: Algunos términos cerrados y sus interpretaciones en $\mathfrak{A}$.

De nuevo se ocupa una notación conveniente en el alfabeto del lenguaje, así, al símbolo funcional S se le interpreta como la suma de $\mathfrak{A}$ $(+)$ y a I como su inverso aditivo $(-)$. Además, la interpretación estará restringida a los términos cerrados pues ¿que interpretación (objeto de $\mathbb{Z}$) se le puede asignar a $S(x_0,\overline{0})$? Se procede ahora a interpretar oraciones (fórmulas cerradas) del lenguaje asignando, mediante una función v, el valor 1 (resp. 0) en el caso que sea verdadera (resp. falsa). Para ello, se adoptarán las reglas, adaptadas a este contexto, de la definición 1.1.4 agregando algunas más.

- $v(t \doteq s)\begin{cases} 1, & \text{si } t^{\mathfrak{A}}=s^{\mathfrak{A}} \\ 0, & \text{en otro caso.}\end{cases}$
- $v(M(t,s))\begin{cases} 1, & \text{si } t^{\mathfrak{A}}<s^{\mathfrak{A}} \\ 0, & \text{en otro caso.}\end{cases}$
- $v(\forall x\varphi)=\text{mín}\{v(\varphi[\overline{n}/x]) \mid n\in\mathbb{Z}\}$.
- $v(\exists x\varphi)=\text{máx}\{v(\varphi[\overline{n}/x]) \mid n\in\mathbb{Z}\}$.

En el caso general, la función v será definida por recursión, además está completamente determinada por la estructura $\mathfrak{A}$ por lo que una mejor notación sería $v_{\mathfrak{A}}$, sin embargo, ninguna de éstas será usada, en su lugar, se ocupará la notación $[\![\varphi]\!]_{\mathfrak{A}}$ (o simplemente $[\![\varphi]\!]$ cuando se haya especificado a $\mathfrak{A}$) en lugar de $v_{\mathfrak{A}}(\varphi)$.

La interpretación de una fórmula con cuantificador universal (resp. existencial) es una generalización de la idea del conjuntor (resp. disyuntor) pues es verdadera solo en el caso en que toda (resp. alguna) instancia de $\varphi(x)$ sea verdadera. Para terminar con este ejemplo, algunas interpretaciones de fórmulas:

- $[\![\ \overline{0}\doteq I(\overline{0})\ ]\!]=1$, puesto que $0=-0$.
- $[\![\ M(\overline{0},\overline{2})\wedge M(\overline{2},\overline{0})\ ]\!]=0$, por que no ocurre que $2<0$..
- $[\![\ \overline{0}\doteq 1\to M(\overline{2},\overline{0})\ ]\!]=1$, el antecedente es falso.
- $[\![\ \forall x\exists y(M(x,y))\ ]\!]=1$, pues $\mathbb{Z}$ no tiene elemento máximo.

Para la definición formal de interpretación sea $\mathfrak{A}=\langle A;\ R_1,\ldots,R_n;\ F_1,\ldots,F_m;\ \{c_i \mid i\in I\}\rangle$ una estructura del tipo de similitud fijo $\langle r_1,\ldots,r_n;\ a_1,\ldots,a_m;\ \kappa\rangle$. El lenguaje correspondiente tiene símbolos predicados $\overline{R}_1,\ \ldots,\ \overline{R}_n$; símbolos funcionales $\overline{F}_1,\ \ldots,\ \overline{F}_m$; y símbolos constantes $\overline{c}_i$; además, el lenguaje $L(\mathfrak{A})$ tendrá una constante adicional $\overline{a}$ por cada $a\in A$.

Definición 1.2.19. *Una* interpretación *de los términos cerrados de* $L(\mathfrak{A})$ *en* $\mathfrak{A}$ *es una función* $(\cdot)^{\mathfrak{A}}:\text{TERM}_C\to|\mathfrak{A}|$ *la cual satisface*

I. $\overline{c}_i^{\mathfrak{A}}=c_i$.
$\overline{a}^{\mathfrak{A}}=a$.

II. $(\overline{F}_i(t_1,\ldots,t_p))^{\mathfrak{A}}=F_i(t_1^{\mathfrak{A}},\ldots,t_p^{\mathfrak{A}})$.

Definición 1.2.20. *Una* interpretación *de las oraciones de* $L(\mathfrak{A})$ *en* $\mathfrak{A}$ *es una función* $[\![\cdot]\!]_{\mathfrak{A}} : \text{SENT} \to \{0,1\}$ *la cual satisface*

I. $[\![\bot]\!]_{\mathfrak{A}} = 0$.

II. $$[\![\overline{R}_i(t_1,\ldots,t_p)]\!]_{\mathfrak{A}} = \begin{cases} 1, & si\ (t_1^{\mathfrak{A}},\ldots,t_p^{\mathfrak{A}}) \in R_i \\ 0, & en\ otro\ caso. \end{cases}$$
$$[\![t_1 = t_2]\!]_{\mathfrak{A}} = \begin{cases} 1, & si\ t_1^{\mathfrak{A}} = t_2^{\mathfrak{A}} \\ 0, & en\ otro\ caso. \end{cases}$$

III. $[\![\varphi \wedge \psi]\!]_{\mathfrak{A}} = \text{mín}\{[\![\varphi]\!]_{\mathfrak{A}}, [\![\psi]\!]_{\mathfrak{A}}\}$.
$[\![\varphi \vee \psi]\!]_{\mathfrak{A}} = \text{máx}\{[\![\varphi]\!]_{\mathfrak{A}}, [\![\psi]\!]_{\mathfrak{A}}\}$.
$[\![\varphi \to \psi]\!]_{\mathfrak{A}} = \text{máx}\{1 - [\![\varphi]\!]_{\mathfrak{A}}, [\![\psi]\!]_{\mathfrak{A}}\}$.
$[\![\varphi \leftrightarrow \psi]\!]_{\mathfrak{A}} = 1 - |[\![\varphi]\!]_{\mathfrak{A}} - [\![\psi]\!]_{\mathfrak{A}}|$.
$[\![\neg\varphi]\!]_{\mathfrak{A}} = 1 - [\![\varphi]\!]_{\mathfrak{A}}$.

IV. $[\![\forall x\varphi]\!]_{\mathfrak{A}} = \text{mín}\{[\![\varphi[\overline{a}/x]]\!]_{\mathfrak{A}} \mid a \in |\mathfrak{A}|\}$.
$[\![\exists x\varphi]\!]_{\mathfrak{A}} = \text{máx}\{[\![\varphi[\overline{a}/x]]\!]_{\mathfrak{A}} \mid a \in |\mathfrak{A}|\}$.

A veces, se utilizará la notación de corchetes en las interpretaciones de términos ($[\![t]\!]_{\mathfrak{A}}$ en lugar de $t^{\mathfrak{A}}$). Para simplificar la comunicación, a partir de ahora se asumirá que las estructuras y lenguajes tienen el tipo de similitud apropiado y no especificará el tipo.

Se ocupará la notación $\mathfrak{A} \vDash \varphi$ (resp. $\mathfrak{A} \nvDash \varphi$) para cuando $[\![\varphi]\!]_{\mathfrak{A}} = 1$ (resp. 0) y si este es el caso se dirá que φ *es verdadera* o *valida* (resp. *falsa*) *en* $\mathfrak{A}$. La (meta-)relación $\vDash$ se llama **relación de satisfacción**. Para ampliarla a fórmulas que no sean oraciones y a conjuntos de fórmulas, se introduce las siguientes definiciones.

Definición 1.2.21. *Sea* φ *una fórmula y* $FV(\varphi) = \{z_1,\ldots,z_k\}$ *entonces la oración* $Cl(\varphi) = \forall z_1 \cdots z_k \varphi$ *es llamada la* clausura universal *de* φ.

Definición 1.2.22. *Sea* φ *una fórmula y* Γ *un subconjunto de* FORM*, se define*

I. $\mathfrak{A} \vDash \varphi$ *si* $\mathfrak{A} \vDash Cl(\varphi)$.

II. $\vDash \varphi$ *si* $\mathfrak{A} \vDash \varphi$ *para toda* $\mathfrak{A}$ *(del tipo apropiado).*

III. $\mathfrak{A} \vDash \Gamma$ *si* $\mathfrak{A} \vDash \varphi$ *para toda* $\varphi \in \Gamma$.

IV. *Si* $\Gamma \cup \{\varphi\} \subseteq$ SENT*, entonces* $\Gamma \vDash \varphi$ *si se cumple que si* $\mathfrak{A} \vDash \Gamma$ *entonces* $\Gamma \vDash \varphi$.

Si $\mathfrak{A} \vDash \varphi$ (resp. $\mathfrak{A} \vDash \Gamma$) se dirá que $\mathfrak{A}$ es **modelo** de φ (resp. Γ); φ será **verdadera** si $\vDash \varphi$ y será una **consecuencia semántica** de Γ si $\Gamma \vDash \varphi$. La notación $\nvDash \varphi$ (resp. $\Gamma \nvDash \varphi$) se ocupa cuando $\vDash \varphi$ (resp. $\Gamma \vDash \varphi$) no es el caso.

La propiedad de *consecuencia semántica* es muy interesante y quizá se necesite aclarar un poco. Se dice que φ es consecuencia semántica de Γ si ocurre que todo modelo de Γ es también modelo de φ, es decir, en cualquier estructura donde los elementos de Γ sean verdaderos también será verdadera φ (no es, en principio, sencillo determinar cuando se cumple esta relación, pues involucra a una *clase* de estructuras).

Sea φ una fórmula con variables libres $z_1, \ldots, z_k$; se dirá que φ se **satisface por** $a_1, \ldots, a_k \in |\mathfrak{A}|$ si[30] $\mathfrak{A} \vDash \varphi[\bar{a}_1, \ldots, \bar{a}_k/z_1, \ldots, z_k]$, si este es el caso, se dirá que φ es **satisfecha en** $\mathfrak{A}$ y finalmente se dirá que φ es **satisfecha** si es satisfecha en alguna estructura $\mathfrak{A}$.

La interpretación de los conectivos del lenguaje formal se corresponde con la idea que se tiene de ellos en el meta-lenguaje, esto es, se pueden simplemente reemplazar por sus respectivas nociones del meta-lenguaje. El siguiente lema menciona formalmente algunos de ellos y su prueba es directa de la definición de interpretación.

Lema 1.2.23. *Si se restringe solo a las oraciones del lenguaje, se cumple*

a) $\mathfrak{A} \vDash \varphi \wedge \psi$ *si y solo si* $\mathfrak{A} \vDash \varphi$ *y* $\mathfrak{A} \vDash \psi$.

b) $\mathfrak{A} \vDash \neg\varphi$ *si y solo si* $\mathfrak{A} \nvDash \varphi$.

c) $\mathfrak{A} \vDash \varphi \to \psi$ *si y solo si,* $\mathfrak{A} \vDash \varphi$ *implica que* $\mathfrak{A} \vDash \psi$.

d) $\mathfrak{A} \vDash \exists x\varphi$ *si y solo si* $\mathfrak{A} \vDash \varphi[\bar{a}/x]$ *para algún* $a \in |\mathfrak{A}|$.

La definición de verdad para la lógica de predicados es, de hecho, una extensión de su versión en la lógica proposicional; así, cualquier formula que sea una (meta-)instancia[31] de una tautología será verdadera en toda estructura $\mathfrak{A}$, por ejemplo, se sabe que la proposición $\varphi \vee \psi \leftrightarrow \neg(\neg\varphi \vee \neg\psi)$ es una tautología, entonces, la fórmula resultante de colocar cualquier fórmula del lenguaje en lugar de φ y cualquier otra en lugar de ψ es satisfecha en toda estructura. Por ello, muchas de las propiedades semánticas enunciadas en la subsección 1.1.2 se pueden transferir a este contexto, así, en lo siguiente solo se presentarán propiedades semánticas para los cuantificadores (sus pruebas se encuentran en [18, cap. 3.5]).

Teorema 1.2.24. Leyes de DeMorgan.

a) $\vDash \neg\forall x\varphi \leftrightarrow \exists x\neg\varphi$

b) $\vDash \neg\exists x\varphi \leftrightarrow \forall x\neg\varphi$

c) $\vDash \forall x\varphi \leftrightarrow \neg\exists x\neg\varphi$

d) $\vDash \exists x\varphi \leftrightarrow \neg\forall x\neg\varphi$

El siguiente teorema demuestra que el orden entre cuantificadores del mismo tipo es irrelevante (por ejemplo, se acepta que $\forall x\forall y(x = y \to \forall a(x + a = y + a))$ y $\forall y\forall x(x = y \to \forall a(x + a = y + a))$ expresan lo mismo) además de que, como se pudo observar desde el momento de su definición, no tiene ningún efecto aplicar un cuantificador con variable ligada x a alguna oración que no tenga a x como variable libre.

Teorema 1.2.25.

a) $\vDash \forall x\forall y\varphi \leftrightarrow \forall y\forall x\varphi$

b) $\vDash \exists x\exists y\varphi \leftrightarrow \exists y\exists x\varphi$

c) Si $x \notin FV(\varphi)$*, entonces* $\vDash \forall x\varphi \leftrightarrow \varphi$.

d) Si $x \notin FV(\varphi)$*, entonces* $\vDash \exists x\varphi \leftrightarrow \varphi$.

[30] La notación $\varphi[t_1, \ldots, t_n/x_1, \ldots, x_n]$ corresponde a una *sustitución simultanea*, es decir, cada variable x_i se sustituye por el término t_i de manera independiente a los demás y *al mismo tiempo*.

[31] Se coloca el prefijo «meta» para evitar confusión con la idea de instancia que se definió dentro del lenguaje.

En principio, al hacer una sustitución iterada[32] se debe tener bastante cuidado, puesto la interpretación del término o la oración puede cambiar completamente. Sin embargo, el siguiente resultado muestra que uno puede acortar ciertas sustituciones.

Lema 1.2.26. *Sea t un término, φ una oración y $a \in |\mathfrak{A}|$.*

a) Si $z \notin FV(t)$ entonces $t[\bar{a}/x] = (t[z/x])[\bar{a}/z]$.

b) Si $z \notin FV(\varphi)$ y z es libre por x en φ, entonces $\varphi[\bar{a}/x] = (\varphi[z/x])[\bar{a}/z]$.

Ahora se analizará un truco muy usado en la matemática, el cual consiste en cambiar, de manera conveniente, la variable ligada a un cuantificador. Por ejemplo, en la oración usada dentro del campo de los reales $\forall x(x^2 \geq 0 \wedge (x > 1 \to x^2 > x)$, quizá uno quiera separar las dos oraciones que abarca el cuantificador y colocar una «nueva variable» (pues x ya fue usada) para la segunda, y obtener así $\forall x(x^2 \geq 0) \wedge \forall y(y > 1 \to y^2 > y)$; para realizar cambios como éste se necesita que las oraciones sean equivalentes (que no se modifique la interpretación), las condiciones para lograrlo se enuncian en el siguiente teorema.

Teorema 1.2.27. Cambio de variables ligadas. *Si x, y son libres por z en φ y además no son variables libres de la fórmula φ, entonces se cumple lo siguiente.*

- $\vDash \exists x\varphi[x/z] \leftrightarrow \exists y\varphi[y/z]$
- $\vDash \forall x\varphi[x/z] \leftrightarrow \forall y\varphi[y/z]$

En la lógica de primer orden también se tiene un teorema de sustitución el cual, en analogía con su versión en la lógica proposicional, asegura que se pueden sustituir términos iguales u oraciones equivalentes dentro de otras.

Teorema 1.2.28. Teorema de sustitución

- $\vDash t_1 = t_2 \to (s[t_1/x] = s[t_2/x])$
- $\vDash t_1 = t_2 \to (\varphi[t_1/x] \leftrightarrow \varphi[t_2/x])$
- $\vDash \varphi_1 \leftrightarrow \varphi_2 \to (\psi[\varphi_1/\sigma] \leftrightarrow \psi[\varphi_2/\sigma])$

Una consecuencia del teorema de sustitución es el siguiente corolario, a cuyo enunciado se le puede dar la interpretación de que el término t del lenguaje formal y la constante $\overline{t^{\mathfrak{A}}}$ son, en el sentido semántico, el mismo objeto. En particular dice que no hay diferencia entre una constante c del lenguaje L de una estructura $\mathfrak{A}$ y la *nueva constante* $\overline{c^{\mathfrak{A}}}$ del lenguaje extendido.

Corolario 1.2.29.

a) $[\![s[t/x]]\!] = [\![s[\overline{[\![t]\!]}/x]]\!]$.

b) $[\![\varphi[t/x]]\!] = [\![\varphi[\overline{[\![t]\!]}/x]]\!]$.

Para terminar esta subsección se introducirán algunas notaciones convenientes, un par de ellas involucra a las relaciones unarias. Por ejemplo la propiedad de densidad de los números de los números racionales en los reales, ésta se puede escribir (abusando un poco de la notación) con el lenguaje de la estructura[33] $\mathfrak{A} = \langle \mathbb{R}, \mathbb{Q}, < \rangle$ como $\forall xy(x < y \to \exists(\mathbb{Q}(z) \wedge x < z < y))$; a pesar de ello, se está más acostumbrado a $\forall xy(x < y \to \exists z \in \mathbb{Q}(x < z < y))$. Las otras son abreviaciones comunes del cuantificador existencial.

[32] No debe confundirse con una sustitución simultánea, ésta última hace los cambios *al mismo tiempo* mientras que la iterada los realiza siguiendo el orden escrito.

[33] En esta estructura $\mathbb{Q}$ está tomando el papel de relación unaria de $\mathbb{R}$.

Definición 1.2.30. *Sea P un símbolo predicado de aridad uno y φ una oración, se ocuparán las siguientes notaciones como abreviaciones.*

- $(\forall x \in P)\varphi \equiv \forall x(P(x) \to \varphi)$
- $(\exists x \in P)\varphi \equiv \exists x(P(x) \to \varphi)$
- $\nexists x\varphi(x) \equiv \neg\exists x\varphi(x)$
- $\exists! x\varphi(x) \equiv \exists x\varphi(x) \wedge \forall y(\varphi(y) \to y = x)$

1.2.4. Deducción natural

La deducción natural de la lógica de predicados se tratará como una extensión (adecuada) de la discutida en la subsección 1.1.3, primero, al conjunto de reglas de derivación expuesto en esa sección se le añadirán cuatro más (dos para el cuantificador universal y dos para el existencial).

Reglas de cuantificación universal.

$$\frac{\varphi}{\forall x\varphi}\ (\forall\ \mathrm{I}) \qquad\qquad \frac{\forall x\varphi}{\varphi[t/x]}\ (\forall\ \mathrm{E})$$

Reglas de cuantificación existencial.

$$\frac{\varphi[t/x]}{\exists x\varphi}\ (\exists\ \mathrm{I}) \qquad\qquad \frac{\exists x\varphi \qquad \begin{array}{c}[\varphi]\\ \vdots\\ \psi\end{array}}{\psi}\ (\exists\ \mathrm{E})$$

Sin embargo, éstas tienen algunas restricciones sobre las variables y términos usados en ellas. Para entender esto, se verá con un ejemplo que ocurriría si no se tiene cuidado en ello.

$$\dfrac{\dfrac{\dfrac{\dfrac{[x=\bar{0}]}{\forall x(x=\bar{0})}\,\forall\ \mathrm{I}}{x=\bar{0}\to\forall x(x=\bar{0})}\to\mathrm{I}}{\forall x(x=\bar{0}\to\forall x(x=\bar{0}))}\,\forall\ \mathrm{I}}{\bar{0}=\bar{0}\to\forall x(x=\bar{0})}\,\forall\ \mathrm{E} \qquad\qquad \dfrac{\dfrac{\dfrac{[\forall x\exists y(x\neq y)]}{\exists y(y\neq y)}\,\forall\ \mathrm{E}}{\forall x\exists y(x\neq y)\to\exists y(y\neq y)}\to\mathrm{I}$$

La primer «derivación» dice que en una estructura con una constante 0 se puede demostrar que, si $0 = 0$, entonces todo elemento del universo es igual a esa constante. La segunda, diría que si para todo elemento existe otro distinto a él, entonces existe un elemento que es diferente a sí mismo. Estas anomalías ocurren porque las anteriores no son derivaciones ya que violan los siguientes requisitos: en $(\forall\ \mathrm{I})$ x no debe ser variable libre en ninguna hipótesis de la cual dependa $\varphi(x)$, esto es, se quiere que la variable x sea *arbitraria*, por lo cual no se puede suponer nada sobre ella (en el primer ejemplo se supone $x = \bar{0}$); en $(\forall\ \mathrm{E})$ se requiere que t sea libre por x en φ, esto para que al sustituirla no quede ligada a un cuantificador (como en el segundo ejemplo). En las reglas de $\exists$ ocurren fenómenos similares, para evitarlo, t debe ser libre por x en φ en la regla $(\exists\ \mathrm{I})$ y en la regla $(\exists\ \mathrm{E})$ x no es libre en ψ ni en cualquier hipótesis, a excepción de φ, de la cual ψ dependa.

Así, la definición del conjunto de derivaciones en lógica de predicados es igual que la definición 1.1.11 salvo por la parte I., donde se cambia PROP por FORM, además de agregar las partes correspondientes a las reglas de los cuantificadores pidiendo las mencionadas restricciones. Se extiende además la notación del símbolo $\vdash$ ((meta-)relación que ahora se da entre conjuntos de fórmulas y fórmulas), la definición de **derivable**, **teorema**, **conclusión**, **consistente** y demás conceptos y notación de la deducción natural para la lógica proposicional.

Los resultados de dicha subsección también se pueden trasladar, con la debida adaptación en este contexto, a esta nueva definición de derivación. El siguiente teorema es solo para mostrar un par de teoremas que involucran a los cuantificadores. Su demostración se sigue de las reglas introducidas.

Teorema 1.2.31. *Sea $\varphi(x)$ una fórmula, se cumple lo siguiente.*

- $\vdash \exists x\varphi(x) \leftrightarrow \neg\forall x\neg\varphi(x)$
- $\vdash \forall x\varphi(x) \leftrightarrow \neg\exists x\neg\varphi(x)$

Para terminar con esto, pues no hay nada nuevo en la deducción natural por agregar, se mostrarán algunos ejemplos de derivaciones utilizando estas nuevas reglas.

Si $x \notin FV(\varphi)$ se tiene la siguiente derivación.

$$\dfrac{\dfrac{\dfrac{\dfrac{[\forall x(\varphi \to \psi(x))]}{\varphi \to \psi}\,\forall\,\mathrm{E} \qquad [\varphi]}{\psi(x)}\,\to\mathrm{E}}{\forall x\psi(x)}\,\forall\,\mathrm{I}}{\varphi \to \forall x\psi(x)}\,\to\mathrm{I}}{\forall x(\varphi \to \psi(x)) \to (\varphi \to \forall x\psi(x))}\,\to\mathrm{I}$$

Si $x \notin FV(\psi)$ se tiene la siguiente derivación.

$$\dfrac{\dfrac{\dfrac{[\exists x\varphi(x)] \qquad \dfrac{\dfrac{[\forall x(\varphi(x) \to \psi)]}{\varphi(x) \to \psi}\,\forall\,\mathrm{E} \qquad [\varphi(x)]}{\psi}\,\to\mathrm{E}}{\psi}\,\exists\,\mathrm{E}}{\exists x\varphi(x) \to \psi}\,\to\mathrm{I}}{\forall x(\varphi(x) \to \psi) \to (\exists x\varphi(x) \to \psi)}\,\to\mathrm{I}$$

1.2.5. Identidad

Hasta ahora, se ha tratado a la igualdad como una relación binaria inherente en toda estructura y en todo lenguaje, aún así, se puede estudiar de manera independiente, esto es, en lugar de ser tratada como una relación matemática se puede ver como otro símbolo lógico, el cual cumple *ciertos axiomas* característicos. Para poder enunciarlos se necesita introducir una nueva notación para la conjunción y la disyunción que servirá como abreviación de oraciones extensas.

Definición 1.2.32. *Sea φ_i una fórmula para cada $i \in \mathbb{N}$; se define para cada natural n a $\bigwedge_{i\leq n}\varphi_i$ y a $\bigvee_{i\leq n}\varphi_i$ como sigue.*

$$\begin{cases} \bigwedge_{i\leq 0}\varphi_i = \varphi_0 \\ \bigwedge_{i\leq n+1}\varphi_i = \bigwedge_{i\leq n}\varphi_i \ \wedge \ \varphi_{n+1} \end{cases}$$

$$\begin{cases} \bigvee_{i\leq 0}\varphi_i = \varphi_0 \\ \bigvee_{i\leq n+1}\varphi_i = \bigvee_{i\leq n}\varphi_i \ \vee \ \varphi_{n+1} \end{cases}$$

Estas notaciones siguen la misma idea que los símbolos $\sum$ y $\prod$ (en cuanto abreviar una expresión finita). Con esto se pueden formular las siguientes oraciones que caracterizan a la identidad.

- $\mathrm{I}_1 \equiv \forall x(x = x)$
- $\mathrm{I}_2 \equiv \forall xy(x = y \to y = x)$
- $\mathrm{I}_3 \equiv \forall xyz(x = y \wedge y = z \to x = z)$
- $\mathrm{I}_{4a} \equiv \forall x_1 \cdots x_n y_1 \cdots y_n(\bigwedge_{i\leq n} x_i = y_i \to t(x_1, \ldots, x_n) = t(y_1, \ldots, y_n))$
- $\mathrm{I}_{4b} \equiv \forall x_1 \cdots x_n y_1 \cdots y_n(\bigwedge_{i\leq n} x_i = y_i \to (\varphi(x_1, \ldots, x_n) \to \varphi(y_1, \ldots, y_n)))$

La notación $t(x_1, \ldots, x_n)$ (resp. $\varphi(x_1, \ldots, x_n)$) representa una sustitución simultánea, estrictamente debería escribirse como $t[x_1, \ldots, x_n/z_1, \ldots, z_n]$ (resp. $\varphi[x_1, \ldots, x_n/z_1, \ldots, z_n]$), pues a veces no se querrá sustituir a todas las ocurrencias de x_i por y_i en φ, más adelante se da un ejemplo para entender esto. Se darán ahora las reglas de inferencia correspondientes para la identidad.

Reglas de identidad.

$$\frac{}{x = x}\ (\mathrm{Id}_1) \qquad \frac{x = y}{y = x}\ (\mathrm{Id}_2) \qquad \frac{x = y \qquad y = z}{x = z}\ (\mathrm{Id}_3)$$

$$\frac{x_1 = y_1, \ldots, x_n = y_n}{t(x_1, \ldots, x_n) = t(y_1, \ldots, y_n)}\ (\mathrm{Id}_4) \qquad \frac{x_1 = y_1, \ldots, x_n = y_n \qquad \varphi(x_1, \ldots, x_n)}{\varphi(y_1, \ldots, y_n)}\ (\mathrm{Id}_4)$$

Donde en (Id_4) las variables $y_1, \ldots, y_n$ son libres por $x_1, \ldots, x_n$ en φ. Las reglas anteriores implican inmediatamente que $\vdash I_i$ para $i = 1, 2, 3, 4$. Se verá ahora un ejemplo de porqué se utilizan las sustituciones simultaneas de la manera antes mencionada, para ello, se trabajará en $\mathfrak{A} = \{\mathbb{Z}, <, +, -, \{0\}\}$ y, para mostrarlo más entendible, se hará un abuso del lenguaje utilizando el meta-lenguaje en las derivaciones.

$$\frac{x = y \qquad x + y < x + 2}{y + y < x + 2} \qquad \frac{x = y \qquad x + y < x + 2}{x + y < y + 2} \qquad \frac{x = y \qquad x + y < x + 2}{y + y < y + 2}$$

Puede parecer que no se está haciendo una buena sustitución en las primeras dos derivaciones puesto que no todas las ocurrencias de x se están sustituyendo por y; lo que ocurre es que la *forma real* de la fórmula que actúa como hipótesis es $z_1 + z_2 < z_3 + 2$, por lo que una manera más precisa, aunque extensa y a veces innecesaria, de escribir las derivaciones es la siguiente.

$$\frac{x = y, y = y, x = x \qquad (z_1 + z_2 < z_3 + 2)[x, y, x/z_1, z_2, z_3]}{(z_1 + z_2 < z_3 + 2)[y, y, x/z_1, z_2, z_3]}$$

$$\frac{x = x, y = y, x = y \qquad (z_1 + z_2 < z_3 + 2)[x, y, x/z_1, z_2, z_3]}{(z_1 + z_2 < z_3 + 2)[x, y, y/z_1, z_2, z_3]}$$

$$\frac{x = y, y = y, x = y \qquad (z_1 + z_2 < z_3 + 2)[x, y, x/z_1, z_2, z_3]}{(z_1 + z_2 < z_3 + 2)[y, y, y/z_1, z_2, z_3]}$$

Por último, el conjunto infinito de reglas[34] representadas por (Id_4) se puede derivar de un conjunto finito, utilizando los símbolos predicados y funcionales del lenguaje. Su prueba está en [18, cap. 3.10]

Lema 1.2.33. *Sea L un lenguaje del tipo $\langle r_1, \ldots, r_n;\ a_1, \ldots, a_m;\ \kappa\rangle$, si las reglas*

$$\frac{x_1 = y_1, \ldots, x_{r_i} = y_{r_i} \qquad P_i(x_1, \ldots, x_{r_i})}{P_i(y_1, \ldots, y_{r_i})} \quad \textit{para cada } i \leq n,$$

y las reglas

$$\frac{x_1 = y_1, \ldots, x_{a_j} = y_{a_j}}{F_j(x_1, \ldots, x_{r_j}) = F_j(y_1, \ldots, y_{r_j})} \quad \textit{para cada } j \leq m$$

están dadas, entonces las reglas (Id_4) son derivables.

