TEOREMA DE KALMAR
A PARTIR DE UN ENFOQUE ALGEBRAICO
DE LOS TEOREMAS DE COMPLETITUD E INCOMPLETITUD DE GÖDEL

Por

Javier Andrés Alberdi Baptista

Presentado en cumplimiento de los
requerimientos para optar al grado de
Licenciado en Matemática por la
Universidad Mayor de San Andrés
La Paz, Bolivia
2019

Se deja esta página en blanco intencionalmente.

El límite del hombre es la perfección, si transita el Tao (camino)

si y solo si el camino es el producto de la Ciencia, el Arte y el Amor.

(A.Alberdi, 1985)

Índice general

Resumen

Los teoremas que se profundizan en el presente trabajo, son los dos teoremas de Kurt Gödel (1906-1978) primero el de Completitud para el Cálculo de Predicados de Primer Orden y segundo el de Incompletitud en Sistemas Axiomáticos, con el objetivo final de llegar a una consecuencia genérica de este último, debida a Kalmar, de esta manera se exhibirá el enfoque algebraico, sustentando la demostración de estos teoremas.

En particular, el Teorema de Incompletitud de Gödel es uno de los resultados fundamentales de la Lógica Matemática de mediados del siglo XX (1930-1931), que inclusive fue considerado como "*La verdad matemática más importante del siglo*".

Para la exposición de los teoremas se pueden tomar varios caminos, de ellos el enfoque más interesante es el algebraico. Usando resultados del Álgebra Universal para construir una base puramente algebraica de la Lógica Matemática, desde el Cálculo Proposicional hasta las Teorías Axiomáticas de Primer Orden, las funciones recursivas y el Teorema de Incompletitud de Gödel.

En el contexto del trabajo, el Teorema de Completitud de Gödel se resume a lo siguiente: "*En el Cálculo de Predicados* $Pred(V, R)$*, una proposición es una conclusión de un subconjunto de* $Pred(V, R)$ *si y solo si se puede deducir del mismo subconjunto*". El Teorema de Incompletitud de Gödel señala que "*Cualquier teoría efectivamente axiomatizada que admita a los Naturales como modelo, es incompleta*". Finalmente resumimos el teorema de Kalmar: "*Si el Cálculo de Predicados* $Pred(V, R)$ *contiene relaciones al menos binarias, es Indecidible.*"

La construcción de estos resultados se fundamenta en definiciones completamente algebraicas, el Teorema de Completitud de Gödel con base en el Cálculo de Predicados y el Teorema de Incompletitud de Gödel en un contexto general de Teorías Matemáticas de Primer Orden y Máquinas de Turing, también definidas algebraicamente. El Teorema de Kalmar es una consecuencia del Teorema de Church, en base al Teorema de Incompletitud de Gödel.

Abstract

The theorems that are deepened in the present work, are the two theorems of Kurt Gödel (1906-1978), first the Completeness of the First Order Predicate Calculus and second the Incompleteness in axiomatic systems, with the ultimate goal of reaching a generic consequence of the latter, due to Kalmar, exhibiting an algebraic approach and supporting the demonstration of these theorems.

In particular, Gödel's Incompleteness Theorem is one of the fundamental results in Mathematical Logic of the mid-twentieth century (1930-1931), which was even considered as "*The most important mathematical truth of the century* ".

For the exposition of the theorems, several paths can be taken, but the most interesting approach is the algebraic one. Using results from Universal Algebra to construct a purely algebraic basis of Mathematical Logic, from Propositional Calculus to First Order Axiomatic Theories, recursive functions and Gödel's Incompleteness Theorem.

In the context of the work, Gödel's Completeness Theorem is summarized as follows: "*In the Predicate Calculus* $Pred(V, R)$*, a proposition is a conclusion of a subset of* $Pred(V, R)$ *if and only if it can be deduced from the same subset* ". Gödel's Incompleteness Theorem states that " *Any theory effectively axiomatized that admits the Naturals as a model is incomplete* ". Finally we summarize Kalmar's theorem: " *If Predicate Calculus* $Pred(V, R)$ *contains at least binary relations, it is Indecidible* ".

The construction of these results is completely based on algebraic definitions, the Gödel Completeness Theorem is based on the Predicate Calculus and Gödel's Incompleteness Theorem in a general context of First Order Mathematical Theories and Turing Machines, also defined algebraically. The Kalmar Theorem is a consequence of Church's Theorem, based on Gödel's Incompleteness Theorem.

Agradecimientos

El principio de gratitud no solamente es un valor importante en nuestras vidas, sino también una consecuencia lógica de nuestro razonamiento.

Cuando contamos con un marco conceptual que rige nuestras acciones, cuyo devenir transcurre en el espacio-tiempo[1], todos nosotros nos encontramos en un punto en el que no habría sido posible llegar sin la participación y decisiones de cada una de las personas que nos rodean.