1.2.6. Ejemplos

En esta subsección se mostrarán las definiciones de algunas estructuras familiares y sus lenguajes. Se supondrá que todas las estructuras satisfacen los axiomas I_1, I_2, I_3 e I_4.

El lenguaje de la Identidad. Del tipo $\langle -;\ -;\ 0\rangle$
Alfabeto:

- Símbolos predicados: $=$.

Una *estructura de identidad* es una estructura muy simple, pues es de la forma $\mathfrak{A} = \langle A\rangle$; por lo que básicamente solo se puede hacer inferencia sobre la cardinalidad de su universo, para ello, se definen las siguientes proposiciones.

- $\lambda_n \equiv \exists y_1 \cdots y_n \left(\bigwedge_{i\neq j} y_i \neq y_j\right)$ para $n > 1$ natural.
- $\mu_n \equiv \forall y_1 \cdots y_n \left(\bigvee_{i\neq j} y_i = y_j\right)$ para $n > 0$ natural.

La primera puede interpretarse como «existen al menos n elementos» y la segunda como «existen a lo más n elementos». Se tiene entonces que $\mathfrak{A} \vDash \lambda_n \wedge \mu_n$ si y solo si $|\mathfrak{A}| = n$.

El lenguaje del Orden Parcial. Del tipo $\langle 2;\ -;\ 0\rangle$
Alfabeto:

- Símbolos predicados: $=$, $\leq$.

Para las posteriores definiciones conviene introducir las siguientes abreviaciones.

$x \neq y \equiv \neg(x = y)$ $\qquad$ $x > y \equiv y < x$ $\qquad$ $x \leq y \leq z \equiv x \leq y \wedge y \leq z$

$x < y \equiv x \leq y \wedge x \neq y$ $\qquad$ $x \geq y \equiv y \leq x$ $\qquad$ $x < y < z \equiv x < y \wedge y < z$

[34] Puesto que representa una regla para cada elección de t y φ, es decir, es un *esquema* de reglas de inferencia.

Definición 1.2.34. $\mathfrak{A}$ *es un* conjunto parcialmente ordenado *(copo) si* $\mathfrak{A}$ *es un modelo de*

$$\forall xyz(x \leq y \leq z \to x \leq z)$$

$$\forall xy(x \leq y \leq x \leftrightarrow x = y)$$

Un copo puede ser *totalmente ordenado* o *densamente ordenado* si además de las anteriores es modelo de $\forall xy(x \leq y \vee y \leq x)$ y $\forall xy(x < y \to \exists z(x < z < y))$ respectivamente.

El lenguaje de Grupos. Del tipo $\langle -;\ 2, 1;\ 2\rangle$
Alfabeto:

- Símbolos predicados: $=$.
- Símbolos funcionales: $\cdot$, $^{-1}$.
- Símbolos constantes: e.

A fin de utilizar una notación más apegada a la usual, se escribirá $t \cdot s$ y t^{-1} en lugar de $\cdot(t, s)$ y $^{-1}(t)$ respectivamente.

Definición 1.2.35. $\mathfrak{A}$ *es un grupo si es modelo de*

$$\forall xyz((x \cdot y) \cdot z = x \cdot (y \cdot z))$$

$$\forall x(x \cdot e = x \ \wedge \ e \cdot x = x)$$

$$\forall x(x \cdot x^{-1} = e \ \wedge \ x^{-1} \cdot x = e)$$

Se ocupó la notación usual para los grupos multiplicativos (los reales o los racionales, por ejemplo); sin embargo, y dado que solamente son símbolos, se puede adoptar la notación de grupos aditivos (los enteros, por ejemplo), esto es, utilizando los símbolos funcionales «$+$» y «$-$» en lugar de «$\cdot$» y «$^{-1}$» respectivamente. Además, se dirá que un grupo es *abeliano* si además de ser modelo de las anteriores oraciones es modelo de $\forall xy(x \cdot y = y \cdot x)$.

El lenguaje de Anillos con Unidad. Del tipo $\langle -;\ 2, 2, 1;\ 2\rangle$
Alfabeto:

- Símbolos predicados: $=$
- Símbolos funcionales: $+$, $\cdot$, $-$.
- Símbolos constantes: 0, 1.

Definición 1.2.36. $\mathfrak{A}$ *es anillo (con unidad) si es modelo de*

$$\forall xyz((x + y) + z = x + (y + z)) \qquad \forall xyz((x + y) \cdot z = x \cdot z + y \cdot z)$$

$$\forall xy(x + y = y + x) \qquad \forall x(x + 0 = x)$$

$$\forall xyz((x \cdot y) \cdot z = x \cdot (y \cdot z)) \qquad \forall x(x + (-x) = 0)$$

$$\forall xyz(x \cdot (y + z) = x \cdot y + x \cdot z) \qquad \forall x(1 \cdot x = x \ \wedge \ x \cdot 1 = x)$$

Un anillo $\mathfrak{A}$ es *conmutativo* si es modelo de $\forall xy(x \cdot y = y \cdot x)$. Un anillo $\mathfrak{A}$ es un *anillo de división* si es modelo de $\forall x(x \neq 0 \to \exists y(x \cdot y = 1))$. Un anillo de división conmutativo es llamado *campo.*

Otra estructura que se puede definir es la de la aritmética, pero esa se verá más adelante con mucho más detalle. Para ver más ejemplos de estructuras ver [18, págs. 78-85].

1.3. Teoremas principales

En esta sección se enunciarán algunos teoremas principales de la lógica de primer orden que están relacionados con el desarrollo del tema principal en el capítulo siguiente. El primero de ellos es la versión en lógica de predicados del lema 1.1.15.

Lema 1.3.1. LEMA DE SUFICIENCIA. *Si* $\Gamma \vdash \varphi$*, entonces* $\Gamma \vDash \varphi$*.*

Como su análogo, este lema se sigue de demostrar que para cada derivación $\mathcal{D}$ con hipótesis en Γ y conclusión φ se tiene que $\Gamma \vDash \varphi$, para lo cual se ocupa inducción sobre el conjunto de derivaciones[35]. Lo que muestra este resultado es que si la oración φ es demostrable a partir de Γ, entonces también es consecuencia semántica. El siguiente lema es consecuencia del anterior.

Lema 1.3.2. *Si un conjunto* Γ *tiene un modelo entonces es consistente.*

Demostración. Se supone lo contrario, si $\Gamma \vdash \bot$ entonces, por el lema anterior, se tiene que $\Gamma \vDash \bot$; por hipótesis se tiene que existe una estructura $\mathfrak{A}$ tal que $\mathfrak{A} \vDash \Gamma$, luego se cumple que $\mathfrak{A} \vDash \bot$, pues $\bot$ es consecuencia semántica de Γ, así $[\![\bot]\!]_{\mathfrak{A}} = 1$ lo cual contradice a la definición de interpretación. □

Este lema asegura que si un conjunto de oraciones tiene un modelo entonces no se pueden demostrar contradicciones a partir de él. Ahora un par de definiciones que formalizan la idea que se tiene del concepto de *teoría* y *axioma*.

Definición 1.3.3.

I. *Una* teoría T *es un conjunto de oraciones con la propiedad de ser cerrado bajo derivaciones; esto es, para cada oración* φ*, si* $T \vdash \varphi$ *entonces* $\varphi \in T$*.*

II. *Un conjunto* Γ *tal que* $T = \{\varphi \mid \Gamma \vdash \varphi\}$ *es llamado un* conjunto de axiomas *de la teoría* T*. Los elementos de* Γ *son llamados* axiomas*.*

En la parte II. de la definición se asume que el conjunto T es una teoría, no es difícil mostrar este hecho. Sea φ una oración tal que $T \vdash \varphi$, entonces, por definición de T, existen finitas oraciones $\sigma_1, \ldots, \sigma_n$ tales que $\sigma_1, \ldots, \sigma_n \vdash \varphi$ y $\Gamma \vdash \sigma_i$ para cada índice i; esto es, existen derivaciones $\mathcal{D}, \mathcal{D}_1, \ldots, \mathcal{D}_n$ tales que, para cada índice $1 \leq i \leq n$, $\mathcal{D}_i$ es una derivación con hipótesis en Γ y conclusión σ_i y $\mathcal{D}$ es una derivación con las oraciones $\sigma_1, \ldots, \sigma_n$ como hipótesis y conclusión φ. Así, existe una derivación $\mathcal{D}'$ con hipótesis en Γ y conclusión φ la cual es el resultado de colocar la derivación $\mathcal{D}$ debajo de las demás como se muestra a continuación.

$$\begin{array}{cccc} \mathcal{D}_1 & \mathcal{D}_2 & \cdots & \mathcal{D}_n \\ \sigma_1 & \sigma_2 & \cdots & \sigma_n \\ & & \mathcal{D} & \\ & & \varphi & \end{array}$$

El siguiente par de definiciones muestra relaciones entre dos teorías de diferente lenguaje.

Definición 1.3.4. *Sean* T' *y* T *dos teorías cuyos respectivos lenguaje son* L' *y* L*.*

I. T' *es una* extensión *de* T *si* $T \subseteq T'$*.*

II. T' *es una* extensión conservativa *de* T *si* $T' \cap L = T$*.*

[35] La prueba completa se encuentra en [18, pág. 89].

La primera es simplemente que la teoría T esté contenida, como conjunto de oraciones, en T', es decir, que todo teorema de T sea teorema de T'; la segunda es más fuerte pues se pide que todos los teoremas de T' que estén en el lenguaje L de T sean también teoremas de esta última. Es claro que si T' es una extensión conservativa de T entonces es también una extensión de T.

Uno de los lemas principales en la semántica de la lógica de primer orden es el lema de existencia de modelo el cual es el dual del lema 1.3.2. La demostración de este lema es bastante técnica y se basa en el hecho de que todo conjunto de oraciones Γ está contenido en la teoría $T = \{\varphi \mid \Gamma \vdash \varphi\}$ y esta, a su vez, está contenida en una teoría maximalmente consistente $T^\star$ (cuya existencia se muestra directamente del lema de Zorn-Kuratowski[36].) y que el lenguaje mismo de $T^\star$ es un conjunto del cual se puede definir un modelo para Γ, esto es, se muestra que si Γ es un conjunto es consistente se puede exhibir una estructura explícita, cuyo universo es un conjunto cociente de los términos cerrados en $T^\star$, que sea modelo de Γ.

Lema 1.3.5. LEMA DE EXISTENCIA DE MODELO. *Si Γ es un conjunto consistente de oraciones entonces tiene un modelo.*

De la demostración del anterior lema[37] se sigue de inmediato una versión más precisa del mismo. Para enunciarlo se define la *cardinalidad de un lenguaje* L, denotado por $|L|$, como el cardinal $\aleph_0$ si L tiene finitas constantes y si el lenguaje tiene $\kappa \geq \aleph_0$ contantes, entonces $|L| = \kappa$.

Lema 1.3.6. *Sea L un lenguaje de cardinalidad κ y Γ un conjunto de oraciones en este lenguaje. Si Γ es consistente, entonces tiene un modelo de cardinalidad $\lambda \leq \kappa$.*

Este último lema, aunado al lema 1.3.2 dan la siguiente versión definitiva.

Lema 1.3.7. *Un conjunto Γ de oraciones es consistente si y solo si Γ tiene un modelo de cardinalidad a lo más la cardinalidad de su lenguaje.*

Un primer resultado que se sigue de este conveniente lema, junto con el lema 1.3.1, es el teorema de completitud; cuya primera demostración la presentó K. Gödel en el año 1930 como parte de su tesis doctoral (en [9]).

Teorema 1.3.8. TEOREMA DE COMPLETITUD.[38] *$\Gamma \vDash \varphi$ si y solo si $\Gamma \vdash \varphi$. Es decir, φ es consecuencia semántica de Γ si y solo si es demostrable a partir de Γ.*

Demostración. $\Leftarrow$) Es el lema 1.3.1.

$\Rightarrow$) Si Γ es inconsistente entonces toda fórmula es demostrable a partir de Γ (lema 1.1.18), en particular $\Gamma \vdash \varphi$, así $\Gamma \vDash \varphi$ implica a $\Gamma \vdash \varphi$.

Se supone entonces que Γ es consistente. Si ocurriese que $\Gamma \nvdash \varphi$ entonces $\Gamma \cup \{\neg\varphi\}$ es consistente, en efecto, si $\Gamma \cup \{\neg\varphi\} \vdash \bot$, al ser Γ consistente y por la regla de derivación (RAA), se tendría que $\Gamma \vdash \varphi$; luego, por el lema de existencia de modelo, $\Gamma \cup \{\neg\varphi\}$ tiene un modelo $\mathfrak{A}$, por lo que se cumple $\mathfrak{A} \vDash \Gamma$ y $\mathfrak{A} \vDash \neg\varphi$, es decir, $\mathfrak{A} \vDash \Gamma$ y $\mathfrak{A} \nvDash \varphi$ (lema 1.2.23), lo cual contradice al supuesto de que $\Gamma \vDash \varphi$. Así, $\Gamma \vDash \varphi$ implica a $\Gamma \vdash \varphi$. □

Existe otra manera de demostrar al lema 1.3.5 de tal manera que, utilizando el teorema de completitud (habiéndolo demostrado sin utilizar este lema), el argumento es bastante corto, sin embargo solo muestra (de manera indirecta) la existencia de un modelo para un conjunto consistente de oraciones y no da más información, con lo cual no se podría llegar al enunciado del lema 1.3.7 que es bastante útil pues da información sobre el modelo. A continuación, y con el fin de exponer un ejemplo de las diferencias entre una prueba directa y otra indirecta, se muestra el lema de existencia de modelo.

[36] Ver A.1.20.
[37] La cual se puede encontrar en [18, cap. 4.1].
[38] Se puede encontrar una demostración de carácter semántico de este resultado en [1].

Lema 1.3.9. *Si Γ es un conjunto consistente de oraciones entonces tiene un modelo.*

Demostración. Por contradicción. Se supone que Γ no tiene modelo; sea φ cualquier oración dentro de su lenguaje, entonces se sigue por vacuidad que $\Gamma \vDash \varphi \wedge \neg\varphi$, ocupando el teorema de completitud se tiene que $\Gamma \vdash \varphi \wedge \neg\varphi$ con lo cual $\Gamma \vdash \bot$ y entonces Γ es inconsistente, contradiciendo la hipótesis. □

Otro resultado importante que es inmediato del lema de existencia de modelo es el importante para la lógica (e imprescindible para el desarrollo del segundo capítulo) teorema de compacidad.

Teorema 1.3.10. TEOREMA DE COMPACIDAD. *Un conjunto Γ tiene un modelo si y solo si cada subconjunto finito de Γ tiene un modelo.*

Es claro que el teorema de compacidad es trivial para cuando $|\Gamma| < \aleph_0$, sin embargo para cuando Γ es infinito es un teorema muy útil. Para su demostración se ocupará una formulación equivalente: Γ no tiene modelo si y solo si algún $\Delta \subseteq \Gamma$ finito no tiene modelo.

Demostración. $\Leftarrow$) Se supone que existe $\Delta \subseteq \Gamma$ finito tal que no tiene modelo. Si Γ tuviera un modelo $\mathfrak{A}$, entonces, por definición, $\mathfrak{A}$ sería modelo de Δ puesto que $\Delta \subseteq \Gamma$. En general, si $\Gamma_2 \subseteq \Gamma_1$ son conjuntos de oraciones del mismo lenguaje, cualquier modelo de Γ_1 es modelo de Γ_2.

$\Rightarrow$) Se supone que Γ no tiene modelo. Por el lema de existencia de modelo se tiene que Γ es inconsistente, por lo que existen $\sigma_1, \ldots, \sigma_n \in \Gamma$ tales que $\sigma_1, \ldots, \sigma_n \vdash \bot$. Esto muestra que $\Delta = \{\sigma_1, \ldots, \sigma_n\}$ es inconsistente y, por el lema 1.3.2, no tiene modelo. □

Para demostrar el siguiente teorema hace falta la definición para cuando una estructura $\mathfrak{B}$ sea una *expansión* de $\mathfrak{A}$. Por ejemplo, sea $\mathfrak{A} = \langle \mathbb{R}, +, 0\rangle$ la estructura de los reales como grupo aditivo, se le puede agregar la función producto $(\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R})$ y la constante uno (1) para así tener la estructura de anillo para los reales, $\mathfrak{B} = \langle \mathbb{R}, +, \cdot, 0, 1\rangle$; así, *expandir* una estructura es conservar el mismo universo y agregar posibles relaciones, posibles funciones y posibles constantes.

Definición 1.3.11. *Sean $\mathfrak{A}$ y $\mathfrak{B}$ estructuras. Se dirá que $\mathfrak{A}$ es una* reducción *de $\mathfrak{B}$ (o que $\mathfrak{B}$ es una* expansión *de $\mathfrak{A}$) si $|\mathfrak{A}| = |\mathfrak{B}|$ y toda relación, toda función y toda constante de $\mathfrak{A}$ es también relación, función y constante de $\mathfrak{B}$. Se ocupará la notación $\langle \mathfrak{A}, S_1, \ldots, S_n, g_1, \ldots, g_m, \{a_j \mid j \in J\}\rangle$ para hacer referencia a una expansión de $\mathfrak{A}$ indicando las relaciones, funciones y constantes extras.*

La siguiente proposición es directa de la definición anterior y se muestra ocupando inducción sobre las oraciones.

Proposición 1.3.12. *Sea $\mathfrak{A}$ una estructura con lenguaje L que es reducción de $\mathfrak{B}$. Se cumple que $\mathfrak{A} \vDash \sigma$ si y solo si $\mathfrak{B} \vDash \sigma$ para cualquier oración σ del lenguaje L.*

Teorema 1.3.13. SKOLEM-LÖWENHEIM DESCENDENTE *Sea Γ un conjunto de oraciones en un lenguaje de cardinalidad κ y sea λ un cardinal tal que $\kappa < \lambda$. Si Γ tiene un modelo de cardinalidad λ, entonces Γ tiene un modelo de cardinalidad κ' para cualquier cardinal κ' tal que $\kappa \leq \kappa' < \lambda$.*

Demostración. Sea L el lenguaje de Γ. Sea L' el lenguaje que extiende a L y que resulta de agregar el conjunto $\{c_i \mid i \in I\}$ de κ' nuevas constantes (es decir, que no están en el alfabeto de L). Sea $\Gamma' = \Gamma \cup \{c_i \neq c_j \mid i, j \in I \text{ y } i \neq j\}$ del lenguaje L'. Se mostrará que Γ' tiene un modelo.

Por hipótesis existe un modelo $\mathfrak{A}$ de Γ de cardinalidad λ. Sea $\mathfrak{A}'$ la expansión de $\mathfrak{A}$ que resulta al agregar κ' constantes distintas (esto es posible pues $\kappa' < \lambda$, y así existe un subconjunto A de $|\mathfrak{A}|$ con cardinalidad κ'). Por la proposición anterior, $\mathfrak{A}'$ es modelo de Γ además, $\mathfrak{A}' \vDash c_i \neq c_j$ para toda $i, j \in I$ con $i \neq j$, por lo tanto, $\mathfrak{A}'$ es modelo de Γ'.

La cardinalidad de L' es κ'. Por el lema de existencia de modelo, Γ' tiene un modelo $\mathfrak{B}'$ de cardinalidad menor o igual que κ', por otro lado, los axiomas $c_i \neq c_j$ implican que $\mathfrak{B}'$ tiene cardinalidad mayor o igual que κ'; así, $\mathfrak{B}'$ tiene cardinalidad κ'. Por último, sea $\mathfrak{B}$ la reducción de $\mathfrak{B}'$ al lenguaje L, entonces por la proposición anterior $\mathfrak{B}$ es modelo de Γ. □

Sea $\mathcal{K}$ una clase[39] de estructuras, del mismo tipo de similitud fijo, entonces se define la *teoría de* $\mathcal{K}$ como el conjunto $Th(\mathcal{K}) = \{\sigma \mid \mathfrak{A} \vDash \sigma \text{ para cada } \mathfrak{A} \in \mathcal{K}\}$. En el caso de que $\mathcal{K}$ esté constituida por una sola estructura, es decir $\mathcal{K} = \{\mathfrak{A}\}$, se ocupará la notación $Th(\mathfrak{A})$. Sea $\mathfrak{R} = \langle \mathbb{R}, +, \cdot, ^{-1}, 0, 1\rangle$ la estructura de campo para los números reales. Entonces, como consecuencia del teorema anterior, la *teoría de los números reales*, es decir $Th(\mathfrak{R})$, tiene un modelo numerable.

Teorema 1.3.14. SKOLEM-LÖWENHEIM ASCENDENTE *Sea Γ un conjunto de oraciones en un lenguaje de cardinalidad κ y sea $\mathfrak{A}$ un modelo de Γ con cardinalidad $\lambda \geq \kappa$. Para cualquier $\mu > \lambda$, Γ tiene un modelo de cardinalidad μ.*

Demostración. Sea L el lenguaje de Γ. Sea L' el lenguaje que extiende a L y que resulta de agregar el conjunto $\{c_i \mid i \in I\}$ de μ nuevas constantes. Sea $\Gamma' = \Gamma \cup \{c_i \neq c_j \mid i, j \in I \text{ y } i \neq j\}$ del lenguaje L'. Se mostrará que Γ' tiene un modelo ocupando el teorema de compacidad.

Sea $\Delta \subseteq \Gamma$ finito. Sea $\{c_{i_0}, \ldots, c_{i_k}\}$ el conjunto de constantes que aparecen en los nuevos axiomas dentro del conjunto Δ, es decir, son las constantes que aparecen en el conjunto $\Delta \cap (\Gamma' \setminus \Gamma)$. Sea $\Gamma_0 = \Gamma \cup \{c_{i_p} \neq c_{i_q} \mid p, q \leq k\}$, entonces $\Delta \subseteq \Gamma_0$. Cualquier modelo de Γ_0 es modelo de Δ.

Sea ahora $\mathfrak{A}' = \langle \mathfrak{A}, a_1, \ldots, a_k\rangle$ la expansión de $\mathfrak{A}$ que resulta al agregar k constantes distintas (puede ocurrir que no se puedan agregar estas constantes, esto ocurre por ejemplo cuando $\lambda = \kappa$ y todo elemento de $|\mathfrak{A}|$ es una constante en $\mathfrak{A}$, lo cual en realidad no importa, pues la expansión $\mathfrak{A}'$ es en realidad $\mathfrak{A}$). Claramente $\mathfrak{A}'$ es modelo de Δ puesto que es modelo de Γ_0. Por el teorema de compacidad, existe $\mathfrak{B}$ modelo de Γ'. Sea $\mathfrak{B}$ la reducción de $\mathfrak{B}'$ al lenguaje L, entonces $\mathfrak{B}$ es modelo de Γ; además, por las oraciones extras de Γ' se tiene que la cardinalidad de $\mathfrak{B}'$, y por lo tanto la de $\mathfrak{B}$, es mayor igual que μ. Si fuera igual a μ se obtiene el resultado, si fuese estrictamente mayor que μ se aplica el teorema de Skolem-Löwenheim descendente para mostrar la existencia de un modelo con este cardinal. □

Así como en el álgebra dos estructuras isomorfas son indistinguibles pues solo difieren en la naturaleza de los objetos, se tendrá una definición similar para estructuras en la lógica en el sentido de que $\mathfrak{A}$ y $\mathfrak{B}$ serán (lógicamente) indistintas si modelan exactamente las mismas oraciones de un lenguaje.

Definición 1.3.15. *Las estructuras $\mathfrak{A}$ y $\mathfrak{B}$ son* elementalmente equivalentes *en un lenguaje L si para toda oración σ de L se cumple que $\mathfrak{A} \vDash \sigma$ si y solo si $\mathfrak{B} \vDash \sigma$. Si este es el caso se ocupa la notación $\mathfrak{A} \equiv \mathfrak{B}$.*

Definición 1.3.16. *Sean $\mathfrak{A}$ y $\mathfrak{B}$ del mismo tipo. Una función $f : |\mathfrak{A}| \to |\mathfrak{B}|$ es un* isomorfismo *si*

- *f es biyectiva,*
- *para cada símbolo predicado P_i, $(a_1, \ldots, a_k) \in P_i^{\mathfrak{A}}$ si y solo si $(a_1, \ldots, a_k) \in P_i^{\mathfrak{B}}$,*
- *para cada símbolo funcional F_j, $f(F_j^{\mathfrak{A}}(a_i, \ldots, a_k)) = F_j^{\mathfrak{B}}(f(a_i), \ldots, f(a_k))$, y*
- *para cada símbolo constante c_i, $f(c_i^{\mathfrak{A}}) = c_i^{\mathfrak{B}}$.*

Se dirá que $\mathfrak{A}$ es **isomorfa** a $\mathfrak{B}$, y en este caso se ocupará la notación $\mathfrak{A} \cong \mathfrak{B}$.

[39] En el sentido de la teoría de conjuntos en ZFC, esto es, una *colección* de conjuntos que no necesariamente es un conjunto.

Lema 1.3.17. *Si $\mathfrak{A} \cong \mathfrak{B}$ entonces $\mathfrak{A} \equiv \mathfrak{B}$ (isomorfo implica elementalmente equivalente).*

El anterior lema se muestra por inducción sobre el lenguaje. En la matemática se ocupa a menudo el prefijo *sub*, así se tiene la noción de subgrupo, subanillo, subespacio, etc. Sean por ejemplo $\mathfrak{R} = \langle \mathbb{R}, +, \cdot, ^{-1}, 0, 1\rangle$ y $\mathfrak{Q} = \langle \mathbb{Q}, +, \cdot, ^{-1}, 0, 1\rangle$ las estructuras de campo para los reales y racionales respectivamente, se dice entonces que $\mathfrak{Q}$ es una *subestructura* de $\mathfrak{R}$ pues $\mathbb{Q} \subseteq \mathbb{R}$ y las funciones en los reales son una extensión de las funciones en los racionales. En general si tiene la siguiente definición.

Definición 1.3.18. *Sean $\mathfrak{A}$ y $\mathfrak{B}$ estructuras del mismo tipo. $\mathfrak{A}$ es una* subestructura *(*submodelo*) de $\mathfrak{B}$ si $|\mathfrak{A}| \subseteq |\mathfrak{B}|$ y para los símbolos del alfabeto de su lenguaje se cumple*

- $P_i^{\mathfrak{B}} \cap |\mathfrak{A}|^{n_i} = P_i^{\mathfrak{A}}$ *donde n_i es el número de argumentos para P_i.*
- $F_j^{\mathfrak{B}}|_{|\mathfrak{A}|^{n_j}} = F_j^{\mathfrak{A}}$ *donde n_j es el número de argumentos para F_j.*
- $c_i^{\mathfrak{B}} = c_i^{\mathfrak{A}}$.

Si $\mathfrak{A}$ es subestructura de $\mathfrak{B}$ se ocupará la notación $\mathfrak{A} \subseteq \mathfrak{B}$.

La noción que se dio de elementalmente equivalente solo requiere que las oraciones (las cuales no hacen referencia a ningún elemento del universo, salvo las constantes) fueran simultáneamente verdaderas en ambas estructuras. La siguiente definición lleva esta noción más lejos permitiendo hacer referencia a los elementos de una estructura.

Definición 1.3.19. *Una estructura $\mathfrak{A}$ es una* subestructura elemental *de $\mathfrak{B}$ (o de manera equivalente, $\mathfrak{B}$ es una* extensión elemental *de $\mathfrak{A}$) si $\mathfrak{A} \subseteq \mathfrak{B}$ y para toda fórmula $\varphi(x_1, \ldots, x_n)$ con n variables libres del lenguaje L se cumple que para todos $a_1, \ldots, a_n \in |\mathfrak{A}|$, $\mathfrak{A} \vDash \varphi(\bar{a}_1, \ldots, \bar{a}_n)$ si y solo si $\mathfrak{B} \vDash \varphi(\bar{a}_1, \ldots, \bar{a}_n)$.*

Si la definición anterior se cumple se ocupará la notación $\mathfrak{A} \prec \mathfrak{B}$, lo cual quiere decir que $\mathfrak{A}$ es subestructura de $\mathfrak{B}$ y además hacen verdaderas a las mismas oraciones del lenguaje con parámetros en el universo de $\mathfrak{A}$. Es claro que $\mathfrak{A} \prec \mathfrak{B}$ implica $\mathfrak{A} \equiv \mathfrak{B}$, además, no es difícil encontrar un contraejemplo para mostrar que no se tiene la otra implicación.

Puede ocurrir que una estructura $\mathfrak{A}$ sea tal que es isomorfa a una subestructura de $\mathfrak{B}$; acorde a la definición no se puede afirmar que $\mathfrak{A}$ es una subestructura de $\mathfrak{B}$, pero el hecho de tener una *copia* dentro de ésta hace que $\mathfrak{A}$ esté *isomórficamente encajada*; así se puede ampliar la notación $\mathfrak{A} \subseteq \mathfrak{B}$ a este caso, en el sentido de identificar a $\mathfrak{A}$ con su imagen bajo el isomorfismo. Similarmente, se dirá que $\mathfrak{A}$ es un *encaje elemental* de $\mathfrak{B}$ si existe una estructura $\mathfrak{A}'$ tal que $\mathfrak{A} \cong \mathfrak{A}'$ y $\mathfrak{A}' \prec \mathfrak{B}$; de nuevo, se generalizará la notación $\mathfrak{A} \prec \mathfrak{B}$ para cuando $\mathfrak{A}$ esté *elementalmente encajado* en $\mathfrak{B}$.

De manera similar a la definición 1.2.18, una estructura $\mathfrak{A}$ se puede extender añadiendo a todos los elementos de su universo como constantes, a esta extensión de $\mathfrak{A}$ se le denotará $\widehat{\mathfrak{A}}$; es decir, $\widehat{\mathfrak{A}} = \langle \mathfrak{A}, |\mathfrak{A}|\rangle$. Ocurre además que el lenguaje de $\widehat{\mathfrak{A}}$ es $L(\mathfrak{A})$.

Por último, se mencionarán un par de resultados que fortalecen a los teoremas de Skolem-Löwenheim y que se pueden ver en [18, pág. 117].

Teorema 1.3.20. Skolem-Löwenheim Descendente. *Sea $\mathfrak{A}$ una estructura cuyo lenguaje es L. Si $\mathfrak{A}$ tiene cardinalidad λ y $|L| = \kappa$ con $\lambda \geq \kappa$ entonces existe una estructura $\mathfrak{B}$ de cardinalidad κ tal que $\mathfrak{B} \prec \mathfrak{A}$.*

Teorema 1.3.21. Skolem-Löwenheim Ascendente. *Sea $\mathfrak{A}$ una estructura cuyo lenguaje es L. Si $\mathfrak{A}$ tiene cardinalidad λ y $|L| = \kappa$ con $\lambda \geq \kappa$ entonces para cada $\mu > \lambda$ existe una estructura $\mathfrak{B}$ de cardinalidad μ tal que $\mathfrak{A} \prec \mathfrak{B}$.*

Capítulo 2

Aritmética de primer orden

La aritmética es ampliamente conocida en el ámbito matemático y una manera formal de presentarla es mediante los *axiomas de Peano*. La forma más conocida de estos axiomas incluye la siguiente versión del *principio de inducción*: si un subconjunto A de los números naturales ($A \subseteq \mathbb{N}$) contiene al número 0 y si ocurre que para todo elemento x de A el sucesor de x también está en A ($0 \in A$ y $x \in A$ implica $s(x) \in A$) entonces $A = \mathbb{N}$. Se puede colocar este axioma en términos lógicos de la siguiente manera $\forall A(0 \in A \wedge (\forall x(x \in A \to s(x) \in A)) \to \forall x(x \in A))$, el problema de este enunciado es que no pertenece a la lógica de primer orden pues, como se mencionó en el comentario siguiente a la definición 1.2.3, en lógica de predicados no se puede cuantificar sobre relaciones o funciones, en particular sobre subconjuntos del universo. Así, la manera de estudiar a la aritmética será desde el enfoque de primer orden, donde se modificará el principio de inducción de segundo orden para convertirlo en un *esquema axiomático* de primer orden.

Así, en este capítulo se definirá la aritmética de primer orden y se ahondará en ella presentando resultados que se enfocan principalmente en la existencia y descripción de las estructuras llamadas *modelos no-estándar*.

2.1. Axiomas de Peano

A lo largo del siglo XIX, algunos matemáticos se dieron cuenta de que gran parte de la matemática descansa en la teoría de los números naturales, esto debido a que la rama matemática conocida como *análisis* (la cual está constituida por el cálculo, la geometría analítica, la teoría de ecuaciones diferenciales y los números complejos, entre otros) se basa en la estructura de los números reales y, en aquellos años, se llegó a la conclusión de que el conjunto $\mathbb{R}$ y sus propiedades se puede deducir a partir de los números naturales[1]. Los matemáticos entonces se interesaron más en la aritmética y, en particular, en la manera de axiomatizarla, es por ello que en el año 1888 R. Dedekind propuso un sistema axiomático de los números naturales que, de manera más precisa, G. Peano presentó en su libro *Arithmetices principia, nova methodo exposita* ([16]) un año después. Es por ello que los hoy conocidos axiomas de Peano (o postulados de Peano) también son llamados axiomas de Dedekind-Peano.

Para la formulación de dichos axiomas hacen falta las nociones primitivas de *número natural*, *0* y *sucesor*; sin embargo, en un lenguaje lógico éstas se pueden formular ocupando únicamente oraciones sintácticas sin necesidad de recurrir a un significado *a priori*. Como se mencionó anteriormente, los

[1] Una construcción, de naturaleza analítica dentro de ZFC, de los números reales se puede consultar en [10, cap. 6] y otra, de carácter más conjuntista, en [14, cap. 3-4].

enunciados originales contienen al axioma del principio de inducción que no puede ser expresado, como un solo axioma, en la lógica de primer orden. Por ese motivo, en este contexto se tendrá una definición adaptada de axiomas de Peano; primero se hará mención del lenguaje de la aritmética.

Definición 2.1.1. *El* lenguaje de la aritmética *(*$\mathrm{L_A}$*) es del tipo* $\langle -; 2, 2, 1; 1\rangle$ *y su alfabeto está constituido por los siguientes símbolos.*

- *Símbolos predicados:* $=$.
- *Símbolos funcionales:* $+$, $\cdot$, s.
- *Símbolos constantes:* 0.

Definición 2.1.2. *Las siguientes oraciones dentro del lenguaje* $\mathrm{L_A}$ *son llamadas los* axiomas de Peano *(*de primer orden*).*

$$\forall x(0 \neq s(x))$$

$$\forall xy(s(x) = s(y) \to x = y)$$

$$\forall x(x + 0 = x)$$

$$\forall xy(x + s(y) = s(x + y))$$

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

$$\forall x(x \cdot s(y) = x \cdot y + x)$$

$$\varphi(0) \ \wedge \ \forall x(\varphi(x) \to \varphi(s(x))) \to \forall x\varphi(x)$$

Al conjunto de los axiomas de Peano se le denotará con PA. El primero de estos se interpreta como *0 no es el sucesor de ningún elemento del universo*, el segundo básicamente expresa que la función unaria *sucesor* es inyectiva. El siguiente par muestra propiedades sobre la suma, y el siguiente par sobre el producto. El último de ellos no es, como se previó, un axioma, pues no es una oración del lenguaje, sino que es una expresión del meta-lenguaje la cual representa un conjunto infinito (numerable) de oraciones (una por cada oración φ en $\mathrm{L_A}$); a este tipo de expresiones se le conoce como *esquema axiomático*. Así, el esquema axiomático de PA expresa que, dada una oración $\varphi(x)$ del lenguaje, si en una estructura adecuada $\varphi(0)$ es verdadera y si siempre que un elemento tiene la propiedad expresada en φ entonces el sucesor de ese elemento también, entonces todo elemento del universo de la estructura tiene dicha propiedad. De lo anterior se tiene que los axiomas de Peano, en lógica de primer orden, son infinitos; es decir, $|\mathrm{PA}| = \aleph_0$.

Se puede pensar que el esquema axiomático de primer orden es *equivalente* al enunciado original, en el sentido de que para todo subconjunto A de los naturales se puede encontrar una oración φ tal que $x \in A$ si y solo si $\varphi(x)$, en otras palabras, que todo subconjunto sea de la forma $A = \{x \mid \varphi(x)\}$. Esto no es cierto y una manera sencilla de darse cuenta de ello es que existen $2^{\aleph_0}$ subconjuntos de los naturales y en lenguaje de la aritmética (de primer orden) solo se pueden construir $\aleph_0$ oraciones. Lo que se obtiene de esto es que existen numerables subconjuntos *especiales* pues pueden ser definidos mediante una oración de primer orden (estos conjuntos son conocidos como *conjuntos definibles* en $\mathrm{L_A}$), pero los otros, que son la mayoría, no tienen esta propiedad.

Se enuncian a continuación algunas oraciones que son consecuencias semánticas de los axiomas, lo cual quiere decir que se validan en toda *estructura aritmética* (definición 2.2.1).

Proposición 2.1.3. *Las siguientes son consecuencias semánticas de* PA.

a) $\forall x(x = 0 \ \vee \ \exists y(x = s(y)))$

b) $\forall xyz(x + (y + z) = (x + y) + z)$

c) $\forall xy(x + y = y + x)$

d) $\forall xyz(x + z = y + z \to x = y)$

e) $\forall xyz(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$

f) $\forall xy(x \cdot y = y \cdot x)$

g) $\forall xyz(z \neq 0 \to (x \cdot z = y \cdot z \to x = y))$

h) $\forall xyz(x \cdot (y + z) = x \cdot y + x \cdot z)$

Demostración. Para mostrar esta proposición se ocupa el teorema de completitud (teorema 1.3.8), así, basta dar una demostración formal (derivación) de cada una de las oraciones tomando como hipótesis los axiomas de Peano. La prueba de cada uno de ellos es similar, así solo se presentarán un par de ellas.

Para la parte a). Sea $\varphi(x) \equiv x = 0 \vee \exists y(x = s(y))$. Entonces se demuestra a $\varphi(0)$, pues $0 = 0$; ahora, suponiendo que $\varphi(t)$, se tiene que mostrar que $\varphi(s(t))$, lo cual es sencillo pues si $t = 0$ entonces $s(t) = s(0)$, y si $t \neq 0$ entonces, por hipótesis, $t = s(r)$ para algún término r, así $s(t) = s(s(r))$, con lo cual se tiene $\varphi(s(t))$. Para concluir se ocupa el esquema de inducción con esta oración φ, de donde $\forall x(x = 0 \ \vee \ \exists y(x = s(y)))$. Estrictamente hablando, esta no es una demostración (en el lenguaje de primer orden) de φ ocupando hipótesis en PA, es más bien una meta-demostración de lo mismo. Sin embargo, no hay problema, pues lo que se hizo fue *interpretar*, en el meta-lenguaje, lo que expresa una demostración en el sentido de esta teoría. A continuación se presenta la *demostración formal*.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{0 = 0}}{\varphi(0)} \qquad \dfrac{\dfrac{\dfrac{[\varphi(t)]}{t = 0 \vee t = s(r)} \qquad \dfrac{[t = 0]}{s(t) = s(0)}}{\exists y(s(t) = s(y))} \qquad \dfrac{[t = s(r)]}{s(t) = s(s(r))}}{\exists y(s(t) = s(y))}}{s(t) = 0 \vee \exists y(s(t) = s(y))}}{\varphi(t) \to \varphi(s(t))}}{\varphi(0) \wedge (\varphi(t) \to \varphi(s(t)))} \qquad \dfrac{}{(\varphi(0) \wedge (\varphi(t) \to \varphi(s(t)))) \to \forall x\varphi(x)}$$

$$\forall x\varphi(x)$$

Para la parte h). Se supondrá que algunos de los anteriores incisos ya fueron demostrados. Sea $\varphi(x, y, z) \equiv x(y + z) = x \cdot y + x \cdot z$, se mostrará primero que $\forall x\varphi(x, y, z)$ ocupando el esquema de inducción sobre $\varphi(x, y, z)$. Si $x = 0$ entonces, por el inciso f), $x \cdot (y + z) = 0 = 0 + 0 = x \cdot y + x \cdot z$, esto es, se demuestra $\varphi(0, y, z)$. Se supone ahora que se cumple $\varphi(x, y, z)$, luego, $s(x) \cdot (y + z) = x \cdot (y + z) + (y + z)$ y por hipótesis se tiene que $s(x) \cdot (y + z) = (x \cdot y + x \cdot z) + (y + z)$, ahora solo hace falta ocupar los incisos b) y c) para concluir que $s(x) \cdot (y + z) = s(x) \cdot y + s(x) \cdot z$, es decir, $\varphi(x, y, z) \to \varphi(s(x), y, z)$; por lo tanto $\forall x\varphi(x, y, z)$, y por último, ocupando la regla ($\forall$ I), se obtiene $\forall xyz\varphi(x, y, z)$. De nuevo, esto es solo una interpretación de una demostración en el sentido de la lógica de primer orden, pero conviene presentarla de esta manera y no como una extensa derivación. Por tal motivo, se ocuparán estás meta-demostraciones en lo que resta del escrito. □

2.2. Modelos

Definición 2.2.1. *Una estructura* $\mathfrak{A}$ *del tipo del lenguaje* $\mathrm{L_A}$ *se llamará* estructura de Peano *(*estructura aritmética *o* modelo aritmético*) si es modelo de* PA*; es decir, si* $\mathfrak{A} \vDash \mathrm{PA}$.

En este texto se ocupará el nombre *modelo aritmético* y a veces, para no sonar repetitivo, simplemente se dirá que $\mathfrak{M}$ es aritmética. Un primer resultado esperado es que el conjunto de números naturales ($\mathbb{N}$) junto con sus operaciones usuales sea una estructura aritmética; y, en efecto, lo es.

Teorema 2.2.2. *La estructura* $\mathfrak{N} = \langle \mathbb{N},\ +, \cdot, s,\ 0 \rangle$ *es aritmética*[2].

Los principales resultados para la demostración de este teorema se muestran en el apéndice A, la prueba completa se puede encontrar en [10, cap. 5]. A $\mathfrak{N}$ se le llama el **modelo estándar** de la aritmética. Por la proposición 2.1.3 se sabe que los naturales validan las oraciones allí enunciadas, lo cual no es sorprendente, sin embargo, ese resultado es más fuerte pues muestra que en todas las estructuras aritméticas, no solo en $\mathfrak{N}$, éstas son verdaderas. La pregunta entonces es, ¿$\mathfrak{N}$ es la única estructura aritmética? Considerando los axiomas originales de Peano se puede mostrar que, ocupando lógica de segundo orden y bajo ciertas consideraciones técnicas, en efecto $\mathfrak{N}$ es (salvo isomorfismo) la única estructura que modela a dichos axiomas; sin embargo, no ocurre lo mismo cuando se trabaja en lógica de primer orden. Este aspecto interesante (o anómalo) al considerar la aritmética en lógica de predicados desemboca en la aparición de nuevas estructuras *diferentes* al estándar que también son modelo de PA. Para mostrar ello, primero se precisará que se quiere decir con *diferentes*.

Definición 2.2.3. *Sea* $\mathfrak{M}$ *un modelo aritmético. Se dirá que* $\mathfrak{M}$ *es un* modelo no-estándar de la aritmética *si* $\mathfrak{M} \ncong \mathfrak{N}$.

Así, un modelo no-estándar de la aritmética es una estructura que es modelo de los axiomas de Peano pero no es isomorfo al estándar. Esto es, o bien es más que numerable[3] o bien no hay una correspondencia entre la interpretación de al menos un símbolo funcional. El lema 2.2.6 muestra una manera alterna de verificar si un modelo de PA es no-estándar. Para enunciarlo se ocupará el concepto *finito-accesible*. (El símbolo $|\mathfrak{M}|$ denota al universo de un modelo, definición 1.2.1)

Definición 2.2.4. *Sea* $\mathfrak{M}$ *un modelo aritmético, se define la* inclusión de $\mathbb{N}$ en $\mathfrak{M}$ *como la función* $\mathfrak{f} : \mathbb{N} \to |\mathfrak{M}|$ *tal que*

$$\mathfrak{f}(m) = \begin{cases} 0^{\mathfrak{M}} & \text{si } m = 0. \\ s^{\mathfrak{M}}(\mathfrak{f}(n)) & \text{si } m = s(n) \text{ para algún } n \text{ natural.} \end{cases}$$

La función inclusión $\mathfrak{f}$ está bien definida, existe y es única gracias al teorema de recursión de ZFC (teorema A.2.8). Como se verá en esta sección, esta función es importante para mostrar ciertos aspectos sobre los modelos no-estándar.

Definición 2.2.5. *Sea* $\mathfrak{M}$ *un modelo aritmético y* $\mathfrak{f}$ *la función inclusión. Un elemento* $a \in |\mathfrak{M}|$ *se llamará* finito-accesible *si* $a \in \mathfrak{f}(\mathbb{N})$*; el conjunto* $\mathfrak{f}(\mathbb{N})$ *es el* conjunto finito-accesible de $\mathfrak{M}$ *y se le denota con* $FA(\mathfrak{M})$.

Así, un elemento a dentro del universo de un modelo aritmético es finito-accesible si, o bien es la constante cero, o bien es igual al resultado de aplicar un número finito de veces la operación sucesor a la constante cero. Cuando $\mathfrak{M} = \mathfrak{N}$ entonces $\mathfrak{f}$ es la función identidad, así, es claro que todo elemento del modelo estándar es finito-accesible; sin embargo, como se comentará después del teorema 2.2.8, esta propiedad no es inherente a los modelos aritméticos.

[2] Se están ocupando los mismos símbolos del lenguaje formal para denotar a las funciones $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ y $s : \mathbb{N} \to \mathbb{N}$ (teoremas A.2.10 y A.2.11); de nuevo, esto es un usual abuso del lenguaje, empero, se debe tener en cuenta el contexto de los símbolos para deducir su naturaleza. Ver apéndice A.2 para más detalles.

[3] De la proposición 2.3.1 se sigue que ningún modelo aritmético es finito.

Lema 2.2.6. *Sea $\mathfrak{M}$ tal que $\mathfrak{M} \vDash$ PA, entonces $\mathfrak{M}$ es no-estándar si y solo si existe $a \in |\mathfrak{M}|$ tal que a no es finito-accesible.*

Se presenta la prueba al enunciado equivalente de este lema: Si $\mathfrak{M} \vDash$ PA, entonces $\mathfrak{M} \cong \mathfrak{N}$ si y solo si todo $a \in |\mathfrak{M}|$ es finito-accesible por $s^{\mathfrak{M}}$ sobre $0^{\mathfrak{M}}$.

Demostración. $\Rightarrow$) Por hipótesis, existe un isomorfismo $f : \mathbb{N} \to |\mathfrak{M}|$. Como f es biyectiva, todo elemento $a \in |\mathfrak{M}|$ se puede indizar con el único número natural n tal que $f(n) = a$; así, se tiene que $|\mathfrak{M}| = \{a_n \mid n \in \mathbb{N}\} = \{a_0, a_1, a_2, \ldots\}$. Más aún, se puede inducir un buen orden $\prec$ (definición A.2.13) en $|\mathfrak{M}|$ donde $a_n \prec a_m$ si y solo si $n < m$ (el orden usual de $\mathbb{N}$) para $a_n, a_m \in |\mathfrak{M}|$.

Si $X = |\mathfrak{M}| \setminus FA(\mathfrak{M}) \neq \emptyset$ entonces X tiene un elemento mínimo a_m en el orden $\prec$, como $a_0 = f(0) = 0^{\mathfrak{M}} \in FA(\mathfrak{M})$ se tiene que $m \neq 0$, entonces $m = s(n)$ para algún n natural. Como a_m es el mínimo de X, $a_n \in FA(\mathfrak{M})$, es decir, a_n es finito-accesible, pero por su definición también $s^{\mathfrak{M}}(a_n)$ es finito-accesible, luego $s^{\mathfrak{M}}(a_n) = s^{\mathfrak{M}}(f(n)) = f(s(n)) = f(m) = a_m$ pues f es un isomorfismo, contradiciendo la condición sobre a_m. Así $X = \emptyset$, con lo cual $|\mathfrak{M}| = FA(\mathfrak{M})$.

$\Leftarrow$) Por hipótesis se tiene que todo $a \in |\mathfrak{M}|$ es finito-accesible. Se mostrará que la función inclusión $\mathfrak{f}$ es, en este caso, un isomorfismo.

Por definición, $\mathfrak{f}(0) = 0^{\mathfrak{M}}$ y $\mathfrak{f}(s(n)) = s^{\mathfrak{M}}(\mathfrak{f}(n))$ para cada n natural. Sea $n \in \mathbb{N}$ arbitrario y fijo, se demostrará por inducción sobre el natural m que $\mathfrak{f}(n + m) = \mathfrak{f}(n) +^{\mathfrak{M}} \mathfrak{f}(m)$; si $m = 0$ se tiene que $\mathfrak{f}(n + 0) = \mathfrak{f}(n) = \mathfrak{f}(n) +^{\mathfrak{M}} 0^{\mathfrak{M}} = \mathfrak{f}(n) +^{\mathfrak{M}} \mathfrak{f}(0)$ pues $\mathfrak{M}$ es aritmética, luego se supone que $\mathfrak{f}(n + m) = \mathfrak{f}(n) +^{\mathfrak{M}} \mathfrak{f}(m)$ para algún m natural, ocupando de nuevo el hecho de que $\mathfrak{M} \vDash$ PA se cumple entonces que $\mathfrak{f}(n + s(m)) = \mathfrak{f}(s(n + m)) = s^{\mathfrak{M}}(\mathfrak{f}(n + m)) = s^{\mathfrak{M}}(\mathfrak{f}(n) +^{\mathfrak{M}} \mathfrak{f}(m)) = \mathfrak{f}(n) +^{\mathfrak{M}} s^{\mathfrak{M}}(\mathfrak{f}(m)) = \mathfrak{f}(n) +^{\mathfrak{M}} \mathfrak{f}(s(m))$; con lo cual queda demostrado. Ocupando esto, es similar la prueba de que $\mathfrak{f}(n \cdot m) = \mathfrak{f}(n) \cdot^{\mathfrak{M}} \mathfrak{f}(m)$ para todo $n, m \in \mathbb{N}$.

Falta entonces mostrar que $\mathfrak{f}$ es biyectiva. Sean $n, m \in \mathbb{N}$ tales que $\mathfrak{f}(n) = \mathfrak{f}(m)$, sin pérdida de generalidad se supone que $n \leq m$, es decir, existe un natural k tal que $m = n + k$; por lo anterior se tiene que $\mathfrak{f}(n) = \mathfrak{f}(m)$ si y solo si $\mathfrak{f}(n) = \mathfrak{f}(n) +^{\mathfrak{M}} \mathfrak{f}(k)$, como $\mathfrak{M}$ es aritmética $\mathfrak{f}(n) = \mathfrak{f}(n) + 0^{\mathfrak{M}}$ y, por la proposición 2.1.3, se tiene que $0^{\mathfrak{M}} = \mathfrak{f}(k)$. Por último, dada la definición de la función inclusión, $\mathfrak{f}(m) = 0^{\mathfrak{M}}$ si y solo si $m = 0$ pues si $m = s(n)$, $\mathfrak{f}(m) = s^{\mathfrak{M}}(\mathfrak{f}(n))$ y $0^{\mathfrak{M}}$ no es sucesor de ningún elemento de $|\mathfrak{M}|$; así $\mathfrak{f}(n) = \mathfrak{f}(m)$ implica $k = 0$, esto es $n = m$, con lo cual $\mathfrak{f}$ es inyectiva.

Mostrar que $\mathfrak{f}$ es suprayectiva es directo de la suposición, puesto que todo elemento $a \in |\mathfrak{M}|$ sea finito-accesible significa que $\mathfrak{f}(\mathbb{N}) = |\mathfrak{M}|$, de donde $\mathfrak{f}$ es suprayectiva. □

De la segunda parte de esta última demostración, puesto que la hipótesis solo se utiliza para mostrar que $\mathfrak{f}$ es suprayectiva, se mostró de manera implícita que el conjunto finito-accesibles FA es una subestructura de $\mathfrak{M}$ (puesto que es cerrado bajos las tres operaciones) y además la función inclusión $\mathfrak{f}$ es un isomorfismo entre el modelo estándar y esta subestructura. En resumen, se mostró el siguiente corolario.

Corolario 2.2.7. *Sean $\mathfrak{M}$ un modelo aritmético y $\oplus$, $\odot$, σ las funciones $+^{\mathfrak{M}}$, $\cdot^{\mathfrak{M}}$ y $s^{\mathfrak{M}}$ restringidas al conjunto $FA(\mathfrak{M})$ respectivamente. Entonces $\langle FA(\mathfrak{M}),\ \oplus, \odot, \sigma,\ 0^{\mathfrak{M}} \rangle$ es una subestructura isomorfa a $\mathfrak{N}$.*

A los elementos de $FA(\mathfrak{M})$ también se les llamará **elementos** (o **números**) **estándar**, es decir, los elementos estándar de un modelo no-estándar son precisamente los finito-accesibles. De manera análoga, si $a \in |\mathfrak{M}|$ no es finito-accesible se dirá que es un **elemento no-estándar**.

En lo venidero se utilizarán términos en $\mathrm{L_A}$ de la forma $s(s(\cdots s(0)\cdots))$ donde el símbolo funcional s aparece un número finito de veces (idea similar a la noción de finito-accesible), por ello conviene tener una notación que simplifique la escritura[4]. Se define la función $\bar{\cdot} : \mathbb{N} \to \mathrm{TERM}_c(\mathrm{L_A})$ de manera recursiva, siendo $\overline{0} = 0$ y $\overline{n+1} = s(\overline{n})$ donde $\mathrm{TERM}_c(\mathrm{L_A})$ es el conjunto de términos cerrados del lenguaje $\mathrm{L_A}$. Una vez más, esta función existe, es única y está bien definida gracias al teorema de recursión (ver teorema A.2.8).

La existencia de modelos no-estándar para la aritmética de primer orden se sigue directamente del teorema de Skolem-Löwenheim (teorema 1.3.14) puesto que $\mathfrak{N} \vDash \mathrm{PA}$ y $|\mathbb{N}| = |\mathrm{L_A}|$; más aún, se tiene la existencia de un modelo no-estándar de cardinalidad λ para cada $\lambda > \aleph_0$. Aún así, se dará una demostración de su existencia ocupando el lema anterior y el teorema de compacidad (teorema 1.3.10).

Teorema 2.2.8. *Existen modelos no-estándar de la aritmética.*

Demostración. Sea $\mathrm{L_A^\star} = \mathrm{L_A} \cup \{c\}$ la extensión del lenguaje de la aritmética que resulta al agregar un símbolo constante c. Se definen las oraciones φ_n para n un número natural como $\varphi_n \equiv c \neq \overline{n}$. Sea $\Gamma = \{\varphi \in \mathrm{L_A^\star} \mid \varphi \equiv \varphi_n \text{ para algún natural } n\}$. Así el conjunto $\mathrm{PA} \cup \Gamma \subseteq \mathrm{L_A^\star}$.

Se mostrará que $\mathrm{PA} \cup \Gamma$ tiene un modelo. Sea $\Delta \subseteq \mathrm{PA} \cup \Gamma$ finito, sea m un número natural tal que $m = 1$ si $\Delta \cap \Gamma = \emptyset$ y $m = \text{máx}\{n \mid \varphi_n \in \Delta\} + 1$ si $\Delta \cap \Gamma \neq \emptyset$, como Δ es finito m está bien definido. Se considera a la estructura $\mathfrak{N}_m = \langle \mathbb{N},\ +, \cdot, s,\ 0, m\rangle$ del mismo tipo que $\mathrm{L_A^\star}$, resulta que $\mathfrak{N}_m$ es modelo de Δ pues $\mathfrak{N} \equiv \mathfrak{N}_m$ en el lenguaje $\mathrm{L_A}$ y $\mathfrak{N}_m \vDash \varphi_n$ para toda $\varphi_n \in \Delta$ dado que $c^{\mathfrak{N}_m} = m$.

Luego, por el teorema de compacidad $\mathrm{PA} \cup \Gamma$ tiene un modelo $\mathfrak{A}$ del tipo $\langle -; 2, 2, 1; 2\rangle$. Basta considerar $\mathfrak{B}$ como la reducción de la estructura $\mathfrak{A}$ al tipo de $\mathrm{L_A}$ que se obtiene al omitir la constante $c^{\mathfrak{A}}$ (se omite como constante, pero sigue siendo un elemento de $|\mathfrak{B}|$), así $\mathfrak{B}$ es una estructura aritmética y tiene un elemento que no es finito-accesible (pues $\mathfrak{A}$ es modelo de Γ) esto es, ocupando el lema 2.2.6, $\mathfrak{B}$ es un modelo no-estándar de la aritmética. □

Del lema 2.2.6 además se sigue que en los modelos no-estándar no se cumple el principio arquimediano, pues existe al menos un elemento en su universo que no es finito-accesible. Otra manera de ver este hecho es que este principio no es expresable en lógica de primer orden; en efecto, si existiera una oración $\varphi(x)$ cuya interpretación fuera «x es finito-accesible» entonces, por el esquema de inducción de PA, todo modelo aritmético sería isomorfo a $\mathfrak{N}$, pero ya se ha demostrado que existen los no-estándar.

La segunda versión del teorema de Skolem-Löwenheim (teorema 1.3.21) implica la existencia de modelos no-estándar de la aritmética que además son extensiones elementales (bajo isomorfismo) de $\mathfrak{N}$; esto es, además de que el modelo estándar está encajado en ellos se tiene que toda oración, con los números naturales como posibles parámetros, es verdadera en $\mathfrak{N}$ si y solo si lo es en el modelo no-estándar. En efecto, se considera el conjunto de oraciones $Th(\widehat{\mathfrak{N}})$, es decir, la teoría del modelo estándar de la aritmética donde todo número natural es una constante; es claro que $\mathfrak{N} \vDash Th(\widehat{\mathfrak{N}})$ por lo que, ocupando el teorema de Skolem-Löwenheim, para $\lambda > \aleph_0$ un cardinal existe una estructura $\mathfrak{M}$, de cardinalidad λ y del tipo de $\mathrm{L_A}$, tal que $\widehat{\mathfrak{M}} \vDash Th(\widehat{\mathfrak{N}})$. Como $\mathrm{PA} \subseteq Th(\widehat{\mathfrak{N}})$ (puesto que $\mathfrak{N}$ es un modelo aritmético), se tiene que $\mathfrak{M} \vDash \mathrm{PA}$, más aún se tiene que, por un lema técnico que caracteriza a los encajes elementales (el cual se puede consultar junto a su demostración en [18, cap. 4.3]), $\mathfrak{N} \prec \mathfrak{M}$.

[4]Estas abreviaciones también pueden tratarse como constantes en cualquier modelo aritmético, pues se puede considerar el lenguaje de la aritmética extendido $\widehat{\mathrm{L_A}}$ donde cada uno de estos términos es una constante.

2.3. Orden

El teorema 2.2.8 muestra, ocupando el teorema de compacidad, la existencia de modelos no-estándar; sin embargo no da más información sobre ellos, es decir, el resultado implica que existen y solo ello. El corolario 2.2.7 da un poco de detalle, pues se sabe que existe una copia de los naturales dentro de cada uno de ellos y el párrafo anterior muestra que cierto tipo de estructuras aritméticas no solo tienen una copia de los naturales, sino que además son extensiones elementales. Más allá de eso no se tiene idea de su estructura. En esta sección se explorará un poco en los modelos no-estándar para obtener más información, definiendo en ellos un orden[5].

En lógica de primer orden, dada una teoría T con lenguaje L se pueden *definir* nuevas constantes, nuevas funciones y nuevas relaciones en ella gracias a las llamadas *expansiones de Skolem*. En donde *definir* significa dar un nuevo símbolo (que no sea parte del lenguaje) para representar cierta oración; además la nueva teoría resultante (pues se tiene un símbolo más) es conservativa sobre la anterior. Concretamente, un resultado (que se ocupará en seguida) afirma que si φ es una oración de L con $FV(\varphi) = \{x_1, \ldots, x_n\}$ como conjunto de variables libres y Q es un símbolo predicado que no sea parte de L, entonces la teoría $T^+ = T \cup \{\forall x_1 \ldots x_n(\varphi \leftrightarrow Q(x_1, \ldots, x_n))\}$ es conservativa sobre T. Es decir, dada una oración φ con n variables libres se puede ocupar un nuevo símbolo predicado para abreviarla, de tal manera que φ y $Q(x_1, \ldots, x_n)$ son equivalentes. En el apéndice B se pueden encontrar los enunciados de estos teoremas. Para detalles más técnicos sobre las *expansiones de Skolem* y el *cómo enriquecer un lenguaje* ver [18, pág. 127-131].

Entonces, se puede definir un orden (formalmente, solo es una relación binaria, sin embargo la proposición 2.3.1 muestra que en efecto es un orden) en las estructuras aritméticas de la siguiente manera, $x < y \equiv \exists z(x = y + s(z))$. Es decir, se está definiendo un orden $<$ (que se leerá como *menor que*) de tal manera que $x < y$ (x es menor que y) si y solo si existe un elemento z tal que x es igual a la suma de y con el sucesor de z. Además, se ocupará la abreviación $x \leq y$ para la oración $x < y \vee x = y$ y se ocupará $x > y$ para la oración $y < x$. Una razón de definir así el orden es que se corresponde con el orden usual del modelo estándar (teorema A.2.14), es decir, la oración $\overline{n} < \overline{m}$ del lenguaje de la aritmética se corresponde con la meta-oración $n < m$, la cual tiene su significado preciso dentro de ZFC.

Primero, algunos resultados semánticos sobre el orden recién definido.

Proposición 2.3.1. *Las siguientes oraciones son consecuencias semánticas de* PA.

a) $\forall xy(x \leq y \leftrightarrow \exists! z(y = x + z))$

b) $\forall x(0 \leq x)$

c) $\forall x(x < s(x))$

d) $\forall xy(x < y \leftrightarrow s(x) < s(y))$

e) $\forall x(\nexists y(x < y \ \wedge \ y < s(x)))$

f) $\forall xyz(x < y \wedge y < z \rightarrow x < z)$

g) $\forall xy(x < y \ \vee \ x = y \ \vee \ x > y)$

h) $\forall xy(\neg(x = y \ \wedge \ x < y) \ \wedge \ \neg(x = y \ \wedge \ x > y) \ \wedge \ \neg(x < y \ \wedge \ x > y))$

i) $\forall xyz(x < y \ \leftrightarrow \ x + z < y + z)$

[5] En [3] se pueden encontrar resultados más profundos del tema.

j) $\forall xyz(z \neq 0 \to (x < y \ \leftrightarrow \ x \cdot z < y \cdot z))$

k) $\forall xyzw(x < z \ \wedge \ y < w \to x + y < z + w)$

La demostración de esto es como en la proposición 2.1.3, es decir, se ocupa el teorema de completitud y se da la demostración de cada una de las oraciones ocupando como hipótesis los axiomas de Peano. A manera de ejemplo, se presenta la demostración de los incisos d), y g).

Demostración. d). Se tiene la siguiente cadena de doble implicación.

$x < y$ si y solo si $y = x + s(z)$ para algún z si y solo si, por inyectividad del sucesor, $s(y) = s(x + s(z))$ si y solo si, por el axioma cuatro, $s(y) = s(x) + s(z)$ si y solo si $s(x) < s(y)$.

g). Sea $\varphi(x, y) = x < y \ \vee \ x = y \ \vee \ x > y$; sea y un elemento arbitrario y fijo, se demostrará a $\varphi(x, y)$ ocupando inducción sobre x. Si $x = 0$, por el inciso b) se tiene que $0 \leq y$, de donde se tiene a $\varphi(0, y)$; se supone a $\varphi(x, y)$ para algún x, entonces hay tres casos.

I. Si $x < y$ entonces existe t tal que $y = x + s(t)$, por la parte a) de la proposición 2.1.3 $t = 0$ o $t = s(u)$ para algún termino u. Si $t = 0$ entonces $y = x + s(0) = s(x + 0) = s(x)$ de donde se tiene a $\varphi(s(x), y)$; si $t = s(u)$ entonces $y = x + s(s(u)) = s(x + s(u)) = s(s(u) + x) = s(u) + s(x) = s(x) + s(u)$, de donde $y < s(x)$ y por ende se tiene a $\varphi(s(x), y)$.

II. Si $x = y$, por la parte c) se cumple que $x < s(x)$, así $y < s(x)$ y se tiene a $\varphi(s(x), y)$.

III. Si $y < x$, por la parte c) se cumple que $x < s(x)$ y por transitividad (inciso f)) se concluye que $y < s(x)$, así se tiene a $\varphi(s(x), y)$.

En cualquier caso, $\varphi(x, y)$ implica a $\varphi(s(x), y)$; ocupando el esquema de inducción se tiene lo deseado. □

Las partes f) y g) de la proposición muestran que el orden $<$ es transitivo y lineal, respectivamente; de hecho los incisos g) y h) muestran que se tiene la propiedad de tricotomía (es decir, para cualquier par de elementos x, y se cumple una y solo una de las oraciones $x < y$, $x = y$ y $x > y$). De la parte b) se sigue que la constante 0 es el primer elemento de toda estructura aritmética; de los incisos c) y e) se tiene que el sucesor de x es el elemento inmediatamente mayor a x y los últimas oraciones muestran leyes de cancelación y conservación del orden.

De esta proposición se sigue un primer bosquejo de la estructura de un modelo no-estándar.

Lema 2.3.2. *Sea $\mathfrak{M}$ un modelo no-estándar, entonces el conjunto $FA(\mathfrak{M})$ ordenado por $<^{\mathfrak{M}}$ es un segmento inicial*[6] *de $|\mathfrak{M}|$ y además es isomorfo (en orden) a $\mathbb{N}$.*

Demostración. Se considera a la función inclusión $\mathfrak{f}$ de la subsección anterior. Por definición de $\mathfrak{f}$ y transitividad, si $n < m$ entonces $\overline{n} < \overline{m}$, como además $\mathfrak{f}$ es una biyección entonces es un isomorfismo (teorema A.1.17).

Ahora, para que sea un segmento inicial se tiene que mostrar que si a es un número no-estándar, entonces $\overline{n} < a$ para cualquier natural n, lo cual se hará ocupando el principio de (meta-)inducción. Por el inciso b) de la proposición y como a no es finito-accesible, $\overline{0} < a$; luego, si $\overline{n} < a$ para algún n entonces, por el inciso e), se tiene que $s(\overline{n}) \leq a$, como a es no-estándar no puede ocurrir la igualdad, así, $\overline{n+1} = s(\overline{n}) < a$. □

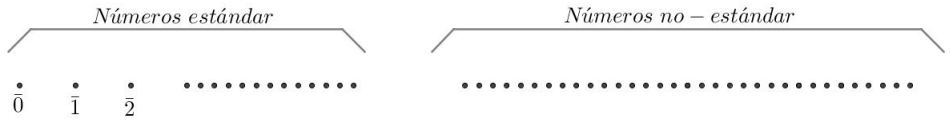


Figura 2.1: $\mathbb{N}$ como un (isomorfo a) segmento inicial de todo modelo no-estándar.

La figura sugiere que hay muchos números no-estándar. Es claro que si la cardinalidad de $\mathfrak{M}$ es $\lambda > \aleph_0$ entonces hay λ números no estándar (puesto que $|FA(\mathfrak{M})| = \aleph_0$, al ser $\mathfrak{f}$ una biyección). Si $\mathfrak{M}$ es numerable en principio solo se sabe, por el lema 2.2.6, que existe un elemento no-estándar, empero, no es difícil demostrar que existe una cantidad numerable de ellos.

Lema 2.3.3. *Sea $\mathfrak{M}$ un modelo no-estándar de* PA*, entonces existen al menos $\aleph_0$ números no-estándar en $|\mathfrak{M}|$.*

Demostración. Se adoptará la notación $NE(\mathfrak{M})$ para el conjunto $|\mathfrak{M}| \setminus FA(\mathfrak{M})$, es decir, $NE(\mathfrak{M})$ es el conjunto de los elementos no-estándar del universo $|\mathfrak{M}|$.

Se tiene, por el lema 2.2.6, que $NE(\mathfrak{M}) \neq \emptyset$. Sea $a \in NE(\mathfrak{M})$, entonces $s^{\mathfrak{M}}(a) \in NE(\mathfrak{M})$, en efecto, si $s^{\mathfrak{M}}(a)$ fuese estándar (finito-accesible) se tendría, por definición, que a también sería estándar. Así, el sucesor de un número no-estándar es no estándar. Luego, ocupando el (meta-)principio de inducción, si a es no-estándar entonces $a + \overline{n}$ es no-estándar para cualquier $n \in \mathbb{N}$.

Al final se tiene que $\{a + \overline{n} \in |\mathfrak{M}| \mid n \in \mathbb{N}\} \subseteq NE(\mathfrak{M})$ y como $|\{a + \overline{n} \in |\mathfrak{M}| \mid n \in \mathbb{N}\}| = \aleph_0$ se concluye que $\aleph_0 \leq |NE(\mathfrak{M})|$. □

Se definirá ahora la función binaria *resta aritmética* para simplificar cierta notación en la definición 2.3.5. Una vez más, esta función se puede definir gracias a los teoremas de Skolem y no hay ambigüedad en su definición debido a la unicidad del elemento z en la parte a) de la proposición 2.3.1.

Definición 2.3.4. *Sea $\mathfrak{M}$ un modelo aritmético y sean $x, y \in |\mathfrak{M}|$. Se define al elemento $x - y$ como sigue.*

$$x - y = \begin{cases} z & \textit{tal que } x = y + z \textit{ si } x \geq y \\ 0 & \textit{si } x < y \end{cases}$$

Para cuando $x \geq y$ la definición de $x - y$ es la esperada por la intuición, y definir a $x - y$ como la constante 0 en el caso $x < y$ es irrelevante. Todas las funciones de una estructura deben ser totales, es decir, deben estar definidas en todo elemento del universo, lo cual no es problema ya que primero se define la función en el conjunto apropiado (en la resta aritmética este conjunto es $\{(x, y) \in |\mathfrak{M}| \mid x \geq y\}$) y luego se define en el complemento de cualquier manera (en este caso, se ocupa la constante cero por simplicidad) puesto que en realidad no importa, ya que si se necesita excluir a los elementos de este último caso solo hace falta especificarlo en las oraciones del lenguaje (como en la oración $\forall xz(z \leq x \to (x - z) + z = x)$ del párrafo siguiente).

[6] En este caso, significa que todo número no-estándar es mayor a cualquier estándar.

Por la parte a) de la proposición 2.1.3 se tiene que todo elemento x distinto de cero en un modelo aritmético es sucesor de algún otro elemento y, más aún, este y es único dado que la función sucesor es inyectiva y puede ser llamado el *antecesor* (*inmediato*)[7] de x. Entonces, se puede decir que todo elemento tiene un único antecesor (con la convención de que el antecesor del cero es él mismo). De la definición anterior se tiene que el antecesor de x es precisamente $x - \overline{1}$, el antecesor de este es $x - \overline{2}$, y así sucesivamente. De esta definición se ocupará el hecho de que la oración $\forall xyz(z \leq x \to (x < y \leftrightarrow x - z < y - z))$ es una consecuencia semántica de los axiomas de Peano, la cual se puede interpretar como la conservación del orden entre x y y cuando se resta un número menor o igual que el más pequeño de ellos. Además, de la definición se sigue que $\forall xz(z \leq x \to (x - z) + z = x)$ también es una consecuencia semántica de PA.

Definición 2.3.5. *Sea $\mathfrak{M}$ un modelo aritmético y $a \in |\mathfrak{M}|$, se define la* clase de *a (denotada por $[a]$) como $[a] = \{x \in |\mathfrak{M}| \mid x = a + \overline{n}$ para algún natural $n\} \cup \{x \in |\mathfrak{M}| \mid x = a - \overline{n}$ para algún natural $n\}$.*

Esto es, la clase de un elemento a son todos aquellos elementos del universo que «distan» de a en un número estándar. Si $\mathfrak{M}$ es aritmética se sigue de esta definición que $FA(\mathfrak{M}) = [0]$ y que si $[a] \cap [b] \neq \emptyset$ entonces $[a] = [b]$. El siguiente resultado muestra que, restringiendo el orden a una clase de un número no-estándar, este subconjunto tiene el orden de los números enteros.

Lema 2.3.6. *Sea $\mathfrak{M}$ un modelo aritmético, si $a \in |\mathfrak{M}|$ es no-estándar, entonces el conjunto $[a]$ con el orden $<^{\mathfrak{M}}$ es isomorfo a $\mathbb{Z}$ con su orden usual.*

Demostración. Sea $i : \mathbb{Z} \to [a]$ definida como sigue.

$$i(m) = \begin{cases} a + \overline{m} & \text{si } m > 0 \\ a & \text{si } m = 0 \\ a - \overline{|m|} & \text{si } m < 0 \end{cases}$$

Si $m > 0$ entonces $\overline{0} < \overline{m}$ de donde $a < a + \overline{m}$, además, restando $\overline{m}$ en la desigualdad anterior se tiene que $a - \overline{m} < a$; en conclusión se tiene que $a - \overline{m} < a < a + \overline{m}$ para cualquier entero m positivo. Por lo que si n, m son enteros tales que $n < m$ se tiene uno de los siguientes casos.

$n = 0$. Entonces $m > 0$ y se tiene $i(n) = a < a + \overline{m} = i(m)$.

$m = 0$. Entonces $n < 0$ y se tiene $i(n) = a - \overline{|n|} < a = i(m)$.

$0 < n$. Entonces se tiene que $\overline{n} < \overline{m}$, de donde $i(n) = a + \overline{n} < a + \overline{m} = i(m)$.

$m < 0$. Entonces se tiene que $i(n) = a - \overline{|n|} < a - \overline{|m|} = i(m)$ si y solo si, sumando $\overline{|n|}$ de ambos lados, $a < a + (\overline{|n|} - \overline{|m|})$ si y solo si, ocupando cancelación, $0 < \overline{|n|} - \overline{|m|}$, lo cual es cierto, pues $|n| > |m|$.

$n < 0 < m$. Entonces $i(n) = a - \overline{|n|} < a < a + \overline{m} = i(m)$.

En cualquier caso, $n < m$ implica $i(n) < i(m)$, en particular i es inyectiva. Luego, es directo de la definición de $[a]$ el hecho de que i sea sobreyectiva. Así, i es un isomorfismo entre $\mathbb{Z}$ y $[a]$. □

Las clases serán de gran utilidad para detallar el orden aritmético. El siguiente lema muestra que todos los elementos entre dos clases distintas conservan el orden que tienen sus representantes.

Lema 2.3.7. *Sean a, b números no-estándar dentro de un modelo aritmético $\mathfrak{M}$. Entonces si $a < b$ y $[a] \cap [b] = \emptyset$ se cumple que $x < y$ para todo $x \in [a]$ y todo $y \in [b]$.*

[7] Lo de *inmediato* es por la parte e) de la proposición 2.3.1.

Demostración. Basta mostrar que $a+\overline{n} < b-\overline{m}$ para cualquier par de naturales n, m. En efecto, los tres casos restantes se siguen de este.

- Si $x = a+\overline{n}$ y $y = b+\overline{m}$ entonces $x = a+\overline{n} < b-\overline{0} = b < b+\overline{m} = y$.
- Si $x = a-\overline{n}$ y $y = b-\overline{m}$ entonces $x = a-\overline{n} < a = a+\overline{0} < b-\overline{m} = y$.
- Si $x = a-\overline{n}$ y $y = b+\overline{m}$ entonces $x = a-\overline{n} < a < b < b+\overline{m} = y$.

Sean entonces n, m números naturales. Si ocurriese que $a+\overline{n} \geq b-\overline{m}$ entonces, como $a < b$ se tiene que $a-\overline{m} < b-\overline{m}$ (pues a es no-estándar), esto es, se cumple que $a-\overline{m} < b-\overline{m} < a+\overline{n+1}$; lo cual quiere decir, dado la parte e) de la proposición 2.3.1, que $b-\overline{m} \in [a]$ (puesto que los únicos elemento entre $a-\overline{m}$ y $a+\overline{n+1}$ son de la forma $a-\overline{k}$ para $k \leq n$ o de la forma $a+\overline{j}$ para $j \leq m$) y por lo tanto $b \in [a]$. Lo cual contradice la hipótesis. Así, $a+\overline{n} < b-\overline{m}$ para cualquier par de naturales n, m. □

Para continuar se necesita introducir la notación $\frac{x}{2}$ para una operación unaria aplicada al elemento x. Para los números estándar, ésta se puede interpretar como la parte entera de su mitad; esto es, si $\overline{n}$ es un número estándar dentro de una estructura aritmética, $\frac{\overline{n}}{2}$ es igual al término $\overline{k}$ para cuando n sea par y $n = 2k$, y será igual a k' para cuando n sea impar y $n-1 = 2k'$. Aunque se ocupe la notación $\frac{x}{2}$ ésta no tiene ninguna relación con la función división que se define, por ejemplo, en los números reales; sin embargo se ocupa porque es cómoda e intuitiva.

Lema 2.3.8. *La oración* $\forall x(\exists! y(x = y+y \ \vee \ x = s(y+y)))$ *es una consecuencia semántica de* PA*, además, ese único elemento y será denotado por* $\frac{x}{2}$*.*

Demostración. Se muestra primero la existencia, luego la unicidad.

Sea $\varphi(x) \equiv \exists y(x = y+y \ \vee x = s(y+y))$, entonces se tiene a $\varphi(0)$ pues $0 = 0+0$. Se supone que $\varphi(x)$ para algún x, entonces hay dos casos. Si $x = y+y$ entonces $s(x) = s(y+y)$ y se tiene a $\varphi(s(x))$. Si $x = s(y+y)$ entonces $s(x) = s(s(y+y)) = s(s(y)+y) = s(y)+s(y)$ de donde se tiene a $\varphi(s(x))$. Así, $\varphi(x)$ implica a $\varphi(s(x))$ y del esquema de inducción se obtiene $\forall x\varphi(x)$. Además, por la parte c) de la proposición 2.3.1, solo una de las oraciones tiene que ocurrir.

Si existieran elementos y, z tales que $(x = y+y \ \vee x = s(y+y))$ y $(x = z+z \ \vee x = s(z+z))$ entonces, en principio, ocurre uno de los siguientes casos.

- $x = y+y$ y $x = z+z$. Se tiene que $\overline{2}\cdot y = \overline{2}\cdot z$, luego $y = z$.
- $x = s(y+y)$ y $x = s(z+z)$. Se tiene que $s(y+y) = s(z+z)$, entonces $y+y = z+z$ y por lo anterior $y = z$.
- $x = y+y$ y $x = s(z+z)$. Entonces $s(y+y) > s(z+z)$ por lo que $\overline{2}\cdot y > \overline{2}\cdot z$, así $y > z$; por lo tanto existe un elemento t tal que $y = z+s(t)$, entonces $z+z+s(t)+s(t) = z+z+s(0)$, de donde $s(t+s(t)) = s(0)$ y entonces $0 = t+s(t)$ lo cual es una contradicción. Por lo tanto, este caso no puede ocurrir.
- $x = s(y+y)$ y $x = z+z$. Esto lleva a una contradicción similar al caso anterior.

De lo anterior se tiene la unicidad. □

Para la demostración del siguiente teorema es necesario mostrar que la suma[8] de números no-estándar es no-estándar. Este hecho es fácil de mostrar ocupando el orden definido, pues si a y b son no-estándar y $a+b$ fuese estándar se tendría que $a+b = \overline{n}$ para algún número natural n; luego, como b no es la

[8]De hecho, también el producto. Basta con mostrar, lo cual no es difícil, que $x\cdot y \geq x$ para todo $y \geq 1$.

constante cero se tiene que $a < a + b$, de donde $a < \overline{n}$ y como los números estándar son un segmento inicial del universo en cualquier modelo aritmético, esto implicaría que a es estándar, contradiciendo la hipótesis.

Teorema 2.3.9. *Sea $\mathfrak{M}$ un modelo no-estándar. Sea $\Omega = \{[a] \mid a \in NE(\mathfrak{M})\}$, es decir el conjunto de las clases de números no-estándar en $\mathfrak{M}$; entonces la relación binaria $\ll$ definida como $[a] \ll [b]$ si y solo si $a < b$ y $[a] \cap [b] = \emptyset$ es un orden lineal en Ω que además es denso y sin puntos extremos.*

Demostración. Por el lema 2.3.7, la relación $\ll$ está bien definida en el sentido de que no depende de la elección para los representantes de $[a]$ y de $[b]$, pues como se mostró, si $a < b$ son tales que $[a] \cap [b] = \emptyset$ entonces cualquier x en la clase de a es menor a cualquier y en la clase de b.

Se mostrará que $\ll$ es un orden estricto. Primero la transitividad. Sean $a, b, c \in NE(\mathfrak{M})$ tales que $[a] \ll [b]$ y $[b] \ll [c]$, entonces $a < b$ y $b < c$ y, por la transitividad del orden $<$, se tiene que $a < c$; luego, si $[a] \cap [c] \neq \emptyset$ entonces $c = a + \overline{n}$ para algún n natural (pues $[a] = [c]$ y $a < c$), de donde $b < a + \overline{n}$ lo cual implica que $b \in [a]$ o $b < a$ contradiciendo las hipótesis, así, $[a] \cap [c] = \emptyset$ y por lo tanto $[a] \ll [c]$. Luego, $\ll$ es una relación antisimétrica pues si $[a] \ll [b]$ entonces no puede ocurrir que $a > b$ (pues por hipótesis $a < b$) y por lo tanto no puede ocurrir $[a] \gg [b]$.

Mostrar que $\ll$ es lineal es directo de la linealidad de $<$ pues si a, b son tales que $[a] \cap [b] \neq \emptyset$ entonces debe ocurrir que $a < b$ o que $b < a$ de donde se tiene que $[a] \ll [b]$ o $[b] \ll [a]$.

Sean a, b elementos no-estándar tales que $[a] \ll [b]$ y sea $c = \frac{a+b}{2}$; del lema anterior se sigue que si a, b son no-estándar entonces también lo es c. Lo primero que se mostrará es que $a < c < b$.

Si $c \leq a$ entonces hay dos casos. Si $a + b = c + c$ entonces $a + b \leq a + a$ (pues $c + c \leq a + a$) y cancelando al número a se tiene que $b \leq a$ contradiciendo la hipótesis sobre a y b. Si $a + b = s(c + c)$ entonces $a + b \leq s(a + a) = a + s(a)$ de donde se tiene que $b \leq s(a)$ lo que, de nuevo, contradice la hipótesis. Luego, por tricotomía, $a < c$. De manera análoga se muestra que $c < b$.

Para mostrar la densidad de $\ll$ falta mostrar que $[a] \cap [c] = \emptyset$ y $[b] \cap [c] = \emptyset$. Si $[a] \cap [c] \neq \emptyset$, como $a < c$, entonces $c = a + \overline{n}$ para algún n, entonces ocurre uno de dos casos.

- Si $a + b = c + c$. Entonces $a + b = (a + \overline{n}) + (a + \overline{n}) = a + (a + \overline{n + n})$, de donde $b = a + \overline{n + n}$ y entonces $b \in [a]$.
- Si $a + b = s(c + c)$. Entonces $a + b = s(a + \overline{n} + a + \overline{n}) = a + s(a + \overline{n + n})$, de donde $b = s(a + \overline{n + n}) = a + s(\overline{n + n})$ y entonces $b \in [a]$.

Así, no puede ocurrir que $c = a + \overline{n}$, entonces $[a] \cap [c] = \emptyset$. Luego, si $[b] \cap [c] \neq \emptyset$ entonces, como $c < b$, $b = c + \overline{m}$ para algún m. Entonces, si $c + c = a + b$ se tiene que $c + c = a + c + \overline{m}$ de donde $c = a + \overline{m}$, contradiciendo lo anterior mostrado. De igual manera se contradice este hecho para cuando $s(c + c) = a + b$. Por lo tanto, se ha demostrado que para cualquier par de elementos no-estándar a, b existe un tercero c tal que $[a] \ll [c] \ll [b]$.

Por último, se muestra que Ω no tiene puntos extremos en el orden $\ll$. Para ello, sea a un número no estándar, entonces $[a] \ll [2 \cdot a]$ pues $a < a + a = 2 \cdot a$ y $2 \cdot a \notin [a]$ pues se encuentra a una *distancia* no-estándar ($2 \cdot a = a + a$) de a. De igual manera, $\frac{a}{2}$ es un número no-estándar y $\frac{a}{2} < a$ (por definición de $\frac{x}{2}$), además, si $\left[\frac{a}{2}\right] \cap [a] \neq \emptyset$ se tiene que $a = \frac{a}{2} + \overline{n}$ para algún natural $n > 0$, de donde $a + a = \frac{a}{2} + \frac{a}{2} + \overline{n} + \overline{n}$ y se tienen dos opciones, $a = \overline{n} + \overline{n}$ o $a = \overline{n} + \overline{n} - \overline{1}$, en cualquier caso se contradice el hecho de que a es no-estándar. Así, $\left[\frac{a}{2}\right] \ll [a]$. □

De la definición del conjunto Ω se tiene que todo elemento x de un modelo aritmético $\mathfrak{M}$ cumple con una, y solo con una, de las siguientes condiciones: o $x \in FA(\mathfrak{M})$ o $x \in [a]$ para algún $a \in NE(\mathfrak{M})$. Otro aspecto interesante de este conjunto es que su cardinalidad es igual a la del conjunto de números no-estándar de cualquier modelo aritmético $\mathfrak{M}$, es decir, $|\Omega| = |NE(\mathfrak{M})|$, en efecto del lema 2.3.6 se tiene que $|NE(\mathfrak{M})| = |\bigcup \Omega| = |\mathbb{Z}| \cdot |\Omega| = \aleph_0 \cdot |\Omega| = |\Omega|$ pues Ω es infinito.

Del anterior teorema se tiene el siguiente bosquejo del orden en un modelo no-estándar, donde cada segmento vertical representa una clase $[a]$ para algún número no-estándar a y estos segmentos tienen un orden lineal, denso y sin puntos extremos.

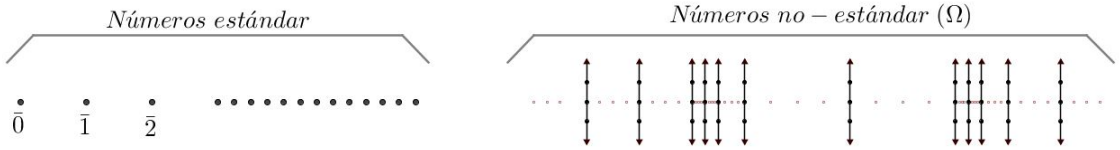


Figura 2.2: El conjunto Ω en un modelo aritmético no-estándar.

Luego, por el lema 2.3.7, si $[a] \ll [b]$ todo elemento de la clase $[a]$ es menor que cualquier elemento de la clase $[b]$ en el orden $<$, esto es, los elementos de una linea son menores que los elementos de cualquier otra linea que esté *a la derecha* en la figura anterior. Además, cada una de las líneas tiene el orden de los enteros, así, si se elige un único representante[9] a_0 de cada clase $[a]$ éste puede considerarse como el cero de los enteros, delante de él se tiene a su sucesor (inmediato) $a_0 + \overline{1}$ y detrás de él se encuentra su antecesor (inmediato) $a_0 - \overline{1}$ y así se siguen inmediatos sucesores para una dirección (la cual, por conveniencia en la figura, será hacia arriba) e inmediatos antecesores para la otra dirección sin tener un elemento mínimo ni un máximo.

En resumen, la interpretación del símbolo predicado $<$ en todo modelo aritmético no-estándar genera un orden lineal que tiene las siguientes características.

- La constante 0 es el primer elemento.
- Los elementos estándar son un segmento inicial del universo que tiene el orden de los naturales.
- Cada número no-estándar a pertenece a una sola clase que tiene el orden de los enteros.
- Estas clases forman entre sí un orden lineal, denso y sin puntos extremos.
- Para cualesquiera dos números no-estándar a y b diferentes ocurre una de las siguientes.
  - a y b están la misma linea, en donde $a < b$ si y solo si a está *por debajo* de b.
  - a y b están en diferentes líneas, en donde $a < b$ si y solo si la linea de a está *a la izquierda* de la linea de b.

Formalmente, esto se sintetiza en el siguiente teorema que es la recopilación del anterior y los lemas 2.3.2 y 2.3.6 y es también la culminación de esta subsección.

[9] Lo cual se puede hacer sin problemas por el axioma de elección (ver A.1.19).

Teorema 2.3.10. ORDEN ARITMÉTICO. *Sea $\mathfrak{M}$ un modelo aritmético. Entonces la interpretación del símbolo $<$ en $\mathfrak{M}$ genera un orden en $|\mathfrak{M}|$ isomorfo al orden de $\mathbb{N} \cup (\mathbb{Z} \times \Omega)$; donde Ω tiene un orden lineal, denso y sin puntos extremos y es tal que $|\Omega| = |NE(\mathfrak{M})|$, además $\mathbb{Z} \times \Omega$ está ordenado con el orden lexicográfico horizontal y $\mathbb{N} \cup (\mathbb{Z} \times \Omega)$ con el orden de yuxtaposición*[10].

Como corolario de este resultado, se conoce específicamente el orden de un modelo no-estándar numerable, puesto que, como mostró Cantor, el único (salvo isomorfismo) orden lineal, denso, sin extremos y numerable es el orden usual de $\mathbb{Q}$. (ver [2]).

Corolario 2.3.11. ORDEN ARITMÉTICO NUMERABLE. *Sea $\mathfrak{M}$ un modelo aritmético numerable. Entonces la interpretación del símbolo $<$ en $\mathfrak{M}$ genera un orden en $|\mathfrak{M}|$ isomorfo al orden de $\mathbb{N} \cup \mathbb{Z} \times \mathbb{Q}$.*

Para terminar, se presenta una figura que muestra con detalle lo expresado en el anterior corolario que concentra lo expuesto en esta sección; en ésta solo los puntos huecos de color rojo son elementos del universo, además se muestran los elementos no-estándar a, b tales que $[a] \ll [b]$, y los elementos no-estándar c_1, c, c_2 tales que $[c_1] \ll [c] \ll [c_2]$.

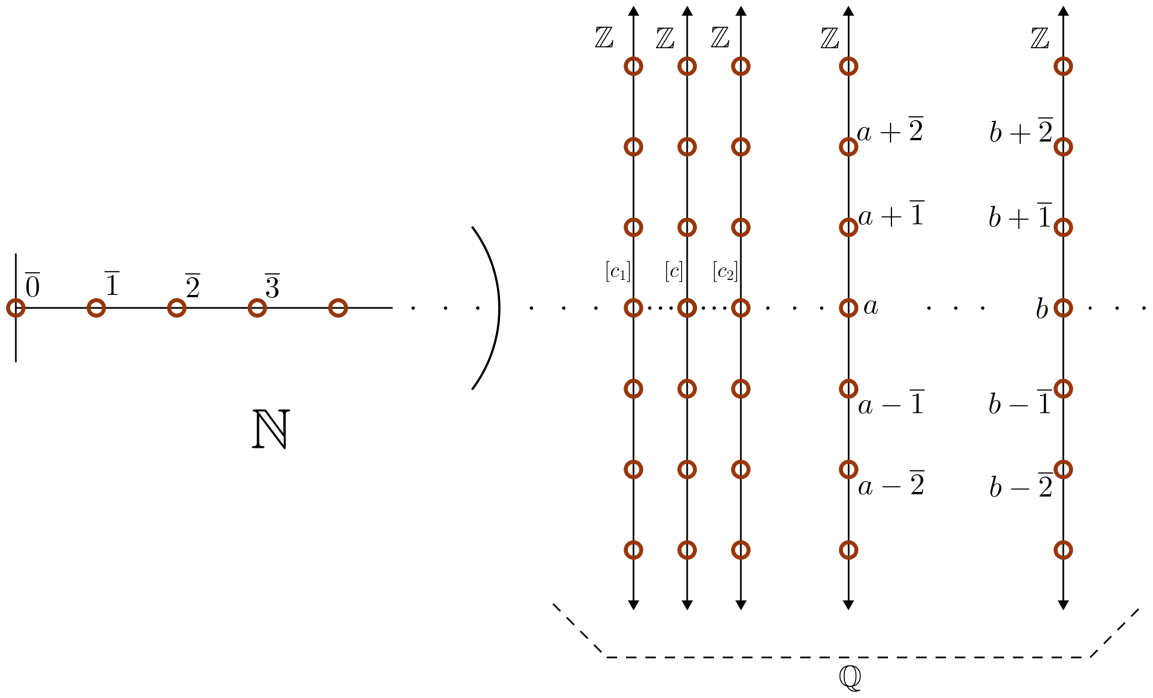


Figura 2.3: Orden aritmético numerable.

[10] Ver A.1.11 y A.1.12.

2.4. Inducción

La inducción que generalmente se utiliza en el ámbito de la matemática es la *inducción de segundo orden*, es decir, se entiende como la oración: «si $A \subseteq \mathbb{N}$ y se cumple que $0 \in$ A y que si $n \in$ A entonces $n+1 \in A$, entonces $A = \mathbb{N}$». Es muy común ver una demostración por inducción, por ejemplo dentro de la teoría de Números, y a veces esta manera de argumentar tiene una modificación particular conocida como *inducción fuerte*.

La *inducción fuerte* o *inducción completa*, en segundo orden, se traduce en la oración: «si $A \subseteq \mathbb{N}$ y se cumple que $0 \in$ A y que si $0, 1, \ldots, n \in$ A entonces $n+1 \in A$, entonces $A = \mathbb{N}$»; la diferencia entre esta inducción fuerte y la inducción usual (también llamada *inducción débil*) radica en que, al contrario de la última, en el antecedente de la inducción completa se tiene que mostrar que $n+1$ tiene cierta propiedad partiendo del hecho de que todos los naturales anteriores (no solo el inmediato anterior) la tienen. La razón de llevar en su nombre la palabra *fuerte* es que el antecedente de la inducción débil (denotado por p_1) es, lógicamente, más fuerte que el otro antecedente (denotado por p_2), es decir, lo implica (en efecto, si se cumple que $n \in A$ implica a $n+1 \in A$, entonces es claro que de suponer a $0, 1, \ldots, n \in A$ se demuestra que $n+1 \in A$); por lo tanto, la inducción fuerte implica a la inducción débil (si $p_1 \to p_2$, entonces $(p_2 \to q) \to (p_1 \to q)$).

No es difícil mostrar que estas dos formas de inducción son equivalentes ocupando el buen orden de los números naturales (teorema A.2.14). Ahora bien, como se mostró en la sección anterior, el universo de cualquier modelo no-estándar de la aritmética no está bien ordenado con el orden usual que hereda del estándar, por lo que, en principio, no se puede realizar un *mutatis mutandis* para demostrar esto en lógica de primer orden.

Esta pequeña sección tiene por objetivo presentar dos esquemas dentro del lenguaje de la aritmética y demostrar que son equivalentes al esquema de inducción. Estos esquemas son las versiones, dentro de la lógica de primer orden, del buen orden e inducción fuerte.

Definición 2.4.1. *Las siguientes oraciones dentro de* $\mathrm{L_A}$ *son llamadas, respectivamente, el* esquema de inducción fuerte en primer orden *(denotada por* SIE*) y el* principio del mínimo elemento *(denotada por* LEP*).*

$$\mathrm{SIE} \equiv (\varphi(0) \ \wedge \ \forall x((\forall y \leq x \varphi(y)) \to \varphi(x+1))) \to \forall x \varphi(x)$$
$$\mathrm{LEP} \equiv \exists x \varphi(x) \to \exists z(\varphi(z) \ \wedge \ \forall y(\varphi(y) \to z \leq y))$$

Las definiciones de estos dos esquemas son la traducción a primer orden de sus homónimas, la diferencia es que no involucran a todos los subconjuntos, es decir, el principio del mínimo elemento asegura la existencia de un elemento mínimo en todo subconjunto no vacío definible[11], pero no implica la existencia de este elemento en subconjuntos generales.

Con IE se denotará al esquema de inducción (es decir, IE $\equiv (\varphi(0) \ \wedge \ \forall x(\varphi(x) \to \varphi(x+1))) \to \forall x \varphi(x)$) y PA^- hace referencia a los axiomas de Peano excepto IE, es decir, las primeras seis oraciones de la definición 2.1.2.

Lo primero que se mostrará es que, como su nombre lo indica, SIE es (lógicamente) más fuerte que IE, es decir, que el esquema de inducción fuerte implica, directamente, al esquema de inducción débil.

[11] Ya se habían mencionado este tipo de conjuntos, son aquellos subconjuntos A tales que existe una oración φ en $\mathrm{L_A}$ tal que $x \in A$ si y solo si $\varphi(x)$, o lo que es igual, $A = \{x \mid \varphi(x)\}$.

Teorema 2.4.2. *Se cumple que* $\mathrm{PA}^- \vdash \mathrm{SIE} \to \mathrm{IE}$.

Demostración. Se supone el antecedente de IE, es decir, a $\varphi(0)$ *(-∗-)* y $\forall x(\varphi(x) \to \varphi(x+1))$ *(-∗∗-)*.

Sea $\psi(x) \equiv (\forall y \leq x\varphi(y)) \to \varphi(x+1)$. Por *(-∗∗-)* aplicado a 0 se tiene que $\psi(0)$ es verdadero[12]. Ahora, es claro que $(\forall y \leq x+1(\varphi(y))) \to \varphi(x+1)$, por otro lado, utilizando a *(-∗∗-)*, se tiene que $\varphi(x+1) \to \varphi(x+2)$; así, por transitividad, se tiene que $\psi(x+1) \equiv (\forall y \leq x+1(\varphi(y))) \to \varphi(x+2)$ siempre es verdadero, en particular se tiene que $(\forall y \leq x\psi(y)) \to \psi(x+1)$ (pues el consecuente es verdadero) por lo que, por SIE, se concluye a $\forall x\psi(x)$.

De lo anterior, y por *(-∗-)*, se tiene que $\varphi(0)$ y $\forall x((\forall y \leq x\varphi(y)) \to \varphi(x+1))$; ocupando una vez más a SIE se concluye a $\forall x\varphi(x)$. Todo esto demuestra que $\mathrm{PA}^-, \mathrm{SIE} \vdash \mathrm{IE}$; lo que se quiere se obtiene al aplicar el meta-teorema de deducción[13]. □

Ahora se mostrará que los dos nuevos esquemas son equivalentes en la teoría aritmética de primer orden.

Teorema 2.4.3. *Se cumple que* $\mathrm{PA} \vdash \mathrm{SIE} \leftrightarrow \mathrm{LEP}$.

Demostración. Ocupando nuevamente el meta-teorema de deducción y el lema 1.2.23, se mostrarán dos incisos: (a) $\mathrm{PA}, \mathrm{SIE} \vdash \mathrm{LEP}$ y (b) $\mathrm{PA}, \mathrm{LEP} \vdash \mathrm{SIE}$.

a. Por contradicción, se supone que $\exists x\varphi(x)$ *(-1-)* y que $\forall z(\neg\varphi(z) \vee \exists y(y < z \wedge \varphi(y)))$ *(-2-)*.

Si ocurriera $\varphi(0)$ entonces, por *(-2-)* se tiene que existe un elemento y tal que $y < 0$ y $\varphi(y)$, lo cual es una contradicción pues de PA se sigue que $\forall x(0 \leq x)$; así, se tiene entonces que $\neg\varphi(0)$. Suponiendo que $\neg\varphi(y)$ para todo $y \leq x$ se tiene que $\neg\varphi(x+1)$, en efecto, si por el contrario se cumpliera que $\varphi(x+1)$, entonces por *(-2-)* existiría un elemento $y < x+1$ tal que $\varphi(y)$, contradiciendo la suposición.

A final, se tiene que $\neg\varphi(0) \wedge \forall x((\forall y \leq x(\neg\varphi(y))) \to \neg\varphi(x+1))$; luego, por SIE, se concluye que $\forall x\neg\varphi(x)$, contradiciendo a *(-1-)*.

b. Por contradicción, se suponen ciertas las oraciones $\varphi(0)$ *(-3-)*, $\forall x((\forall y \leq x\varphi(y)) \to \varphi(x+1))$ *(-4-)* y $\exists x\neg\varphi(x)$ *(-5-)*.

De *(-5-)* y LEP se sigue que existe el mínimo elemento que no cumple con φ, es decir, existe un elemento z tal que $\neg\varphi(z+1)$ y $\forall y \leq z\varphi(y)$ (pues, por *(-3-)*, el elemento mínimo no puede ser cero, entonces es sucesor); de esta última oración, y por *(-4-)*, ocurre que $\varphi(z+1)$. □

Si en la demostración anterior todos los teoremas para cuya prueba se utilizo el esquema de inducción se pudieran demostrar utilizando las hipótesis en cada caso (SIE para la parte a y LEP para la parte b) entonces el resultado sería aún más fuerte, como lo muestra el siguiente corolario.

Corolario 2.4.4. *Se cumple que* $\mathrm{PA}^- \vdash \mathrm{SIE} \leftrightarrow \mathrm{LEP}$.

Demostración. Se sigue del teorema anterior y observaciones para cada uno de los incisos.

a. Se tiene del teorema 2.4.2; en efecto, de ese resultado se sigue que todo lo que se pueda demostrar con el esquema de inducción débil se puede demostrar suponiendo a SIE en su lugar.

[12] Puede parecer un poco tramposa esta afirmación, pues para mostrar que $\forall x(0 \leq x)$ se ocupó al esquema inductivo; empero, esto mismo se puede probar ocupando a SIE en su lugar y la demostración es prácticamente la misma.

[13] Ver lema 1.1.14.

b. El único resultado que depende de IE es la oración $\varphi \equiv \forall x(x = 0 \ \vee \ \exists t(x = s(t)))$; por lo que basta con mostrar que $\mathrm{PA}^- \cup \{\mathrm{LEP}\} \vdash \varphi$.

Sea $\psi(x) \equiv \nexists t(x = s(t))$, como $\psi(0)$ entonces, por LEP, existe el mínimo elemento z que cumple con ψ. Ahora, si existiera un y distinto de z tal que $\psi(y)$ se tendría que $z < y$, es decir, existiría t tal que $y = z + s(t) = s(z + t)$, lo cual es una contradicción; por lo tanto, cero es el único elemento que no es sucesor de algún elemento. □

El siguiente resultado muestra que, si bien SIE implica a LEP, IE es lo suficientemente fuerte para probar también al principio del mínimo elemento.

Teorema 2.4.5. *Sea $\varphi(x)$ una $\mathrm{L_A}$-fórmula, entonces se cumple que* $\mathrm{PA} \vdash \exists x\varphi(x) \rightarrow \exists z(\varphi(z) \ \wedge \ \forall y(\varphi(y) \rightarrow z \leq y))$

Demostración. Por contradicción. Se supone a $\exists x\varphi(x)$ *(-1-)* y a $\forall z(\varphi(z) \rightarrow \exists y < z(\varphi(y)))$ *(-2-)*. De *(-1-)* se sigue la existencia de un elemento a tal que $\varphi(a)$.

Sea $\theta(x) \equiv \forall w(w < x \rightarrow \neg\varphi(w))$. De *(-2-)*, por vacuidad, se concluye a $\theta(0)$. Se supone ahora a $\theta(x)$, si ocurriese $\neg\theta(x + 1)$ entonces existe un elemento w tal que $w < x + 1$ y $\varphi(w)$, como se supone a $\theta(x)$ este elemento w cumple además que $x \leq w$, por lo que entonces $w = x$; así se tiene que $\varphi(x)$ lo cual, por *(-2-)*, contradice a $\theta(x)$, por lo tanto $\theta(x) \rightarrow \theta(x + 1)$.

De lo anterior se tiene que $\theta(0) \ \wedge \ \forall x(\theta(x) \rightarrow \theta(x + 1))$; de IE se concluye a $\forall x(\theta(x))$, en particular $\theta(a + 1)$, de donde se tiene a $\neg\varphi(a)$ y, por ende, una contradicción. □

La anterior demostración es la versión adaptada de la primera parte de la prueba del teorema 2.4.3 para usar, en lugar de inducción fuerte, el esquema de inducción débil.

Después de lo hecho en la sección anterior, un resultado que se sigue de este teorema es que, si $\mathfrak{M}$ es un modelo no-estándar, ningún subconjunto $[a]$ del universo, con a un elemento no-estándar, es definible, pues cada uno de ellos no tiene un elemento mínimo.

Los siguientes corolarios son las conclusiones de esta sección.

Corolario 2.4.6. *Se cumple que* $\mathrm{PA}^- \vdash (\mathrm{IE} \rightarrow \mathrm{LEP}) \ \wedge \ (\mathrm{LEP} \rightarrow \mathrm{SIE}) \ \wedge \ (\mathrm{SIE} \rightarrow \mathrm{IE})$*; es decir, para toda $\mathrm{L_A}$-fórmula $\varphi(x)$, en la teoría de PA^-, los siguientes enunciados son equivalentes.*

$$\mathrm{IE} \equiv (\varphi(0) \ \wedge \ \forall x(\varphi(x) \rightarrow \varphi(x + 1))) \rightarrow \forall x\varphi(x)$$

$$\mathrm{LEP} \equiv \exists x\varphi(x) \rightarrow \exists z(\varphi(z) \ \wedge \ \forall y(\varphi(y) \rightarrow z \leq y))$$

$$\mathrm{SIE} \equiv (\varphi(0) \ \wedge \ \forall x((\forall y \leq x\varphi(y)) \rightarrow \varphi(x + 1))) \rightarrow \forall x\varphi(x)$$

Corolario 2.4.7. *Si $\mathfrak{M}$ es un modelo no-estándar de la aritmética, entonces su parte estándar no es definible; es decir, el subconjunto $FA(\mathfrak{M})$ no es definible.*

Demostración. Si, por el contrario, existiera una fórmula $\varphi(x)$ en $\mathrm{L_A}$ tal que $\varphi(x)$ si y solo si x es estándar, entonces existiría un elemento a tal que $\neg\varphi(a)$ (existe un elemento no-estándar); luego, por LEP, existiría el mínimo elemento que cumple esto, es decir, el primer número no-estándar lo cual, como se mostró en la sección anterior, no es posible. □

2.5. Recursión

En la sección 2.2 se mostró la existencia de los modelos no-estándar para la aritmética de primer orden, sin embargo, de la demostración del teorema 2.2.8 no se sigue nada sobre la cardinalidad del modelo, más aún, como también se mencionó al final de esa sección, el teorema de Skolem-Löwenheim solo implica la existencia de estructuras aritméticas no-estándar más que numerables (es decir, cuyo cardinal es mayor a $\aleph_0$), además no existen modelos finitos de PA. Sin embargo, en la sección anterior ya se han dado un resultado importante para los modelos numerables (modelos aritméticos con cardinal igual a $\aleph_0$). Así, responder a la pregunta: «¿existen modelos no-estándar de PA numerables?» es uno de los objetivos de esta sección, para ello se tendrá que abordar un poco en la rama de la matemática denominada *teoría de la computabilidad* o *teoría de la recursión*.

La noción de *computable* es puramente intuitiva y descansa en la idea de *algoritmo*, por un algoritmo se entiende un procedimiento basado en reglas que se puede ejecutar de manera automática con el único objetivo de llegar a una determinada meta, a fin de entender esto se puede poner el ejemplo informal de una receta de cocina, la cual es un conjunto de reglas que, en principio, cualquiera puede seguir para preparar cierto platillo. En la matemática hay muchos de estos algoritmos (está el algoritmo de Euclides o los algoritmos de división para polinomios, por ejemplo); ahora bien, la idea de computable enfatiza la parte *automática* de los algoritmos, en otras palabras, se dirá que algo (un algoritmo) es computable si puede realizarse de manera mecánica. Una vez más, estas nociones son puramente intuitivas.

Al intentar formalizar esto algunos matemáticos dieron diversas definiciones que, si bien en principio no son muy parecidas, resulta que muchas de ellas, las principales, son equivalentes entre si[14]. Destacan por ejemplo (las cuales son equivalentes) la definición de *máquina de Turing* dada por A. Turing en la primera mitad del siglo XX, el *cálculo* λ propuesto por A. Church en la misma época y, más recientemente, la *máquina de registro ilimitado* (URM[15] por sus siglas en inglés). Para tener una idea de estos conceptos formales se dará la definición de *función recursiva parcial*, la cual es equivalente a las tres anteriores, propuesta por Gödel y Kleene en el año 1936.

Todas las funciones que se consideran para las siguientes definiciones son *funciones numéricas*, esto se refiere a que son funciones cuyo dominio es una potencia cartesiana natural de $\mathbb{N}$ (o un subconjunto propio de esta potencia, en el caso de las llamadas *funciones parciales*) y cuyo contradominio es $\mathbb{N}$; es decir, se trabajará con las funciones f tales que $f : \mathbb{N}^n \to \mathbb{N}$ (más en general, tales que $f : X \to \mathbb{N}$ para $X \subseteq \mathbb{N}^n$) para algún $n \geq 1$ natural. La razón de esto es que todo conjunto numerable se puede *codificar* en el conjunto de los números naturales[16].

Definición 2.5.1. *Una función se llamará* base *si y solo si es una de las siguientes.*

- *La* función cero $z : \mathbb{N} \to \mathbb{N}$ *tal que* $x \mapsto z(x) = 0$.
- *La* función sucesor $s : \mathbb{N} \to \mathbb{N}$ *tal que* $x \mapsto s(x) = x + 1$.
- *Cualquier* función proyección $\pi^n_k : \mathbb{N}^n \to \mathbb{N}$ *tal que* $\mathbf{x} = (x_1, \ldots, x_n) \mapsto \pi^n_k(\mathbf{x}) = x_k$ *para* k, n *naturales tales que* $1 \leq k \leq n$.

El objetivo de estas funciones base es que son tan simples que pueden ser consideras por la intuición como *computables*. Lo siguiente es definir un par de operaciones aplicables a funciones computables para generar nuevas funciones computables.

[14] La referencia [5] es el principal texto sobre el cual se basa la primera parte de esta sección. En su capítulo 3 se pueden encontrar las definiciones correspondientes y las demostraciones de estas equivalencias.

[15] Una definición detallada y amigable de estas máquinas se puede encontrar en [5, cap. 1].

[16] Para una explicación más detallada de esto, ver la última parte de [5, cap. 1].

Definición 2.5.2. *Sea f una función de aridad n y $\{g_i\}_{i=1,2,\ldots,n}$ una familia de n funciones, cada una de aridad m. Se define la* función composición *de las funciones f y $g_i's$, denotada por $\Phi(f, g_1, \ldots, g_n)$, como la función $h : \mathbb{N}^m \to \mathbb{N}$ tal que $\mathbf{x} \mapsto h(\mathbf{x}) = f(g_1(\mathbf{x}), \ldots, g_n(\mathbf{x}))$*

Definición 2.5.3. *Sean g, h funciones de aridad n y $n+2$ respectivamente. La* función recursión *de g y h, denotada por $R(g, h)$, es la función $f : \mathbb{N}^{n+1} \to \mathbb{N}$ tal que para todo $\mathbf{x} \in \mathbb{N}^n$ y todo k natural se cumple:*

- $f(\mathbf{x}, 0) = g(\mathbf{x})$.
- $f(\mathbf{x}, k+1) = h(\mathbf{x}, k, f(\mathbf{x}, k))$.

La idea de estas dos maneras de crear funciones a partir de otras es la usual que se tiene para la composición y la recursión. Ahora, se definirá un primer conjunto importante de funciones, el cual estará constituido por todas aquellas funciones numéricas que sean básicas o el resultado de aplicar un numero finito de la operación composición y la operación recursión a éstas.

Definición 2.5.4. *El conjunto de las* funciones recursivas primitivas*, denotado por FRP, es el conjunto más pequeño que cumple las siguientes propiedades.*

I) *Toda función base está en FRP.*

II) *FRP es cerrado bajo las operaciones composición y recursión, esto es, si $f, g_1, \ldots, g_n, g, h$ están en FRP (y son de aridad adecuada) entonces también están $\Phi(f, g_1, \ldots, g_n)$ y $R(g, h)$.*

De manera análoga a la prueba de que PROP existe[17] se puede mostrar que tanto FRP como FR (el cual se definirá después) existen. Además, toda función recursiva primitiva es *total* (su dominio es algún $\mathbb{N}^n$); la manera de probar esto es partiendo de que toda función básica es total y las operaciones recursión y composición, por su definición, preservan esta propiedad.

La idea del conjunto FRP es que es que abarca a funciones *simples* (pues parten de las básicas y se forman por recursión o composición) y, por lo tanto, son computables. Sin embargo, este conjunto no es exhaustivo. Se pueden dar argumentos sobre la existencia de funciones computables (y totales) que no pertenecen a FRP. Un ejemplo sencillo, mas no explícito, parte del hecho de que[18] $|FRP| = \aleph_0$, por lo tanto se pueden *enumerar* (existe una biyección computable[19] a $\mathbb{N}$) las funciones recursivas primitivas, así se tiene que $FRP = \{\mathrm{f}_1, \mathrm{f}_2, \ldots\}$. Se define la función $f : \mathbb{N} \to \mathbb{N}$ tal que $f(n) = \mathrm{f}_n(n) + 1$; f es total y, como cada f_n es computable, f es además computable (intuitivamente lo es, basta calcular la n-ésima función recursiva primitiva, evaluarla en n y tomar el sucesor del resultado). Claramente $f \neq \mathrm{f}_n$ para cada índice n, pues difieren en al menos un valor.

Algunos ejemplos de funciones en FRP son los siguientes, las cuales son (y de acuerdo a la intuición deberían de ser) computables.

La *función suma* $\Sigma(x, y) = x + y$.

La *función producto* $\Pi(x, y) = x \cdot y$.

La *función distancia* $d(x, y) = |x - y|$.

La *función factorial* $fact(x) = x!$

[17] El argumento está en la primera subsección de los preliminares.

[18] Se sigue de su definición y el hecho de que las funciones base son numerables.

[19] Es decir, se puede indizar a las funciones de tal manera que dado un elemento de FRP se puede calcular su índice mediante un algoritmo y viceversa. Una manera de hacerlo es identificando a cada función con una cadena finita de símbolos.

Como ya se comentó antes el conjunto FRP no abarca a todas las funciones recursivas (la función de Ackermann ([5, pág. 46]) es un buen ejemplo explícito de una función computable que no es primitiva recursiva), por lo tanto se desea ampliar este conjunto a uno más grande; para ello se necesitará de una nueva operación llamada *minimización* la cual, dada una función f, será una función g tal que $g(x)$ será el mínimo valor t para el cual $f(x,t) = 0$.

Definición 2.5.5. *Sea f una función de aridad $n+1$, la* función minimizador $\mathrm{M}[f] : \mathbb{N}^n \to \mathbb{N}$ *es la función numérica tal que:*

$$\mathrm{M}[f](\mathbf{x}) = \begin{cases} \textit{el mínimo } t \textit{ tal que:} & f(\mathbf{x},k) \textit{ está definida para toda } k \leq t, \textit{ y además } f(\mathbf{x},t) = 0. \\ \textit{indefinido} & \textit{si no existe tal } t. \end{cases}$$

La definición anterior tiene un «pequeño detalle» para el caso $n = 0$, puesto que el dominio de la función minimizador es $\mathbb{N}^0$ y el único elemento $\mathbf{x}$ de este conjunto es $\emptyset$ (la función vacía), lo cual puede generar confusión en el término $f(\mathbf{x}, k)$; sin embargo no hay ningún problema pues este último es igual a $f(k)$ al ser f una función unaria. En otras palabras, el elemento $\mathbf{x}$ se considera como una $n-$ada de parámetros y en el caso $n = 0$ no hay tales parámetros.

La función minimizador puede ser parcial, esto es para evitar «ciertos problemas» con las funciones a las que se le aplica la minimización; por ejemplo en la función factorial, como $fact(0) = 1$ y esta función es creciente entonces no existe un natural t tal que $f(t) = 0$, por lo que la función $\mathrm{M}[fact]$ no debería de arrojar valor alguno, así el acuerdo es que quede indeterminada. De igual manera, existen funciones $f : \mathbb{N} \to \mathbb{N}$ tales que el mínimo valor t que las anula no es cero y no están definidas en al menos un $k < t$, en este caso $\mathrm{M}[f]$ no estará definida pues la idea de la minimización, para que ésta sea computable, es verificar paso a paso si la función f se anula en algún natural, es decir, comienza calculando $f(0)$ y una vez calculado $f(n)$, si este valor no es cero, continua con $f(n+1)$, por lo que si f no está definida en algún k y aún no ha encuentra un valor que la anule, $\mathrm{M}[f]$ se «trabará».

A pesar de estos detalles que la composición y la recursión no tenían, esta operación extiende la idea de función computable pues si f es computable $\mathrm{M}[f]$ también lo será. Un ejemplo de esto es la función raíz cuadrada, en efecto, dado un número natural x se puede calcular, en caso de existir, al único natural y tal que $x = y^2$ mediante la función computable (puesto que es recursiva primitiva) $f(x,y) = |x - y^2|$. Por lo tanto, el conjunto FRP se extenderá a uno más grande.

Definición 2.5.6. *El conjunto de todas las* funciones recursivas*, denotado por FR, el conjunto más pequeño que cumple las siguientes propiedades.*

I) *Si $f \in FRP$ entonces $f \in FR$ (Toda función recursiva primitiva es recursiva).*

II) *Si $f \in FR$ entonces $\mathrm{M}[f] \in FR$ (Toda función minimizador es recursiva).*

La pregunta ahora es ¿el conjunto FR contiene a todas las funciones recursivas? La respuesta a esto es conocida como la tesis de Church-Turing.

Tesis 2.5.7. Tesis de Church-Turing. *El conjunto de las funciones computables coincide con el de las funciones recursivas.*

Este resultado no es formal, ni puede ser formal, debido al hecho de que la noción *computable* es puramente intuitiva y, por ende, no puede haber una demostración de esto. Más que nada, este resultado expresa que es inconcebible pensar una función que se considere computable y no esté dentro de las funciones recursivas. Los demás intentos por definir computable solo refuerzan esta creencia, pues el conjunto FR es igual al conjunto de las funciones Turing-computables e igual al conjunto de las funciones URM-calculables (para lo cual sí hay una demostración matemática). Ahora bien, como $|FR| = \aleph_0$,

existen (y muchas) funciones no computables (puesto que el conjunto de todas las funciones numéricas tiene cardinalidad igual a $2^{\aleph_0}$). La característica de estas *funciones no-computables* o *no-recursivas* es que son «muy extrañas», en el sentido de no tener una manera mecánica o algoritmo alguno para conocer su valor en cualquiera de sus argumentos; puede pensar por ejemplo en una «función aleatoria».

La idea de función recursiva se utiliza para definir un *conjunto recursivo* y una *relación recursiva*.

Definición 2.5.8. *Sea $A \subseteq \mathbb{N}$. Se dirá que A es un* conjunto recursivo *si su función característica*[20] $\mathcal{X}_A$ *es recursiva.*

Algunos ejemplos de conjuntos recursivos son el mismo $\mathbb{N}$, el conjunto de los números pares, el conjunto de los números primos, cualquier conjunto finito. Además, se puede mostrar que si A, B son recursivos entonces también lo son $A \cup B$, $A \cap B$, $A \setminus B$ y A^c $(= \mathbb{N} \setminus A$, el complemento de $A)$.

Definición 2.5.9. *Sea R una relación de números naturales de aridad n, es decir, $R \subseteq \mathbb{N}^n$. Se dirá que R es una* relación recursiva *(o un* predicado decidible*) si $\mathcal{X}_R : \mathbb{N}^n \to \{0, 1\}$ es recursiva.*

La relación binaria identidad $Id = \{(x, x)\} \subseteq \mathbb{N}^2$ es, por ejemplo, recursiva (o de manera equivalente, la propiedad de identidad es decidible).

La manera de conectar estas definiciones con lo que en este capítulo corresponde, es decir, con los modelos aritméticos, es que el modelo estándar de la aritmética ($\mathfrak{N}$) puede ser llamado un *modelo recursivo*, puesto que las funciones que lo definen (el sucesor, la suma y el producto) son, como ya se ha visto, recursivas. Más adelante se retomará esta observación para llegar a responder la segunda pregunta fundamental de esta sección: «¿en que aspectos difieren los modelos no-estándar numerables del modelo estándar?»

Después de esta breve introducción teoría de la recursión se continuará con el teorema de Gödel-Rosser, que se enuncia y demuestra en esa rama[21], y que es el resultado fundamental para mostrar que existen modelos no-estándar numerables. Este teorema es la versión refinada del célebre primer teorema de incompletitud de Gödel.

Teorema 2.5.10. DE GÖDEL-ROSSER. *Sea T una teoría recursivamente axiomatizada en el lenguaje* $\mathrm{L_A}$ *que extiende a* PA^-*, es decir, que su conjunto de axiomas A contiene al conjunto* PA^-*. Entonces existe una oración τ tal que $T \nvdash \tau$ y $T \nvdash \neg\tau$.*

Lo de *teoría recursivamente axiomatizada* se puede formalizar dentro de la teoría de recursión (de nuevo, en [5] se puede encontrar todo un capítulo, el octavo, dedicado a estos conceptos y resultados), sin embargo, basta con pensar que es una teoría tal que, una vez que se codificó el conjunto de oraciones (pues en una teoría aritmética se pueden formular numerables oraciones) dentro de los números naturales, el conjunto que le corresponde a los axiomas es recursivo; además de que la codificación del sistema deductivo (en este caso la deducción natural, el cual lo cumple) sea de tal manera que la relación de derivación (en este caso $\vdash$) sea *decidible*.

Una interpretación del teorema anterior es que la teoría aritmética de primer orden (pues PA cumple las hipótesis de dicho teorema.) es incompleta, pues existe una oración que no puede, y su negación tampoco, ser demostrada a partir de PA. Esta oración τ expresa de manera formal a la meta-oración «no soy demostrable»; esto es, es una oración que hace auto-referencia sobre ser demostrable; así, intuitivamente, es verdadera pero no demostrable. En particular, este teorema quiere decir que existe una oración verdadera en el modelo estándar que no puede ser inferida por los axiomas de Peano.

[20] Dado $A \subseteq X$, la función característica de A respecto a X es la función $\mathcal{X}_A : X \to \{0, 1\}$ tal que $\mathcal{X}_A(x) = 1$ si $x \in A$ y $\mathcal{X}_A(x) = 0$ si $x \notin A$.

[21] En [5, cap. 8] se puede encontrar una demostración del mismo.

Teorema 2.5.11. *Existen $2^{\aleph_0}$ modelos aritméticos numerables no elementalmente equivalentes entre sí.*

Demostración. Primero hay que observar que a lo más pueden existir $2^{\aleph_0}$ modelos aritméticos numerables; en efecto, si una estructura $\mathfrak{M} = \langle A,\ \sigma, \oplus, \otimes,\ 0\rangle$ es modelo aritmético numerable entonces $|A| = \aleph_0$, con lo cual existe una biyección con el conjunto $\mathbb{N}$ y, por ende, se puede pensar que son los números naturales (en otras palabras, como ya se ha visto, la naturaleza del universo es irrelevante para el modelo); así, las diferencias entre los modelos están dadas por las diferentes formas de definir las funciones y elegir la constante 0.

Como el conjunto de funciones unarias es igual a $\mathbb{N}^{\mathbb{N}}$, entonces se tienen $2^{\aleph_0}$ funciones unarias (ver sección 3 del apéndice A). De la misma manera, existen $2^{\aleph_0}$ funciones binarias y $\aleph_0$ elecciones de la constante 0. Así, existen $2^{\aleph_0} \cdot 2^{\aleph_0} \cdot \aleph_0 = 2^{\aleph_0}$ posibles estructuras en el lenguaje $\mathrm{L_A}$. Claramente muchas de ellas no serán modelos aritméticos. Lo que se mostrará a continuación es que, a pesar de ello, siguen siendo bastantes.

Considere el conjunto de axiomas PA, por el teorema de Gödel-Rosser existe una oración τ_1 tal que $\mathrm{PA} \nvdash \tau_1$ y $\mathrm{PA} \nvdash \tau_0$, donde $\tau_0 \equiv \neg\tau_1$. Luego $\mathrm{PA} \cup \{\tau_0\}$ y $\mathrm{PA} \cup \{\tau_1\}$ son ambos conjuntos consistentes; así, por el lema de existencia de modelo en su versión fuerte del lema 1.3.7, los dos conjuntos tienen un modelo numerable. Sean entonces $\mathfrak{M}_0$ y $\mathfrak{M}_1$ tales que $\mathfrak{M}_0 \vDash \mathrm{PA} \cup \{\tau_0\}$ y $\mathfrak{M}_1 \vDash \mathrm{PA} \cup \{\tau_1\}$.

La idea intuitiva de la prueba es que, como los conjuntos $\mathrm{PA} \cup \{\tau_0\}$ y $\mathrm{PA} \cup \{\tau_1\}$ siguen cumpliendo las hipótesis del teorema de Gödel-Rosser, aplicando este procedimiento una cantidad infinita de veces se obtienen los $2^{\aleph_0}$ modelos. Se mostrará el segundo estrato de la prueba de forma explícita para después hacerlo de manera general.

Se tiene entonces que existe una oración τ_{01} tal que $\mathrm{PA} \cup \{\tau_0\} \nvdash \tau_{01}$ y $\mathrm{PA} \cup \{\tau_0\} \nvdash \tau_{00}$, donde $\tau_{00} \equiv \neg\tau_{01}$. Se tiene así que los conjuntos $\mathrm{PA} \cup \{\tau_0, \tau_{00}\}$ y $\mathrm{PA} \cup \{\tau_0, \tau_{01}\}$ son consistentes; entonces, por el lema 1.3.7, ambos tienen un modelo numerable. Sean $\mathfrak{M}_{00}$ y $\mathfrak{M}_{01}$ tales que $\mathfrak{M}_{00} \vDash \mathrm{PA} \cup \{\tau_0, \tau_{00}\}$ y $\mathfrak{M}_{01} \vDash \mathrm{PA} \cup \{\tau_0, \tau_{01}\}$. De la misma manera, existen oraciones τ_{11} y τ_{10}, con $\tau_{10} \equiv \neg\tau_{11}$ y modelos numerables $\mathfrak{M}_{10}$ y $\mathfrak{M}_{11}$ tales que $\mathfrak{M}_{10} \vDash \mathrm{PA} \cup \{\tau_1, \tau_{10}\}$ y $\mathfrak{M}_{11} \vDash \mathrm{PA} \cup \{\tau_1, \tau_{11}\}$.

Dado el conjunto $\mathrm{PA} \cup \{\tau_{k_1}, \tau_{k_1k_2}, \ldots, \tau_{k_1k_2\ldots k_n}\}$ (donde $k_i \in \{0,1\}$) existen oraciones $\tau_{k_1k_2\ldots k_n1}$ y $\tau_{k_1k_2\ldots k_n0}$, con $\tau_{k_1k_2\ldots k_n0} \equiv \neg\tau_{k_1k_2\ldots k_n1}$ tales que $\mathrm{PA} \cup \{\tau_{k_1}, \tau_{k_1k_2} \ldots, \tau_{k_1k_2\ldots k_n}\} \nvdash \tau_{k_1k_2\ldots k_n1}$ y $\mathrm{PA} \cup \{\tau_{k_1}, \tau_{k_1k_2} \ldots, \tau_{k_1k_2\ldots k_n}\} \nvdash \tau_{k_1k_2\ldots k_n0}$. Así los conjuntos $\mathrm{PA} \cup \{\tau_{k_1}, \tau_{k_1k_2} \ldots, \tau_{k_1k_2\ldots k_n}, \tau_{k_1k_2\ldots k_n0}\}$ y $\mathrm{PA} \cup \{\tau_{k_1}, \tau_{k_1k_2} \ldots, \tau_{k_1k_2\ldots k_n}, \tau_{k_1k_2\ldots k_n1}\}$ son consistentes; luego, por el lema 1.3.7, existen estructuras numerables $\mathfrak{M}_{k_1k_2\ldots k_n0}$ y $\mathfrak{M}_{k_1k_2\ldots k_n1}$ que modelan a estos conjuntos respectivamente.

Así, que para cada sucesión s finita de ceros y unos (es decir, cualquier $s \in \{0,1\}^{<\omega}$) de longitud n se tiene un modelo numerable $\mathfrak{M}_s$ para el conjunto de oraciones $\mathrm{PA} \cup \{\tau_{s|_1}, \tau_{s|_2}, \ldots, \tau_s\}$, donde $s|_i$ representa a la sucesión s truncada en la posición i.

Por último, sea z una sucesión infinita de ceros y unos (es decir, $z \in \{0,1\}^{\omega}$), se mostrará que existe una estructura numerable $\mathfrak{M}_z$ que es modelo del conjunto $\mathrm{PA}\restriction_z = \mathrm{PA} \cup \{\tau_{z|_1}, \tau_{z|_2}, \ldots, \tau_{z|_n}, \ldots\}$. Esto es inmediato del teorema de compacidad, el lema de existencia de modelo y lo obtenido en el párrafo anterior; pues si $\Delta \subseteq \mathrm{PA}\restriction_z$ es finito, existe un natural n (la máxima longitud en los índices de τ que aparecen en el conjunto Δ) tal que, si s es la sucesión finita de longitud n que resulta de truncar a z, $\mathfrak{M}_s \vDash \Delta$ (en el caso en que Δ no contenga ninguna oración τ el modelo estándar funciona para el mismo propósito). Luego, como $\mathrm{PA}\restriction_z$ tiene un modelo es consistente y por el lema 1.3.7 tiene un modelo numerable, el cual es denotado por $\mathfrak{M}_z$.

Si z y z' son elementos distintos de $\{0,1\}^\omega$ se tiene que, por construcción, los modelos correspondientes a estas sucesiones difieren en la validez de al menos una oración de PA (es decir, existe una oración en el lenguaje $\mathrm{L_A}$ tal que uno de ellos la valida y el otro la niega), así, cualesquiera dos de estos modelos no son elementalmente equivalentes. □

Es claro que $\mathfrak{N}$ modela a solo uno de estos conjuntos $\mathrm{PA}\lfloor_z$, por lo que los demás modelos no son elementalmente equivalentes a él y se tiene el primer resultado principal de la sección.

Corolario 2.5.12. *Existen* $2^{\aleph_0}$ *modelos no-estándar numerables de la aritmética.*

La respuesta a la segunda pregunta «¿en qué difieren estos modelos no-estándar del numerable?» está dada por el teorema presentado por Stanley Tennenbaum en el año 1959 y publicado en una sola hoja de la revista *Notices of the American Mathematical Society*, para enunciarlo se tiene que ampliar la idea de *recursivo* (*computable*) a los modelos numerables.

Definición 2.5.13. *Sea* $\mathfrak{M}$ *un modelo aritmético, se dirá que* $\mathfrak{M}$ *es* recursivo *si existen un par de funciones binarias recursivas* $\oplus : \mathbb{N}\times\mathbb{N}\to\mathbb{N}$, $\otimes : \mathbb{N}\times\mathbb{N}\to\mathbb{N}$, *una función unaria recursiva* $\sigma : \mathbb{N}\to\mathbb{N}$ *y un número natural* n_0 *tal que* $\mathfrak{M} \cong \langle \mathbb{N},\ \sigma, \oplus, \otimes,\ n_0\rangle$.

Esto es, una estructura aritmética $\mathfrak{M}$ es recursiva si existe una biyección $f : |\mathfrak{M}| \to \mathbb{N}$ tal que, identificando a $\mathbb{N}$ como el dominio y codominio mediante f, sus funciones sucesor, suma y producto son recursivas. Debe notarse que las funciones recursivas de la definición anterior no tienen que ser necesariamente las funciones usuales, además de que el modelo estándar es recursivo y que, por la definición, un modelo recursivo forzosamente es numerable.

El segundo resultado importante de esta sección es que, de hecho, $\mathfrak{N}$ es el único modelo numerable recursivo de la aritmética.

Teorema 2.5.14. DE TENNENBAUM. *Si* $\mathfrak{M}$ *es un modelo no-estándar numerable de* PA, *entonces* $\mathfrak{M}$ *no es recursivo.*

La prueba de este teorema requiere ahondar más en la teoría de recursión, particularmente en la técnica de codificación (que básicamente es encontrar una manera *computable* de asociar un número natural a cada oración de la aritmética, los llamados *números de Gödel*), por lo tanto, en lo que resta del capítulo, se presentará un bosquejo de la idea detrás de la prueba.

Un resultado previo y fundamental para el teorema de Tennenbaum es el lema de fuga o desbordamiento (*overspill lemma* en inglés) el cual afirma que, dentro de un modelo aritmético no-estándar, si todos los números estándar cumplen una cierta propiedad expresada por la fórmula φ entonces existe al menos un elemento no-estándar que también cumple dicha propiedad.

Lema 2.5.15. LEMA OVERSPILL. *Sea* $\mathfrak{M}$ *un modelo de* PA *no-estándar y* $\varphi(x) \in \mathrm{L_A}$ *una fórmula tal que* $\mathfrak{M} \vDash \varphi(\overline{n})$ *para todo n natural, entonces existe un elemento* $a \in |\mathfrak{M}|$ *no-estándar tal que* $\mathfrak{M} \vDash \varphi(\overline{a})$.

Demostración. Por contradicción. Si ningún número no-estándar cumpliera con $\varphi(x)$ entonces se tiene que $\varphi(0)$ y que $\varphi(x)$ implica a $\varphi(x+\overline{1})$, en efecto, 0 cumple por ser estándar, si x es estándar la implicación se tiene por la hipótesis del lema y si es no-estándar se tiene por hipótesis de la contradicción, así, por el esquema de inducción, se tiene a $\forall x(\varphi(x))$ y al ser $\mathfrak{M}$ no-estándar se tiene una contradicción. □

El lema de fuga implica directamente que no existe ninguna fórmula $\varphi(x)$ del lenguaje tal que *defina* a la parte estándar dentro de un modelo no-estándar, es decir, no existe $\varphi(x) \in \mathrm{L_A}$ tal que se cumpla «x es estándar si y solo si $\varphi(x)$». Gracias a esta observación se puede afinar el resultado.

Lema 2.5.16. *Sea $\mathfrak{M}$ un modelo no-estándar de* PA*. Si $\varphi(x)$ es una fórmula tal que $\mathfrak{M} \vDash \varphi(\overline{n})$ para infinitos números naturales n, entonces existe un elemento $a \in |\mathfrak{M}|$ no-estándar tal que $\mathfrak{M} \vDash \varphi(\overline{a})$.*

Demostración. Por contradicción. Si no existiera ningún número no-estándar que cumpla con $\varphi(x)$ entonces la oración $\psi(x) \equiv \exists y(x < y \ \wedge \ \varphi(y))$ define a los números naturales, lo cual contradice al lema de fuga. □

La versión paramétrica del lema de fuga dada por Robinson es la que se ocupa para la demostración del teorema de Tennenbaum, su demostración es la misma que para la primera versión.

Lema 2.5.17. Robinson's overspill *Sea $\mathfrak{M}$ un modelo no-estándar de* PA*, $c \in |\mathfrak{M}|$ y $\theta(x, y)$ una fórmula tal que $\mathfrak{M} \vDash \theta(\overline{n}, \overline{c})$ para todo n natural, entonces existe un elemento $a \in |\mathfrak{M}|$ no-estándar tal que $\mathfrak{M} \vDash \theta(\overline{a}, \overline{c})$.*

El otro resultado fundamental para la prueba es un teorema que afirma la existencia de cierto tipo de conjuntos en los números naturales, para enunciarlo antes hay que definir la noción de *semi-computable* o *recursivamente enumerable*.

Definición 2.5.18. *Sea $A \subseteq \mathbb{N}$, se dice que A es* recursivamente enumerable *(abreviado por* r.e.*) si la función parcial dada por*

$$f(x) = \begin{cases} 1 & si\ x \in A \\ indefinido & si\ x \notin A \end{cases}$$

es computable.

La idea de que un conjunto A sea r.e. es que existe un programa (computable) que responde «sí» para cuando la entrada x es elemento de A y no da respuesta alguna (es decir, puede entrar en un *loop* infinito o puede continuar indefinidamente sin detenerse) cuando no. Este tipo de conjuntos son de suma importancia dentro del estudio de la recursividad, en [5, cap. 7] se puede encontrar mucha información sobre ellos. La función f de la definición anterior a veces es llamada *función característica parcial*.

La razón de ser llamados *recursivamente enumerables* es porque la definición 2.5.18 es equivalente a que A sea vacío o que sea el rango de una función computable unaria y total, esto es, omitiendo el caso vacío, que el conjunto A se puede enumerar mediante una función h recursiva; así se tiene que $A = \{h(0), h(1), h(2), \ldots\}$.

Teorema 2.5.19. *Existen conjuntos r.e. $A, B \subseteq \mathbb{N}$ tales que son* recursivamente inseparables*; es decir, no existe ningún conjunto recursivo $C \subseteq \mathbb{N}$ tal que $A \subseteq C$ y $B \cap C = \emptyset$.*

Dado un modelo no-estándar de la aritmética, la prueba también involucra el llamado *sistema estándar de conjuntos codificados en* $\mathfrak{M}$, el $SSy(\mathfrak{M})$ por sus siglas en inglés.

Definición 2.5.20. *Sea $\mathfrak{M}$ un modelo no-estándar de* PA*. Se define el conjunto $SSy(\mathfrak{M}) \subseteq \mathcal{P}(\mathbb{N})$ de tal manera que $A \in SSy(\mathfrak{M})$ si y solo si $A = \{n \in \mathbb{N} \mid \mathfrak{M} \vDash \varphi(\overline{n}, \overline{a})\}$ para alguna fórmula $\varphi(x, y)$ y algún elemento $a \in |\mathfrak{M}|$.*

La prueba del teorema de Tennenbaum consiste en ocupar el teorema 2.5.19 y el lema overspill para mostrar que $SSy(\mathfrak{M})$ contiene a un conjunto C que es no recursivo. Luego, suponer que $\mathfrak{M}$ es recursivo llevaría a que este conjunto C es recursivo. De hecho, la prueba muestra que ambas operaciones (la suma y el producto) no son recursivas.

Para concluir, el teorema 2.5.14 muestra que no se puede exhibir *de manera explícita*[22] un modelo numerable no-estándar de la aritmética; por otro lado, si bien se conoce explícitamente el orden en un modelo aritmético numerable, en modelos de mayor cardinalidad no se sabe aún el orden específico que tienen (el teorema 2.3.10 dice que el orden debe ser de cierto tipo, más no determina cuál es). Es por este motivo que hasta este momento no se ha dado (y por el mismo motivo no se dará) un *ejemplo amigable* de un modelo no-estándar de PA.

Para conocer más sobre la historia, implicaciones y la prueba de todos los resultados aquí expuestos (principalmente del teorema de Tennenbaum) se recomienda consultar [13].

2.6. Teoría de números

En esta última sección se mostrarán algunas definiciones y resultados de la teoría de números que pertenecen a la aritmética de primer orden, es decir, que son teoremas bajo los axiomas de Peano. Es conveniente aclarar que, no porque esta rama de la matemática se fundamente en los números naturales y éstos son un modelo de PA entonces, mediante algunas modificaciones menores, todos los resultados se puedan *trasladar* sin ningún problema. Un ejemplo es el siguiente. En $\mathbb{N}$ se puede mostrar el *algoritmo de Euclides* el cual manifiesta que, si a y b son números naturales, entonces $a = bq_1 + r_1$ para algún q_1 y r_1 tal que $0 \leq r_1 < b$, si r_1 no es cero se repite el resultado para los números b y r_1, es decir, existen q_2 y r_2 tales que $b = r_1q_2 + r_2$ donde $0 \leq r_2 < r_1$ y así *sucesivamente* hasta que *en algún momento* alguno de estos r_{k+1} será cero, el anterior a éste es el *máximo común divisor* de los originales a y b. La frase crucial en el anterior argumento es *en algún momento*, pues se está haciendo uso de que toda sucesión decreciente de números naturales es eventualmente constante, lo cual, como ya se vio a lo largo de este capítulo, no ocurre con los números que conforman un modelo no-estándar de PA pues básicamente el buen orden en el universo no es una cualidad inherente en ellos.

Si bien el algoritmo de Euclides para encontrar el máximo común divisor falla dentro de PA, el lema que se ocupa en cada uno de sus pasos sí es una oración que puede ser demostrada, a este resultado se le conoce como el *lema de división*.

Lema 2.6.1. Lema de división. $\text{PA} \vDash \forall xy(y \neq 0 \to \exists qr(x = y \cdot q + r \ \wedge \ 0 \leq r < y))$.

Demostración. Este resultado se puede probar de manera rápida y elegante usando el esquema de inducción sobre la variable x. Sin embargo se dará una demostración que hace uso de LEP (definición 2.4.1) y propiedades del orden. Se denota con $\varphi(x, y)$ la fórmula $y \neq 0 \to \exists qr(x = y \cdot q + r \ \wedge \ 0 \leq r < y)$.

Por hipótesis $1 \leq y$, entonces $x \leq y \cdot x < y \cdot s(x)$, así, por LEP, se tiene la existencia del mínimo elemento z tal que $x < y \cdot z$, sea $q = z - 1$. Por la elección de q se sigue que $x \geq y \cdot q$; si ocurriera la igualdad entonces se cumple $\varphi(x, y)$ con $r = 0$, si por el contrario ocurriera que $x > y \cdot q$ entonces, por definición del orden, existe r tal que $x = y \cdot q + r$, si $r \geq y$ entonces $x \geq y \cdot q + y = y \cdot s(q) = y \cdot z > x$, una contradicción, con lo cual $r < y$. □

El lema anterior se puede mejorar, mostrando que, de hecho, los elementos q y r son únicos.

Lema 2.6.2. Lema de división única. $\text{PA} \vDash \forall xy(y \neq 0 \to \exists! qr(x = y \cdot q + r \ \wedge \ 0 \leq r < y))$.

Demostración. Solo falta mostrar la unicidad. Sean q_1, q_2, r_1, r_2 tales que $x = y \cdot q_1 + r_1$ y $x = y \cdot q_2 + r_2$. Si $q_1 = q_2$ entonces, por la ley de cancelación, $r_1 = r_2$. Si por el contrario $q_1 \neq q_2$ se puede suponer, sin pérdida de generalidad, que $q_1 > q_2$, entonces existe un elemento $k \geq 1$ tal que $q_1 = q_2 + k$, sustituyendo se tendría que $y \cdot (q_2 + k) + r_1 = y \cdot q_2 + r_2$, de donde $y \cdot k + r_1 = r_2$, pero $y \cdot k + r_1 \geq y$ y $r_2 < y$, lo cual lleva a una contradicción. □

[22] En el sentido de la recursividad.

A estos elementos únicos se les puede dar un nombre y una interpretación. Al elemento q del lema anterior se le llamará *cociente de x con y*, y a r el *residuo de x con y*; así, dados dos números x y y la «división» entre ellos deja un único cociente y un único residuo menor que el número y.

Para enunciar los siguientes resultados es conveniente abreviar algunas fórmulas.

Definición 2.6.3. *Se introduce la siguiente notación.*

$$x|y \equiv \exists z(y = x \cdot z)$$

$$x \not| y \equiv \neg(x|y)$$

$$irred(x) \equiv \forall z(z|x \ \rightarrow \ z = 1 \ \vee \ z = x)$$

$$prime(x) \equiv x > 1 \ \wedge \ \forall zw(x|z \cdot w \ \rightarrow \ x|z \ \vee \ x|w)$$

La fórmula $x|y$ se lee como *x divide a y*, *x es un divisor de y* o *y es un múltiplo de x* y se entiende como la propiedad de que el elemento x «divida por completo» a y, es decir, que el residuo del lema 2.6.2 sea cero; más aún, del mismo lema se sigue que $x|y$ si y solo si el residuo de x con y es cero. Su negación, *x no divide a y* (o cualquiera de las otras dos formas de leerse), hace referencia a que «la división no es exacta», es decir, a que el residuo no es cero.

Por su parte, se dirá que un elemento m es *irreducible* si $irred(m)$ se valida; lo que expresa es que los únicos divisores de m son el uno y el mismo m. Por último, la fórmula $prime(m)$ se lee como *el elemento m es primo* y, de ser verdadera, afirma que m es un número mayor[23] a 1 tal que si divide al producto de dos elementos entonces necesariamente divide a uno de los dos.

Una inquietud que puede nacer del último par de fórmulas puede estar representada por la pregunta, «¿acaso la definición de número primo no es la que, por el contrario, está de alguna manera expresada en la propiedad de irreducible?» Lo que ocurre es que estos dos conceptos, como se mostrará más adelante, son equivalentes[24]. Primero algunos resultados básicos.

Proposición 2.6.4. *Los siguientes son teoremas en* PA.

a) $\forall xy(x|y \leftrightarrow \exists z(z \leq y \wedge y = x \cdot z))$

b) $\forall x(1|x \ \wedge \ x|x \ \wedge \ x|0 \ \wedge \ (0|x \rightarrow x = 0))$

c) $\forall xy(y \neq 0 \wedge x|y \rightarrow x \leq y)$

d) $\forall xyz(x|y \wedge y|z \rightarrow x|z)$

e) $\forall xyz(x|y \rightarrow x|y \cdot z)$

f) $\forall xyz(x|y \wedge x|z \rightarrow x|y + z)$

g) $\forall xyz(x|y + z \wedge x|y \rightarrow x|z)$

h) $\forall xy(x \neq 1 \wedge y > 1 \wedge x|y \rightarrow x \not| y - 1 \wedge x \not| y + 1)$

[23] La razón de dejar al 1 sin el título de número primo está basada en la conveniencia; esto es, se excluye porque así una gran parte de los resultados que involucran a primos es *más sencilla* de escribir.

[24] La razón de definir las dos propiedades por separado es que en el álgebra, más específicamente en la teoría de anillos, estas definición no son siempre equivalentes.

Demostración. Se mostrará el último par de incisos, las demás oraciones son (también) resultados directos de la definición 2.6.3.

Si $x = 0$ entonces $x|y + z$ solo si $y + z = 0$ (inciso b)), por lo que la única opción es que $y = z = 0$ y el resultado se cumple. Sean entonces x, y, z tales que $x \neq 0$, $x|y + z$ y $x|y$, entonces existen k_1, k_2 que cumplen con $y + z = x \cdot k_1$ y $y = x \cdot k_2$, además, por el lema 2.6.2 existen k_3, r tales que $z = x \cdot k_3 + r$ con $0 \leq r < x$. Sustituyendo se tiene que $x \cdot k_2 + x \cdot k_3 + r = x \cdot k_1$, entonces $x \cdot (k_2 + k_3) + r = x \cdot k_1 + 0$; por la unicidad del mismo lema, se tiene que $r = 0$, es decir, $x|z$.

Si $x|y + 1$ entonces, como por hipótesis $x|y$, se tendría por lo anterior demostrado que $x|1$, lo cual no puede ser pues $x \neq 1$. Como $y > 1$, la misma contradicción resultaría de suponer a $x|y - 1$. □

Teorema 2.6.5. $\text{PA} \vDash \forall x(x > 1 \to (prime(x) \leftrightarrow irred(x)))$

Demostración. La primer parte es más directa. Sea x un primo y sea z un elemento tal que $z|x$, como $x > 1$ entonces $z \neq 0$. Por definición se tiene que $x = z \cdot q$ para algún q, si $z > 1$ entonces $x > q$, por lo tanto $x \nmid q$ (parte c) de la proposición 2.6.4), así $x|z$, entonces $x \leq z$ y $z \leq x$, por lo que $z = x$; si por el contrario $z \leq 1$ entonces $z = 1$. De donde x es irreducible.

Para la segunda implicación sea $x > 1$ irreducible. Se define la fórmula $\varphi_x(w)$ como $\varphi_x(w) = \top$ si $w = 0$ y $\varphi_x(w) \equiv \forall yz\,(y \cdot z \leq w \wedge x|y \cdot z \ \to \ x|y \vee x|z)$ si $w > 0$. La idea es ocupar inducción fuerte para mostrar que $\forall w \varphi_x(w)$, lo cual basta para probar que x es primo; en efecto, sean y, z tales que $x|y \cdot z$ entonces, si se cumple $\varphi_x(s(y \cdot z))$, se tiene que $x|y$ o $x|z$.

Se supone la veracidad de la oración $\forall t \leq w \varphi_x(t)$. Por contradicción, se supone la existencia de elementos y, z tales que $yz \leq s(w)$, $x|yz$, $x \nmid y$ y $x \nmid z$. Sin pérdida de generalidad se puede suponer que $y < x$; en efecto, por el lema de división se tiene que $y = x \cdot q_y + s$ con $s < x$, y se cumple que $x \nmid s$ (parte f) de la proposición dado que $x \nmid y$), que $x|sz$ ($yz = xqz + sz$ y la parte g) de la proposición), y que $sz < yz \leq s(w)$; por lo que si $y \geq x$ se renombra a s como y.

Por la parte b) de la proposición 2.6.4 se tiene que $y \neq 0$ y $z \neq 0$, además $y = 1$ implica que $x|z$ (similar para $z = 1$), por lo que $1 < y < x$ y $1 < z$. Del lema de División se tiene que $x = y \cdot q + r$ con $0 \leq r < y$, si ocurriese $r = 0$ entonces $y|x$ y como x es irreducible $y = 1$ o $y = x$, lo cual es una contradicción. Así $0 < r < y$. Como $xz = yzq + rz$ entonces $x|rz$ (parte g) de la proposición), y como $r < y < x$ entonces $x \nmid r$ (pues $r \neq 0$), además $rz < yz \leq s(w)$. Por lo que existen r, z tales que $rz \leq w$, $x|rz$, $x \nmid r$ y $x \nmid z$, y como $r \leq w$ (en caso contrario, $rz > w$) se contradice a $\varphi_x(r)$.

Como $\varphi_x(0) = \top$ y $\forall w((\forall t \leq w \varphi_x(t)) \to \varphi_x(s(w)))$ entonces $\forall w \varphi_x(w)$. □

A continuación se mostrará uno de los teoremas más importantes (teorema 2.6.7) en la teoría de números el cual ya se conocía desde tiempos de Euclides y cuya demostración, ya sea de manera directa o por contradicción, es una de las más *bellas y elegantes*[25] demostraciones de la matemática.

Lema 2.6.6. *De los axiomas de Peano se sigue que para todo número mayor que uno existe un primo que lo divide, es decir,* $\text{PA} \vDash \forall x(x > 1 \to \exists p(prime(p) \ \wedge \ p|x))$

Demostración. Si $x = 0$ o $x = 1$ el resultado se tiene trivialmente.

[25]Es una, de hecho la primera, prueba que aparecen en el texto *Proof from THE BOOK*. Escrito por Martin Aigner & Giinter M. Ziegler, nace como una aproximación a la idea que tenía P. Erdös sobre *El Libro*. Se recomienda leer sobre esta agradable anécdota de la matemática.

Si $x > 1$ entonces, como $x|x$, existe el mínimo p tal que $p > 1$ y $p|x$. Claim: p es primo. Si no fuese así entonces p no sería irreducible (teorema 2.6.5) y existiría un elemento q tal que $1 < q < p$ que además $q|p$; por transitividad de la división $q|x$, contradiciendo la elección de p. □

Teorema 2.6.7. *De los axiomas de Peano se sigue que existen primos arbitrariamente grandes, es decir,* $\text{PA} \vDash \forall x \exists p(x < p \ \wedge \ prime(p))$. *En particular, el conjunto de los números primos en todo modelo aritmético es infinito*[26].

La demostración se basará en la idea que Euclides ocupó hace más de dos mil años. Interpretando, a partir de un x se mostrará la existencia de un elemento que sea divisible por todos los primos (en sí todos los números) anteriores a él y luego, tomando su sucesor, se mostrará que de hecho hay un primo mayor que él. La diferencia con el argumento de Euclides es que en éste último se construye específicamente el número que se necesita para la prueba, pues es un producto finito de números primos, acá no se puede ocupar ese *paso*, empero, se mostrará por inducción que este número existe sin necesidad de exhibirlo.

Demostración. Se mostrará primero que la oración $\forall x \varphi(x) \equiv \forall x \exists y(y > 0 \ \wedge \ \forall z(1 \leq z \leq x \to z|y))$ es un teorema. Se tiene a $\varphi(0)$ por vacuidad. Luego, se supone que $\varphi(x)$ para algún x, entonces existe un y con la propiedad descrita en $\varphi(x)$, se considera a $y' = y \cdot s(x)$. Claim: $y' > 0 \ \wedge \ \forall z(1 \leq z \leq s(x) \to z|y')$. Es claro que $y' > 0$ por hipótesis de inducción y el primer axioma de Peano; sea z tal que $1 \leq z \leq s(x)$, entonces hay dos opciones, si $z < s(x)$ entonces $z \leq x$ y como $z|y$ se tiene que $z|y'$ (proposición 2.6.4 parte e)), si $z = s(x)$ entonces $z|y'$ (por la misma proposición), en ambos casos se tiene a $\varphi(s(x))$. Así, por inducción, se demuestra a $\forall x \varphi(x)$.

Por último, sea x cualquier elemento y sea y el elemento que existe por lo anterior demostrado. Se aplica el lema 2.6.6 al número $y + 1$, entonces existe un p primo que lo divide. Si $p \leq x$ entonces $p|y$ lo cual no puede ocurrir por la parte h) de la proposición 2.6.4, por lo tanto, $p > x$. □

Aplicado el algoritmo de Euclides a un par de números n, m, se encuentra el *máximo común divisor* de éstos, además de la manera de expresarlo como una combinación lineal de los mismos; mostrar que existe tal combinación lineal sí es un resultado de PA (como muestra el siguiente teorema). Los conceptos de *máximo común divisor* (denotado por gcd) y *mínimo común múltiplo* (lcm) conservarán el significado intuitivo que tienen dentro de la teoría de números, es decir, dados x, y, $\text{lcm}(x, y)$ denotará al mínimo elemento que sea múltiplo de ambos; por su parte, $\gcd(x, y)$ será el elemento máximo que sea divisor común.

Lema 2.6.8. $\text{PA} \vDash \forall xy(x \cdot y \neq 0 \to \exists! z(z > 0 \wedge x|z \wedge y|z \wedge \forall w(x|w \wedge y|w \to z \leq w)))$

Demostración. Como por hipótesis $x \cdot y \neq 0$ y además $x|x \cdot y$ y $y|x \cdot y$, la existencia y unicidad de z se sigue del principio del mínimo elemento. □

El elemento descrito por el anterior lema será denotado por $\text{lcm}(x, y)$. Por el lema de división se tiene que $x \cdot y = \text{lcm}(x, y) \cdot q + r$ para algunos q, r con $0 \leq r < \text{lcm}(x, y)$, si $r \neq 0$ entonces $x|r$ y $y|r$, además $0 < r < \text{lcm}(x, y)$, contradiciendo a la elección de $\text{lcm}(x, y)$. Por lo tanto existe un único q tal que $x \cdot y = q \cdot \text{lcm}(x, y)$, este elemento será denotado por $\gcd(x, y)$ y, como $x \cdot y \neq 0$, $\gcd(x, y) \geq 1$. En conclusión, para todos x, y distintos de cero se tiene que $x \cdot y = \gcd(x, y) \cdot \text{lcm}(x, y)$ con $1 \leq \gcd(x, y)$ y $\text{lcm}(x, y) \leq x \cdot y$.

Los elementos $\gcd(x, y)$ y $\text{lcm}(x, y)$ se han definido para cuando ambos son distintos de cero. Si ambos fueran cero no existiría *el elemento más grande* que fuera un divisor común, puesto que todo x divide a cero, sin embargo, la definición se puede ampliar para cuando uno, y solo uno, de los dos es cero. Si

[26] La *cantidad* de números primos depende de la cardinalidad el modelo, por ejemplo, si es un modelo de cardinalidad $2^{\aleph_0}$ entonces se tendrían «tantos primos como números reales». Lo que siempre ocurre es que existen al menos $\aleph_0$.

$x \neq 0$ se define $\gcd(x,0) = \gcd(0,x) = x$, lo cual conserva la idea del máximo común divisor, en este caso se tendría que $\text{lcm}(x,0) = \text{lcm}(0,x) = 0$. La definición se extiende solo para fines prácticos, pues en realidad estos casos no tienen mucha importancia.

Lema 2.6.9. *Los siguientes son teoremas dentro de la aritmética de Peano.*

a) $\forall xy(x \cdot y \neq 0 \ \rightarrow \ \gcd(x,y)|x \wedge \gcd(x,y)|y)$

b) $\forall xy(x \cdot y \neq 0 \ \rightarrow \ \forall w(w|x \wedge w|y \rightarrow w|\gcd(x,y)))$

c) $\forall xy(x \cdot y \neq 0 \ \rightarrow \ \forall w(w|x \wedge w|y \rightarrow w \leq \gcd(x,y)))$

d) $\forall xy(x \cdot y \neq 0 \ \rightarrow \ \forall w(x|w \wedge y|w \rightarrow \text{lcm}(x,y)|w))$

e) $\forall xy(x \cdot y \neq 0 \ \rightarrow \ \exists! x'y'(x = x' \cdot \gcd(x,y) \ \wedge \ y = y' \cdot \gcd(x,y) \ \wedge \ \gcd(x',y') = 1))$

f) $\forall xyqr(x \neq 0 \wedge y = x \cdot q + r \ \rightarrow \ (\gcd(x,y)|r \ \wedge \ \gcd(x,r) = \gcd(x,y)))$

Se mostrarán solo algunas partes del lema, pues para demostrarlo en su totalidad haría falta introducir nueva notación y resultados previos que, si bien son interesantes para la formación de una teoría más amplia, no son necesarios para el objetivo de esta sección[27].

Demostración. Parte a). Por definición $x \cdot y = \gcd(x,y) \cdot \text{lcm}(x,y)$, como $y|\text{lcm}(x,y)$ se tiene que $x = \gcd(x,y) \cdot q$ para algún q, de donde $\gcd(x,y)|x$, de manera similar se demuestra que $\gcd(x,y)|y$.

Parte d). Como $\text{lcm}(x,y) \neq 0$ se tiene que $w = \text{lcm}(x,y) \cdot q + r$ para algunos p, r tales que $0 \leq r < \text{lcm}(x,y)$; como $x|\text{lcm}(x,y)$ y $x|w$, se tiene que $x|r$, de manera análoga se tiene que $y|r$ por lo que, si $r \neq 0$, se tendría una contradicción con la definición de $\text{lcm}(x,y)$.

Parte e). Mostrar que $\gcd(x,y)|r$ se sigue de la proposición 2.6.4 parte g). Para lo demás, como $\gcd(x,y)$ divide tanto a x como y se tiene, por el lema de división, que existen únicos x', y' tales que $x = x' \cdot \gcd(x,y)$ y $y = y' \cdot \gcd(x,y)$, falta mostrar que $\gcd(x',y') = 1$. Como $x' = q_1 \cdot \gcd(x',y')$ se sigue que $x = (\gcd(x,y)\gcd(x',y')) \cdot q_1$ de donde $\gcd(x,y)\gcd(x',y')|x$, de manera análoga se tiene también que $\gcd(x,y)\gcd(x',y')|y$. Por la parte c) del lema, se tiene que $\gcd(x,y)\gcd(x',y') \leq \gcd(x,y)$ por lo que $\gcd(x',y') = 1$. □

Para la demostración el teorema de Bézout, además del lema anterior, se necesitará probar el siguiente *truco aritmético*. Sea $\upsilon = s(s(\zeta))$ y $\eta = s(\zeta)$, entonces $\eta^2 \equiv \eta \cdot \eta = s(\zeta \cdot \upsilon)$; en efecto, $\eta^2 = s(\zeta) \cdot s(\zeta) = \zeta \cdot s(\zeta) + s(\zeta) = s(\zeta \cdot s(\zeta) + \zeta) = s(s(s(\zeta)) \cdot \zeta) = s(\zeta \cdot \upsilon)$. Visto en una notación más amigable tomará sentido el haberlo llamado *truco*, lo que se expresa con este resultado, de acuerdo a la definición 2.3.4, es que si $\upsilon \geq 2$ entonces $(\upsilon - 1)^2 = (\upsilon - 2)\upsilon + 1$.

Teorema 2.6.10. Teorema de Bézout. $\text{PA} \vDash \forall xy(x \cdot y \neq 0 \rightarrow \exists uv(u \cdot x = v \cdot y + gcd(x,y)))$

Demostración. Sea $\varphi(x,y) \equiv xy \neq 0 \rightarrow \exists uv(ux = vy + gcd(x,y))$. Para $x = 0$ el resultado es trivial; para $x = 1$, por ejemplo, se tiene que $\gcd(x,y) = 1$, por lo que $u = 1$ y $v = 0$ validan a $\varphi(1,y)$.

Sea $x \geq 1$, se supone verdadera a cada oración $\varphi(z,y)$ con $z < x$. Por el lema de División se tiene que $y = xq + r$ con $0 \leq r < x$. Si $r = 0$ entonces $\gcd(x,y) = x$ (pues $x|y$), por lo que $u = 1$ y $v = 0$ validan a $\varphi(x,y)$. Si $r = \gcd(x,y)$ sea x' tal que $x = x' \cdot \gcd(x,y)$ con $x' \neq 0$ (pues $x \geq 1$), se tiene entonces que $(x'-1)y + \gcd(x,y) = (x'-1)q \cdot x + x'\gcd(x,y) = ((x'-1)q + 1) \cdot x$, por lo que $u = (x'-1)q + 1$ y $v = x' - 1$ validan a $\varphi(x,y)$. Se pude suponer entonces que $r \neq 0$ y $r \neq \gcd(x,y)$.

[27] Los conceptos y demostraciones que aquí se omiten se encuentran en [19].

Por la primera parte del inciso f) del lema 2.6.9 se tiene que $\gcd(x, y)$ divide a x, y y r por lo que $y' = x'q + r'$ con y', x' y r' los respectivos cocientes y $1 < r' < x$; se cumple además, por los incisos e) y f), que $\gcd(x', r') = 1$. Ocupando la hipótesis de inducción sobre r' se tiene que $u'r' = v'x' + 1$ para algunos u', v', y como $1 < r'$ entonces $u'r' \geq 2$. Ocupando el truco citado en el párrafo previo al enunciado del teorema, se tiene que $ax' = br' + 1$ con $a = v'x'v'$ y $b = (u'r' - 2)u'$.

Por último, multiplicando por $\gcd(x, y)$ en la igualdad $ax' = br' + 1$ se tiene que $ax = br + \gcd(x, y)$ y sumando bqx en está última se tiene que $(a + bq)x = by + \gcd(x, y)$; por lo que $u = a + bq$ y $v = b$ hacen válida a $\varphi(x, y)$. El principio de inducción fuerte finaliza la prueba. □

Este teorema, más allá de ser la traducción a primer orden de un resultado importante y conocido de la matemática, es una parte fundamental para la misma aritmética pues de este depende un resultado conocido como *lema de Gödel*, el cual permite *simular* cuantificaciones finitas de tamaño arbitrario. A lo que esto se refiere es que existe una función $\beta(x, y, z)$ (llamada *función beta de Gödel*[28].) definible en primer orden tal que para toda sucesión finita $x_0, x_1, \ldots, x_{n-1}$ de elementos en cualquier modelo aritmético $\mathfrak{M}$ se tiene que existe un par de elementos $a, b \in \mathfrak{M}$ tal que $\mathfrak{M} \vDash \beta(a, b, i) = x_i$ para todo $i < n$. La utilidad de este lema es que sirve para trasladar enunciados de la matemática a la aritmética de primer orden que, en principio, parecen *intraducibles*. Por ejemplo, el teorema fundamental de la aritmética se enuncia como «todo número, distinto de 1, es producto (único) de *algunos* primos», lo que en un lenguaje menos informal quiere decir, es que para todo número $n > 1$ existe un (único) subconjunto finito (con posibles repeticiones[29]) de $\mathbb{P}$ (el conjunto de los números primos) tal que el producto de éstos es igual a n; el problema con esto es que se está haciendo referencia a un subconjunto, lo cual no puede ser traducido de manera directa; ahora, como la cantidad de estos números primos es arbitraria, el problema (de enunciarlo solamente, probarlo será después) se vuelve algo complejo. Ocupando el lema de Gödel, este subconjunto queda completamente determinado por un par de elementos.

Así, gracias a la función β, el problema de traducir algún enunciado de la forma «existen finitos elementos tal que...» se reemplaza por traducir algo como «existe un par de elementos tal que...» lo cual es, claramente, una manera muy ingeniosa de solucionarlo.

[28]Esta función es, además, la clave para la prueba de los teoremas de incompletitud de Gödel. Para un entendimiento profundo sobre el tema se recomienda [12, cap. 5].

[29]Puede parecer que se está abusando de la noción de conjunto, pues éstos *no permiten* repeticiones; sin embargo, todo primo se puede repetir una infinidad de veces e indizar a sus copias para que sean «distintas», es decir, se puede pensar que $\mathbb{P} = \{2_0, 2_1, \ldots, 3_0, 3_1, \ldots, p_0, p_1, \ldots\}$.

Apéndice A

Teoría de conjuntos

En este primer apéndice se enuncian algunas definiciones y resultados en la teoría de conjuntos que se ocupan o mencionan a lo largo de este trabajo. Se divide en tres secciones. En la primera se presentan los axiomas de Zermelo-Fraenkel-Choice (ZFC) y resultados básicos de los conjuntos (basado en los primeros capítulos de [10]); en la segunda se da la definición de un número natural dentro de esta teoría y algunos resultados importantes que llevan a que $\mathbb{N}$ (el conjunto de los números naturales aquí definidos) sea el universo de un modelo aritmético; la última muestra un poco de la aritmética de cardinales.

A.1. Axiomas

Primeramente se enuncian los axiomas que conforman el conjunto ZFC, donde las nociones primitivas son *conjunto* (detonados con letras tales como como A, B, C o x, y, z) y la relación de pertenencia *ser un elemento de*, para la cual se ocupa el símbolo $\in$. Es útil notar que los axiomas siguientes no son axiomas de una cierta teoría en el sentido de la lógica de predicados (definición 1.3.3), puesto que no se presentan como oraciones dentro de un lenguaje de primer orden, sino como oraciones del meta-lenguaje a las cuales se está más acostumbrado en el estudio de la ciencia matemática; esto es, se pueden considerar como meta-axiomas. Algunas de las palabras y símbolos usados para enunciarlos no se han definido aún, empero, se pueden tratar como los conceptos habituales que se tienen de ellos.

Definición A.1.1. Axiomas de Zermelo-Fraenkel. *El siguiente conjunto de axiomas es conocido como el* sistema axiomático de Zermelo-Fraenkel *y se denota por* ZF.

Axioma I *(de existencia). Hay un conjunto que no tiene elementos.*
(Se muestra que este conjunto es único, se le llama conjunto vacío *y se denota por* $\emptyset$*.)*

Axioma II *(de extensión). Si todo elemento de A es elemento de B y todo elemento de B es elemento de A, entonces $A = B$.*

Axioma III *(esquema de Comprensión). Sea $\mathbf{P}$ una propiedad. Para cualquier conjunto A existe un conjunto B tal que $x \in B$ si y solo si $x \in A$ y además x satisface la propiedad $\mathbf{P}$.*
(Este axioma indica que dado un conjunto A existe su subconjunto $B = \{x \in A \mid \mathbf{P}(x)\}$).

Axioma IV *(del par). Para cualesquiera conjuntos A y B existe un conjunto C tal que $x \in C$ si y solo si $x = A$ o $x = B$.*
(Se muestra que este conjunto es único y se le denota por $\{A, B\}$).

Axioma V *(de unión). Para cualquier conjunto A existe un conjunto S tal que $x \in S$ si y solo si $x \in C$ para algún $C \in A$.*
(Se muestra que este conjunto es único y se le denota por $\bigcup A$).

AXIOMA VI *(del potencia). Para cualquier conjunto A existe un conjunto P tal que $C \in P$ si y solo si $C \subseteq A$.*
(Se muestra que este conjunto es único y se le denota por $\mathcal{P}(A)$).

AXIOMA VII *(de infinitud). Existe un conjunto inductivo.*

AXIOMA VIII *(de fundación). En cada conjunto no vacío A existe un elemento x tal que x y A son ajenos, es decir, no tienen elementos en común.*

AXIOMA IX *(esquema de reemplazo). Sea $\mathbf{P}(x, y)$ una propiedad tal que para todo x existe un único y para el cual $\mathbf{P}(x, y)$ se satisface. Entonces para cualquier conjunto A existe un conjunto B tal que para todo $x \in A$ existe $y \in B$ para los cuales se cumple $\mathbf{P}(x, y)$.*

Definición A.1.2. SUBCONJUNTO. *Sean A, B conjuntos. Se dice que B es un* subconjunto *de A (y se denota por $B \subseteq A$) si ocurre que todo elemento de B es elemento de A, esto es, si $x \in B$ implica $z \in A$.*

Definición A.1.3. PAR ORDENADO. *Sean a, b conjuntos, se define el* par ordenado de a y b *como el conjunto $(a, b) = \{\{a\}, \{a, b\}\}$.*

Definición A.1.4. PRODUCTO CARTESIANO. *Sean A y B conjuntos. El* producto cartesiano *de A y B, denotado por $A \times B$, es el conjunto formado por los pares ordenados (a, b) tales que $a \in A$ y $b \in B$, esto es, $A \times B = \{(a, b) \mid a \in A \text{ y } b \in B\}$. Se denota con A^2 al producto cartesiano de A consigo mismo (es decir, $A^2 = A \times A$) y, en general, $A^n = \underbrace{A \times \cdots \times A}_{n \text{ veces}}$.*

Definición A.1.5. RELACIÓN. *Un conjunto R es una* relación *(*binaria*) si todo elemento de R es un par ordenado. Si además, $R \subseteq A \times B$ se dirá que R es una* relación de A en B*; para el caso particular donde $A = B$ simplemente se dirá que R es una* relación en A.

Definición A.1.6. FUNCIÓN. *Una relación F tal que para todo a, b, c se cumple que si $(a, b), (a, c) \in F$ entonces $b = c$ es llamada* función.

La definición de función se traduce en que es una relación que asocia un único elemento x (denotado por $f(a)$) a cada elemento a. Para cuando f sea una función de A en B (es decir, $f \subseteq A \times B$) se ocupará la notación $f : A \to B$.

Definición A.1.7. FUNCIÓN BIYECTIVA. *Sea $f : A \to B$ una función, se dirá que f es* biyectiva *si cumple lo siguiente.*

I. *Es* inyectiva. *Esto es, para todo $a_1, a_2 \in A$ si $a_1 \neq a_2$ entonces $f(a_1) \neq f(a_2)$.*

II. *Es* suprayectiva. *Esto es, para todo $b \in B$ existe $a \in A$ tal que $f(a) = b$.*

Si este es el caso, se dirá que f es una biyección *de A en B.*

Definición A.1.8. ORDEN PARCIAL. *Si R es una relación en A tal que:*

I. *Es* reflexiva. *Es decir, $(a, a) \in R$ para todo $a \in A$.*

II. *Es* antisimétrica. *Es decir, para todo $a, b \in A$, si $(a, b), (b, a) \in R$ entonces $a = b$.*

III. *Es* transitiva. *Es decir, para todo a, b, c se tiene que si $(a, b), (b, c) \in R$ entonces $(a, c) \in R$.*

se dirá entonces que R es un orden *(*parcial*)*[1] *en A. Al par (A, R) se le llama* conjunto *(*parcialmente*)* ordenado.

[1]Para los ordenes se ocuparán los símbolos $\leq$, $\ll$ y $\preceq$. Y en lugar de escribir $(a, b) \in <$ se utilizará $a < b$ como simplificación.

Definición A.1.9. Orden estricto. *Si R es una relación transitiva y asimétrica (es decir, si $(a,b) \in R$ entonces $(b,a) \notin R$) entonces se dirá que es un* orden estricto.

Definición A.1.10. Orden lineal. *Un orden $\leq$ es* lineal *si para cualquier par de elementos $a, b \in A$ se cumple*[2] *$a \leq b$ o $b \leq a$. Si este es el caso, el par $(A, \leq)$ es llamado* conjunto linealmente ordenado.

Teorema A.1.11. Orden de yuxtaposición. *Sean $(A, \leq)$ y $(B, \preceq)$ dos conjuntos ordenados tales que $A \cap B = \emptyset$. Entonces la relación $\ll$ en $A \cup B$ definida como*

$$x \ll z \text{ si y solo si } \begin{cases} x, z \in A \text{ y } x \leq z, \text{ o} \\ x, z \in B \text{ y } x \preceq z, \text{ o} \\ x \in A \text{ y } z \in B \end{cases}$$

es un orden para $A \cup B$ llamado el orden de yuxtaposición.

Teorema A.1.12. Orden lexicográfico. *Sean $(A, \leq)$ y $(B, \preceq)$ conjuntos linealmente ordenados, entonces las siguientes relaciones son órdenes lineales para el conjunto $A \times B$.*

- *El* orden lexicográfico vertical *definido como $(a_1, b_1) \ll_v (a_2, b_2)$ si y solo si ($a_1 < a_2$) o ($a_1 = a_2$ y $b_1 \preceq b_2$).*
- *El* orden lexicográfico horizontal *definido como $(a_1, b_1) \ll_h (a_2, b_2)$ si y solo si ($b_1 \prec b_2$) o ($b_1 = b_2$ y $a_1 \leq a_2$).*

Definición A.1.13. Cadena. *Sea $(A, \leq)$ un conjunto ordenado y $B \subseteq A$. Se dice que B es una* cadena *de A si cualquier par de elementos en B son $\leq$-comparables.*

Definición A.1.14. *Sea $\leq$ un orden en A y $B \subseteq A$.*

a) $b \in B$ *es el* elemento mínimo *de B en el orden $\leq$ si para todo $x \in B$ se cumple $b \leq x$.*

b) $b \in B$ *es un* elemento minimal *de B en el orden $\leq$ si no existe $x \in B$ tal que $x \leq b$ y $x \neq b$.*

c) $b \in B$ *es el* elemento máximo *de B en el orden $\leq$ si para todo $x \in B$ se cumple $x \leq b$.*

d) $b \in B$ *es un* elemento maximal *de B en el orden $\leq$ si no existe $x \in B$ tal que $b \leq x$ y $x \neq b$.*

Definición A.1.15. *Sea $\leq$ un orden en A y $B \subseteq A$.*

a) $a \in A$ *es una* cota inferior *de B en el orden $\leq$ si para todo $x \in B$ se cumple $a \leq x$.*

b) $a \in B$ *es el* ínfimo *de B en el orden $\leq$ si a es elemento máximo del conjunto de todas las cotas inferiores de B en $\leq$.*

c) $a \in A$ *es una* cota superior *de B en el orden $\leq$ si para todo $x \in B$ se cumple $x \leq a$.*

d) $a \in B$ *es el* supremo *de B en el orden $\leq$ si a es elemento mínimo del conjunto de todas las cotas superiores de B en $\leq$.*

Definición A.1.16. Isomorfismo de orden. *Sean $(A, \leq)$ y $(B, \prec)$ conjuntos ordenados. Un* isomorfismo de orden *es una función biyectiva $f : A \to B$ tal que para todo $a_1, a_2 \in A$ se tiene que $a_1 \leq a_2$ si y solo si $f(a_1) \prec f(a_2)$. Si este es el caso, se dirá que los conjuntos $(A, \leq)$ y $(B, \prec)$ son* isomorfos *(*en orden*) y f es un* isomorfismo *(*de orden*) entre $(A, \leq)$ y $(B, \prec)$.*

[2] Si se cumple esta propiedad se dice que a y b son $\leq$-comparables.

Teorema A.1.17. *Sean Sean $(A, \leq)$ y $(B, \preceq)$ conjuntos linealmente ordenados y $f : A \to B$ una biyección para la cual se cumple que $f(a_1) \preceq f(a_2)$ siempre que $a_1 \leq a_2$. Entonces f es un isomorfismo entre $(A, \leq)$ y $(B, \preceq)$.*

Definición A.1.18. Función de elección. *Sea A un conjunto. Una* función de elección para A *es una función $f : \mathcal{P}(A) \setminus \{\emptyset\} \to A$ tal que para todo $B \in \mathcal{P}(A) \setminus \{\emptyset\}$ se tiene que $f(B) \in B$.*

Definición A.1.19. Axioma X *(de elección). Todo conjunto no vacío tiene una función de elección.*

Al conjunto de axiomas de la definición A.1.1 más el anterior se le conoce como ZFC (el C es por *choice*, elección en inglés). El siguiente lema es equivalente al Axioma de Elección y ambos son utilizados en varias ramas de la matemática para mostrar importantes resultados, el lema en cuestión es esencial para la existencia de teorías maximalmente consistentes las cuales, a su vez, sirven para la demostración del lema de existencia de modelo (lema 1.3.5).

Lema A.1.20. Lema de Kuratowski-Zorn. *Cualquier conjunto no vacío parcialmente ordenado en el cual toda cadena tiene una cota superior tiene un elemento maximal.*

A.2. Números naturales

Se continua mostrando definiciones y proposiciones de la teoría de conjuntos enfocados a la definición formal, dentro de esta teoría matemática, de los *intuitivos* números naturales. Todas las demostraciones de los resultados están en [10, cáp. 5].

Definición A.2.1. *Sea A un conjunto. La* relación de pertenencia restringida *al conjunto A está definida por* $\in_A = \{(a,b) \in A \times A \mid a \in b\}$

Definición A.2.2. Conjunto transitivo. *Un conjunto x es* transitivo *si ocurre que para todo $y \in x$ se tiene que $y \subseteq x$.*

Definición A.2.3. Número natural. *Un conjunto x es un* número natural *si cumple*

I. *x es transitivo.*

II. *$\in_x$ es un orden estricto en x.*

III. *Todo $z \subseteq x$ no vacío tiene un elemento mínimo y un elemento máximo en el orden $\in_x$.*

Definición A.2.4. Sucesor. *Sea x un conjunto, el* sucesor *de x es el conjunto $s(x) = x \cup \{x\}$.*

Dada la definición A.2.3, el conjunto vacío es un número natural al cual se le denota con el símbolo 0. Más aún, se demuestra que el sucesor de un número natural es también un número natural, por lo que los siguientes son números naturales.

$$0 = \emptyset.$$

$$1 = s(0) = \{0\} = \{\emptyset\}.$$

$$2 = s(1) = \{0,1\} = \{\emptyset, \{\emptyset\}\}.$$

$$3 = s(2) = \{0,1,2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}.$$

$$\vdots$$

$$n = s(n-1) = \{0,1,\ldots,n-1\}.$$

Definición A.2.5. *Sea A un conjunto, se dirá que A es* inductivo *si ocurre que*

I. $0 \in A$

II. *Si $x \in A$ entonces $s(x) \in A$*

El axioma VII postula que existe al menos un conjunto inductivo, de este axioma se obtiene el siguiente resultado.

Teorema A.2.6. *El conjunto de todos los números naturales, denotado por $\mathbb{N}$, existe.*

Teorema A.2.7. Principio de inducción. *Sea $\mathbf{P}(x)$ una propiedad, entonces todo número natural tiene la propiedad expresada en $\mathbf{P}$ si ocurre lo siguiente.*

I. *$\mathbf{P}(0)$ y*

II. *para todo $n \in \mathbb{N}$, $\mathbf{P}(n)$ implica $\mathbf{P}(s(n))$*

Teorema A.2.8. DE RECURSIÓN. *Sea A un conjunto no vacío, $a \in A$ y $g : A \times \mathbb{N} \to A$ una función. Entonces existe una única función $f : \mathbb{N} \to A$ tal que:*

I. $f(0) = a$.

II. $f(s(n)) = g(f(n), n)$ *para todo* $n \in \mathbb{N}$.

Definición A.2.9. *Una* operación binaria *en un conjunto A es una función $* : A \times A \to A$. Al elemento $*(x, y)$ se le denotará con $x * y$.*

Teorema A.2.10. SUMA EN $\mathbb{N}$. *Existe una única operación binaria $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que:*

I. $m + 0 = m$ *para todo* $m \in \mathbb{N}$.

II. $n + s(m) = s(n + m)$ *para todo* $n, m \in \mathbb{N}$.

Teorema A.2.11. PRODUCTO EN $\mathbb{N}$. *Existe una única operación binaria $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que:*

I. $n \cdot 0 = 0$ *para todo* $n \in N$.

II. $n \cdot s(m) = n \cdot m + n$ *para todo* $n, m \in \mathbb{N}$.

Definición A.2.12. *Para cualquier par de números naturales n, m se define la relación binaria $\leq$ de tal manera que $n \leq m$ si y solo si $n \in m$ o $n = m$.*

Definición A.2.13. *Un conjunto parcialmente ordenado $(W, \leq)$ se llamará* bien ordenado *si cada subconjunto no vacío B de W tiene un elemento mínimo en $\leq$. Si este es el caso, el orden $\leq$ será un* buen orden.

Teorema A.2.14. ORDEN EN $\mathbb{N}$. *El conjunto $(\mathbb{N}, \leq)$ es bien ordenado.*

Teorema A.2.15. *La estructura $\mathfrak{N} = \langle \mathbb{N},\ +, \cdot, s,\ 0 \rangle$ es aritmética.*

A.3. Cardinales

En la matemática se está naturalmente acostumbrado a hablar de la cardinalidad de un conjunto, teniendo en mente que ésta debe asociarle un cierto *número* que represente la *cantidad de elementos* de dicho conjunto. Si el conjunto es *finito* entonces su cardinal es un número natural, sin embargo, si el conjunto no es finito (es decir, es *infinito*) entonces no es muy claro qué es lo que significa su cardinalidad. Una parte de la teoría de conjuntos estudia esto, definiendo primero que es un *número ordinal* (que es un concepto más débil al de número natural de la definición A.2.3, pues en la tercera condición se omite la existencia del máximo) para luego trabajar con ciertos números ordinales muy particulares que son los llamados *números cardinales*[3].

Esta última sección del primer apéndice no tiene por objeto definir los números cardinales (los cuales serán denotados por letras griegas tales como κ, λ o μ), sino que partirá del hecho de conocerlos y se enunciarán algunas definiciones y resultados sobre su aritmética que han sido utilizados a lo largo de este trabajo. Es importante mencionar que del axioma de elección se sigue que todo conjunto tiene asociado un único número cardinal y que además existe un orden lineal $<$ en la clase de los cardinales. Si X es un conjunto, se denotará con $|X|$ a su (único) número cardinal.

Lema A.3.1. *Sean A, B, C conjuntos. Si $A \subseteq B \subseteq C$ y $|A| = |C| = \kappa$, entonces $|B| = \kappa$.*

Teorema A.3.2. Cantor-Schröder-Bernstein. *Si A, B son conjuntos tales que $|A| \leq |B|$ y $|B| \leq |A|$ entonces $|A| = |B|$.*

Definición A.3.3. *Si $|A| = \kappa$, $|B| = \lambda$ y $A \cap B = \emptyset$, entonces se define la* suma *de κ y λ como $\kappa + \lambda = |A \cup B|$.*

Teorema A.3.4. *Si $\kappa \leq \lambda$ entonces $\kappa + \lambda = \lambda$.*

Definición A.3.5. *Si $|A| = \kappa$ y $|B| = \lambda$, entonces se define el* producto *de κ y λ como $\kappa \cdot \lambda = |A \times B|$.*

Teorema A.3.6. Tarski. *El axioma de elección es equivalente a que cualesquiera dos números cardinales κ y λ cumplan $\kappa + \lambda = k \cdot \lambda$.*

Definición A.3.7. *Si A y B son conjuntos, se define el conjunto A^B como el conjunto de todas las funciones de B en A, es decir, $A^B = \{f \mid f \text{ es función y } f : B \to A\}$.*

Definición A.3.8. *Si $|A| = \kappa$ y $|B| = \lambda$, entonces se define la* exponenciación *de κ y λ como $\kappa^\lambda = \left|A^B\right|$.*

Teorema A.3.9. *Si $\alpha \leq \beta$, entonces $\aleph_\alpha^{\aleph_\beta} = 2^{\aleph_\beta}$*

Teorema A.3.10. *Si $|A| = \kappa$, entonces $|\mathcal{P}(A)| = 2^\kappa$.*

Teorema A.3.11. Cantor. *Para todo cardinal κ, $\kappa < 2^\kappa$.*

[3] En [10, cap. 9] se hace un estudio detallado de estos conjuntos.

Apéndice B

Teoremas de Skolem

La finalidad de este apéndice es mostrar los teoremas y definiciones que permiten *definir* nuevas constantes, relaciones y funciones dentro de una estructura. Para ello, partiendo de una teoría T se encontrará una extensión de ésta que posea, por ejemplo, un nuevo símbolo funcional que *sirva como abreviación* para una fórmula dentro del lenguaje de la teoría T. En la práctica de la ciencia matemática esto se hace a menudo; por ejemplo, después de mostrar la existencia y unicidad de cierto elemento se le denota con un símbolo nuevo y se ocupa en el subsecuente desarrollo de la teoría.

Este apéndice está basado en [18, cap. 4.4].

Definición B.0.12. *Sea φ una fórmula dentro de un lenguaje L tal que $FV(\varphi) = \{x_1, \ldots, x_n, y\}$. Asociado a φ sea f_φ (llamado el* símbolo funcional de Skolem para φ*) un símbolo funcional de aridad n. La oración*

$$\forall x_1 \ldots x_n(\exists y \varphi(x_1, \ldots, x_n, y) \to \varphi(x_1, \ldots, x_n, f_\varphi(x_1, \ldots, x_n)))$$

es llamada el axioma de Skolem para φ.

En la definición de estructura (definición 1.2.1) se tiene de manera implícita que solo puede tener finitas funciones y finitas relaciones. Sin embargo, se extenderá la definición de estructura permitiendo tener un número infinito de éstas.

Definición B.0.13. *Sea T una teoría dentro del lenguaje L. Se define la* extensión de Skolem de T *como la teoría $T^{sk} = T \cup \{\sigma \mid \sigma$ es un axioma de Skolem para alguna fórmula del lenguaje $L\}$. Sea L^{sk} el lenguaje de T^{sk}, entonces este lenguaje extiende a L al incluir todos los símbolos funcionales de Skolem para L. Además, sea $\mathfrak{A}$ una estructura del tipo de L, entonces una* expansión de Skolem de $\mathfrak{A}$ *es una estructura $\mathfrak{A}^{sk}$ que es del tipo de L^{sk} tal que $\mathfrak{A}^{sk} \vDash \sigma$ para todo σ axioma de Skolem de L y que además $|\mathfrak{A}| = |\mathfrak{A}^{sk}|$.*

La interpretación de un símbolo funcional de Skolem en la estructura $\mathfrak{A}^{sk}$ es llamada *función de Skolem*.

Teorema B.0.14. *Sea T una teoría dentro del lenguaje L. Entonces T^{sk} es conservativa sobre T y además todo modelo $\mathfrak{A}$ de T tiene una expansión de Skolem $\mathfrak{A}^{sk}$ que a su vez es modelo de T^{sk}.*

Teorema B.0.15. *Sea T una teoría, φ una fórmula con $FV(\varphi) = \{x_1, \ldots, x_n, y\}$ y f un símbolo funcional de aridad n que pertenece al lenguaje de T tales que $T \vdash \forall x_1 \ldots x_n \exists! y \varphi(x_1, \ldots, x_n, y)$. Entonces $T^+ = T \cup \{\forall x_1 \ldots x_n y(\varphi(x_1, \ldots, x_n, y) \leftrightarrow y = f(x_1, \ldots, x_n))\}$ es conservativa sobre T*

Corolario B.0.16. *Sea t un término del lenguaje L tal que $FV(t) = \{x_1, \ldots, x_n\}$ y f un símbolo que no pertenece al lenguaje. Entonces $T^+ = T \cup \{\forall x_1 \ldots x_n(f(x_1, \ldots, x_n) = t)\}$ es conservativa sobre T.*

A la oración $f(x_1, \ldots, x_n) = t$ se le llamará la *definición explícita* de f.

Teorema B.0.17. *Sea φ una fórmula dentro del lenguaje L tal que $FV(\varphi) = \{x_1, \ldots, x_n\}$ y sea Q un símbolo predicado que no pertenece a L. Entonces $T^+ = T \cup \{\forall x_1 \ldots x_n(\varphi \leftrightarrow Q(x_1, \ldots, x_n))\}$ es conservativa sobre T.*

Resumiendo, a las extensiones del anterior corolario y los dos últimos teoremas se les llamará *extensiones por definición* donde las oraciones

$$\forall x_1 \ldots x_n y(\varphi \leftrightarrow y = f(x_1, \ldots, x_n))$$

$$\forall x_1 \ldots x_n y(f(x_1, \ldots, x_n) = t)$$

$$\forall x_1 \ldots x_n(\varphi \leftrightarrow Q(x_1, \ldots, x_n))$$

son llamadas los *axiomas de definición* para f y Q respectivamente.

Apéndice C

Una semántica topológica

En este apéndice se mostrará un ejemplo que relaciona la lógica de orden cero con la topología, más específicamente, se definirá una función de PROP (y en general de $\mathcal{P}(\text{PROP})$) a un espacio topológico con lo cual se podrá interpretar algunas propiedades mencionadas a lo largo de esta sección en el contexto de conjuntos. Se ocupan algunas definiciones y resultados básicos de topología, los cuales se pueden consultar en [4, cap. 1] y [8, cap. 1].

Sea $\mathcal{C}$ el conjunto de todas las sucesiones formadas por ceros y unos, esto es[1], $\mathcal{C} = 2^{\omega}$. Si $v \in \mathcal{C}$ entonces tiene la forma $v = (x_0, x_1, x_2, \ldots)$ donde $x_i \in \{0, 1\}$. Se denota con $(v)_k$ al $k-$ésimo elemento de la sucesión v.

Sean n, m naturales que indizan a $i_1, \ldots, i_n$, $j_1, \ldots, j_m$ números naturales también, se define el conjunto $V^{j_1,\ldots,j_m}_{i_1,\ldots,i_n}$ como sigue.

$$V^{j_1,\ldots,j_m}_{i_1,\ldots,i_n} = \{v \in \mathcal{C} \mid (v)_{i_k} = 1 \text{ para cada } k \leq n \text{ y } (v)_{j_l} = 0 \text{ para cada } l \leq m\}$$

Es decir, el conjunto de sucesiones tales que n de sus entradas están fijas e iguales a 1 y otras m están fijas e iguales a 0. Se nota que si existen k, l tales que $i_k = j_l$ entonces $V^{j_1,\ldots,j_m}_{i_1,\ldots,i_n}$ es el conjunto vacío; para evitar la anexión repetitiva del vacío, se supondrá también que $i_k \neq j_l$ para cada $k \leq n$ y $l \leq m$. Si n o m es cero entonces se suprimirán los subíndices o superíndices respectivamente y se colocará una estrella, por ejemplo, si $m = 0$ al conjunto se le denotará simplemente con $V^{\star}_{i_1,\ldots,i_n}$.

Se ocuparán estos conjuntos para definir una base topológica para el conjunto $\mathcal{C}$.

Lema C.0.18. *Sea $\beta = \{V^{j_1,\ldots,j_m}_{i_1,\ldots,i_n} \mid n, m, i_1, \ldots, i_n, j_1, \ldots, j_m$ son naturales y $i_k \neq j_l$ para cada $k \leq n$ y $l \leq m\}$. Entonces β es base de una topología τ en $\mathcal{C}$.*

Demostración. Si $n = m = 0$ entonces $\mathcal{C} = V^{\star}_{\star} \in \beta$, de donde se tiene que $\bigcup \beta = \mathcal{C}$.

Sean $V_1, V_2 \in \beta$ tales que $V_1 \cap V_2 \neq \emptyset$, entonces existen n_1, n_2, m_1, m_2 naturales que indizan a los naturales $i^1_1, \ldots, i^1_{n_1}$, $i^2_1, \ldots, i^2_{n_2}$, $j^1_1, \ldots, j^1_{m_1}$, $j^2_1, \ldots, j^2_{m_2}$ (donde el superíndice no denota potenciación o alguna función aritmética, simplemente se ocupa para diferenciar unos índices de otros) tales que

$$V_1 = V^{j^1_1,\ldots,j^1_{m_1}}_{i^1_1,\ldots,i^1_{n_1}} \qquad \text{y} \qquad V_2 = V^{j^2_1,\ldots,j^2_{m_2}}_{i^2_1,\ldots,i^2_{n_2}}$$

[1] Ver la definición A.3.7.

Luego, si $v \in V_1 \cap V_2$ entonces se cumple que $(v)_r = 1$ si $r \in \{i_1^1, \ldots, i_{n_1}^1, i_1^2, \ldots, i_{n_2}^2\}$ y que $(v)_s = 0$ si $s \in \{j_1^1, \ldots, j_{m_1}^1, j_1^2, \ldots, j_{m_2}^2\}$, esto es, $v \in V_{i_1^1,\ldots,i_{n_1}^1,i_1^2,\ldots,i_{n_2}^2}^{j_1^1,\ldots,j_{m_1}^1,j_1^2,\ldots,j_{m_2}^2}$ el cual se denotará por V_3.

Por último, es fácil darse cuenta de que $V_3 \subseteq V_1 \cap V_2$. □

Se tiene que cada abierto básico es infinito (no numerable), además, se cumple que es cerrado (esto es, un conjunto *clopen*[2]), como muestra el siguiente lema.

Lema C.0.19. *Si $V \in \beta$ entonces V es cerrado.*

Demostración. Sea $V \in \beta$, se considera que tiene la forma $V = V_{i_1,\ldots,i_n}^{j_1,\ldots,j_m}$, luego $v \in V^c$ si y solo si $v \in \bigcup_{k\leq n} V_\star^{i_k} \cup \bigcup_{l\leq m} V_{j_l}^\star$, en efecto, si v no está en V es porque (y solo porque) es una sucesión con un 1 en alguna posición j_l o con un 0 en algún i_k. Así, el complemento de V es unión de abiertos básicos, por lo que es un abierto, esto es, V es cerrado. □

Corolario C.0.20. *Todo conjunto $A \subseteq \mathcal{C}$ que sea unión finita de abiertos básicos es clopen.*

Demostración. Al ser unión de abiertos es abierto, para mostrar que es cerrado basta aplicar el lema anterior y las leyes de De'Morgan para conjuntos. □

Esto es todo lo que se necesita para definir el puente entre la lógica proposicional y el espacio topológico $(\mathcal{C}, \tau)$. Para ello, se pensará a cada valuación v como un elemento de $\mathcal{C}$ (de allí la notación sugestiva) puesto que, como se mencionó, toda valuación queda unívocamente determinada por sus valores en cada átomo p_k. Así, si v es una valuación de la lógica entonces se corresponde con el único elemento $v \in \mathcal{C}$ tal que $[\![p_k]\!]_v = (v)_k$. Así, se pensará que los elementos de $\mathcal{C}$ son valuaciones.

Sea $[\![\cdot]\!] : \text{PROP} \to \mathcal{P}(\mathcal{C})$ con $\varphi \mapsto [\![\varphi]\!] = \{v \in \mathcal{C} \mid [\![\varphi]\!]_v = 1\}$, es decir, esta función manda a cada proposición al conjunto de valuaciones que la hacen verdadera. Por ejemplo, $[\![p_0]\!] = V_0^\star$ y $[\![p_5 \to p_6]\!] = V_\star^5 \cup (V_5^\star \cap V_6^\star) = V_\star^5 \cup V_6^\star$. En general, se tiene el siguiente resultado.

Proposición C.0.21. *Sean φ, ψ proposiciones. Se cumple lo siguiente.*

a) $[\![\varphi]\!]$ *es clopen.*

b) $[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\varphi]\!]$; $[\![\varphi \vee \psi]\!] = [\![\varphi]\!] \cup [\![\varphi]\!]$ *y* $[\![\neg\varphi]\!] = [\![\varphi]\!]^c$.

c) $\vDash \varphi$ *si y solo si* $[\![\varphi]\!] = \mathcal{C}$.

d) $\vDash \varphi \to \psi$ *si y solo si* $[\![\varphi]\!] \subseteq [\![\psi]\!]$.

Demostración. La demostración completa de esta proposición es más extensa que compleja, por lo que solo se mostrará parte de ella siendo lo faltante argumentos análogos a los presentados. Conviene primero demostrar la parte *b)* lo cual es sencillo siendo cuidadosos en las diferencias del lenguaje y el meta-lenguaje al aplicar la definición de valuación.

b) Sea $v \in \mathcal{C}$. $v \in [\![\varphi \wedge \psi]\!]$ si y solo si $[\![\varphi \wedge \psi]\!]_v = 1$, si y solo si $[\![\varphi]\!]_v = 1$ y $[\![\psi]\!]_v = 1$, si y solo si $v \in [\![\varphi]\!]$ y $v \in [\![\psi]\!]$, si y solo si $v \in [\![\varphi]\!] \cap [\![\psi]\!]$; todo esto muestra que $v \in [\![\varphi \wedge \psi]\!]$ si y solo si $v \in [\![\varphi]\!] \cap [\![\psi]\!]$, esto es, $[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\psi]\!]$. De manera análoga se muestra que $[\![\varphi \vee \psi]\!] = [\![\varphi]\!] \cup [\![\psi]\!]$.

Sea $v \in \mathcal{C}$. $v \in [\![\neg\varphi]\!]$ si y solo si $[\![\neg\varphi]\!]_v = 1$, si y solo si $[\![\varphi]\!]_v = 0$, si y solo si $v \notin [\![\varphi]\!]$, si y solo si $v \in [\![\varphi]\!]^c$; esto es, $[\![\neg\varphi]\!] = [\![\varphi]\!]^c$.

De manera similar se muestra que $[\![\varphi \to \psi]\!] = [\![\varphi]\!]^c \cup [\![\psi]\!]$ y que $[\![\varphi \leftrightarrow \psi]\!] = ([\![\varphi]\!] \cap [\![\psi]\!]) \cup ([\![\varphi]\!]^c \cap [\![\psi]\!]^c)$.

[2]De la abreviación en el inglés, un conjunto es *clopen* en un espacio topológico si es cerrado (*closed*) y abierto (*open*) a la vez.

a) Se procede por inducción sobre PROP.

- Si $\varphi = p_i$ entonces $[\![\varphi]\!] = V_i^\star$ que, por el lema C.0.19, es clopen. Si $\varphi = \bot$ entonces $[\![\varphi]\!] = \emptyset$ el cual es clopen.
- Si $\varphi = \neg\psi$ entonces $[\![\varphi]\!] = [\![\psi]\!]^c$, por hipótesis de inducción, $[\![\psi]\!]$ es clopen, y el complemento de cualquier clopen es a su vez clopen.
- Si $\varphi = \varphi_1 \square \varphi_2$. Si $\square = \wedge$ se tiene, por *b)*, que $[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\psi]\!]$, por hipótesis de inducción, $[\![\varphi]\!]$ y $[\![\psi]\!]$ son clopen, luego $[\![\varphi]\!] \cap [\![\psi]\!]$ es clopen. De manera similar se muestra el resultado para $\square \in \{\vee, \to, \leftrightarrow\}$.

c) Se sigue inmediatamente de la definición de tautología.

d) Se mostrará equivalentemente que $\nvDash \varphi \to \psi$ si y solo si $[\![\varphi]\!] \nsubseteq [\![\psi]\!]$.

$\nvDash \varphi \to \psi$ si y solo si existe una valuación v tal que $[\![\varphi \to \psi]\!]_v = 0$, si y solo si existe una valuación v tal que $[\![\varphi]\!]_v = 1$ y $[\![\psi]\!]_v = 0$, si y solo si $v \in [\![\varphi]\!]$ y $v \notin [\![\psi]\!]$, si y solo si $[\![\varphi]\!] \nsubseteq [\![\psi]\!]$. □

La definición de este puente se puede extender a los conjuntos de proposiciones de la siguiente manera, sea $[\![\cdot]\!] : \mathcal{P}(\text{PROP}) \to \mathcal{P}(\mathcal{C})$ con $\Gamma \mapsto [\![\Gamma]\!] = \{v \in \mathcal{C} \mid [\![\psi]\!]_v = 1 \text{ para cada } \psi \in \Gamma\}$, esto es, asocia a cada conjunto de proposiciones con el conjunto de valuaciones que hacen verdad a todos sus elementos. Para el caso en que el subconjunto sea unitario ($\Gamma = \{\varphi\}$) se omitirá el uso de corchetes, así la notación para $[\![\{\varphi\}]\!]$ es simplemente $[\![\varphi]\!]$, con lo cual esta definición es una extensión de la anterior. El siguiente lema muestra algunas propiedades inmediatas.

Lema C.0.22. *Sean* $\Delta, \Gamma \subseteq \text{PROP}$ *y* $\varphi \in \text{PROP}$*, se cumple.*

- $[\![\Gamma]\!] = \bigcap_{\psi \in \Gamma} [\![\psi]\!]$.
- $[\![\Gamma]\!]$ *es cerrado.*
- *Si* $\Delta \subseteq \Gamma$ *entonces* $[\![\Gamma [\![\subseteq [\![\Delta]\!]$.
- $\Gamma \vDash \varphi$ *si y solo si* $[\![\Gamma]\!] \subseteq [\![\varphi]\!]$.

Por el teorema de completitud y los lemas 1.1.19 y 1.1.23 se tiene que Γ es consistente si y solo si $[\![\Gamma]\!] \neq \emptyset$. Para un último resultado, se definirá la función $[\cdot] : \mathcal{P}(\mathcal{C}) \to \mathcal{P}(\text{PROP})$ de una manera natural en este contexto, esto es, $V \mapsto [V] = \{\varphi \mid [\![\varphi]\!]_v = 1 \text{ para cada } v \in V\}$; así, en analogía con la anterior, esta función asocia a cada conjunto de valuaciones V el conjunto de proposiciones $[V]$ que son verdaderas bajo todos los elementos $v \in V$. Si V es unitario ($V = \{v\}$) se simplifica la notación utilizando $[v]$.

Proposición C.0.23. *Sea* $\Gamma \subseteq \text{PROP}$. Γ *es maximalmente consistente si y solo si existe* $v \in \mathcal{C}$ *tal que* $\Gamma = [v]$

Demostración. $\Leftarrow$). Se supone que $\Gamma = [v]$ para algún $v \in V$. Sea $\Delta \subseteq \text{PROP}$ tal que $\Gamma \subsetneq \Delta$, entonces existe $\varphi \in \Delta$ tal que $\varphi \notin \Gamma$, por hipótesis se tiene que $[\![\varphi]\!]_v = 0$, por lo que $[\![\neg\varphi]\!]_v = 1$, así $\neg\varphi \in \Gamma$ y por lo tanto $\neg\varphi \in \Delta$; de donde Δ es inconsistente. Luego, Γ es maximalmente consistente.

$\Rightarrow$). Se supone que Γ es maximalmente consistente. Por el lema 1.1.23 existe $v \in V$ tal que $[\![\varphi]\!]_v = 1$ para cada $\varphi \in \Gamma$; por lo tanto, $\Gamma \subseteq [v]$, por lo anterior, $[v]$ es consistente y como Γ es maximalmente consistente, $\Gamma = [v]$. □

Bibliografía

[1] Amor Montaño, José Alfredo, *Compacidad en la lógica de primer orden y su relación con el teorema de completud*; 3ra edición, Universidad Nacional Autónoma de México, 2013.

[2] Amor Montaño, José Alfredo, *La teoría de conjuntos en el siglo XX*; Miscelánea Matemática No. 31, año 2000, pp. 1-27.

[3] Bovykin, Andrey & Kaye, Richard, *Order-types of models of Peano arithmetic: a short survey*; 2001.

[4] Casarrubias Segura, Fidel & Tamariz Mascarúa, Ángel, *Elementos de topología de conjuntos*; Facultad de Ciencas, Universidad Nacional Autónoma de México, 2011.

[5] Cutland, Nigel, *Computability. An introduction to recursive function theory*; Press Syndicate of the University of Cambridge, 1980.

[6] Gentzen, Gerhard, *Untersuchungen über das logische schließen. I*; Mathematische Zeitschrift 39(2), pp. 176–210, 1934.

[7] Gentzen, Gerhard, *Untersuchungen über das logische schließen. II*; Mathematische Zeitschrift 39(3), pp. 405–431, 1935.

[8] García Máynez, Adalberto, *Introducción a la topología de conjuntos*; 1a edición, Aportaciones Matemáticas, Universidad Nacional Autónoma de México, 2011.

[9] Gödel, Kurt, *Die vollständigkeit der axiome des logischen funktionenkalküls*, Monatshefte für Mathematik 37(1), pp. 349–360.

[10] Hernández Hernández, Fernando, *Teoría de conjuntos. Una introducción*; 3a edición, Universidad Nacional Autónoma de México, 2014.

[11] Hilbert, David, *Fundamentos de las matemáticas*; 2da edición, colección MATHEMA, Faculdad de Ciencias, Universidad Nacional Autónoma de México, 2011.

[12] Kaye, Richard, *Models of Peano arithmetic*; Oxford University Press, New York, USA, 1991.

[13] Kaye, Richard, *Tennenbaum's theorem for models of arithmetic*; on *Set Theory, Arithmetic, and Foundations of Mathematics: Theorems, Philosophies*, Cambridge University Press, 2011, pp. 66-79.

[14] Landau, Edmund, *Foundations of analysis*; (traducción al inglés por F. Steinhard del original en alemán *Grundlagen der Analysis*) Chelsea Publishing Company, 1966

[15] Mendelson, Elliott, *Introduction to mathematical logic*; Fourth edition, Chapman & Hall, 1997.

[16] Peano, Giuseppe, *Arithmetices principia, nova methodo exposita*; Ediderunt Fratres Bocca, 1889.

[17] Švejdar, Vítězslav, *Infinite natural numbers: an unwanted phenomenon, or a useful concept?*; The Logica Yearbook 2010, pp. 283–294, College Publications, London, 2011.

[18] van Dalen, Dirk, *Logic and structure*; Springer, 5th editon, 2013.

[19] van Oosten, Jaap, *Gödel incompleteness and nonstandar models*; 2015.