En este punto me encuentro rodeado de un cúmulo de historia, que se encuentra impregnada de recuerdos, que a su vez se presentan atemporalmente, permitiendo que confluyan en el presente cada una de las personas cuyos conos de tiempo se cruzaron con el mío. Sin embargo, lamentablemente, los mecanismos neurológicos de defensa nos impiden en un lapso corto de tiempo denotar suficientes personas importantes, siendo riesgoso inclusive listar las necesarias.

Por este motivo me disculpo contigo, querido lector, por no mencionarte explícitamente en mis agradecimientos, puedes estar completamente seguro que eres muy importante para mi. El hecho de leer este párrafo no solamente te hace merecedor de mi agradecimiento, sino también te posiciona en él explícitamente. Te lo digo sinceramente y de corazón.

Mira mis ojos, mi gesto y mi sonrisa, que se encuentran en tus recuerdos en este momento y notarás mi sinceridad, me llena de orgullo que estés leyendo esto, eres importante para mi, puedes estar seguro que te recuerdo y realmente te agradezco.

La vida llega y se va, las personas que viven en nuestro corazón permanecen incólumes, eternas, inmortales, los círculos concéntricos de nuestro entorno nos dan la seguridad necesaria para que el viaje temporal limitado trascienda nuestra pequeñez, permitiéndonos trascender.

[1] Aunque posiblemente tenga unas dimensiones adicionales (positivas o negativas).

La influencia de una persona, no solo se mide en el periodo de tiempo a su lado, sino en el impacto que tiene[2], esto explica que una persona pueda estar agradecida con seres que nunca ha conocido, seres que están presentes por la FE, seres que están inmersos en el AMOR, seres que comparten la CIENCIA y seres que sienten el ARTE.

Y, como ya sabes, muchas gracias sobre todo a ti.

La Paz, Bolivia

[2]Teniendo una atemporalidad casi como los números.

TEOREMA DE KALMAR A PARTIR DE UN ENFOQUE ALGEBRAICO DE LOS TEOREMAS DE COMPLETITUD E INCOMPLETITUD DE GÖDEL

Capítulo 1

Prólogo

Kurt Gödel, de familia alemana, nacido en Brünn, ciudad del Imperio Austro-Húngaro (actualmente Brno, República Checa) el 28 de abril de 1906, estudió Matemática en la universidad de Viena, doctorándose en 1930 bajo la tutoría de Hans Hahn. Su tesis doctoral de apenas 11 páginas, fue el primer trabajo donde se resolvió la pregunta de si los axiomas de un sistema formal son suficientes para que las sentencias verdaderas en cualquier modelo del sistema, puedan ser probadas. La respuesta a este interrogante fue el establecimiento de la completitud del cálculo de predicados de primer orden, conocido ahora como el Teorema de Completitud de Gödel. Luego de la publicación de estos resultados, por la Academia de Ciencias de Viena, Gödel se perfiló como un gran estudioso de los fundamentos de la matemática, llegando a ser considerado actualmente como uno de los más relevantes lógicos de todos los tiempos, a la altura de Aristóteles.

Durante su vida universitaria, tuvo gran influencia en él su participación en el Círculo de Viena[1], junto a Moritz Schilk, Hans Hahn y Rudolf Carnap, siendo impulsado a la lógica matemática luego de haber trabajado en teoría de números y luego de estudiar a B. Russell en su *Introduction to Mathematical Philosophy*. Sin embargo el rumbo de vida fue determinado por su participación en un seminario sobre completitud y consistencia dictado por D. Hilbert y por la lectura de *Grundzüge der theoretischen Logik* (*Fundamentos de lógica teórica*) de D. Hilbert y W. Ackerman [Hilbert and trad.Víctor Sánchez, 1975].

[1]El Círculo de Viena (Wiener Kreis), grupo de filósofos formado alrededor de Moritz Schlick sobre todo por profesores de la Universidad de Viena, centro formador del "Positivismo Lógico", donde la experiencia es la única fuente de conocimiento y el método preferido para resolver problemas filosóficos es la lógica simbólica, aspectos en los que justamente Gödel disentía.

En 1931, publicó su obra más célebre: *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme* (Sobre proposiciones formalmente indecidibles de Principia Mathematica y sistemas relacionados) [Gödel and trad. B.Meltzer, 1992] y [Gödel and trad. B.Hirzel, 2000]. Allí, se prueba que cualquier sistema axiomático computable (en el que existen procesos computables), donde se pueda desarrollar la aritmética de los números naturales (Axiomas de Peano o Zermelo-Fraenkel), no puede ser simultáneamente consistente y completo, además que la consistencia de sus axiomas no puede ser probada en el mismo sistema. La prueba involucra el uso de una relación entre el sistema lógico y los números naturales (llamada numeración de Gödel, que sin embargo fue también desarrollada en paralelo por Tarski), obteniendo un enunciado verdadero que afirma su propia improbabilidad a partir de una fórmula numérica, independiente del sistema formal que se haya tomado.

Este hito en la historia de la matemática echó por tierra los intentos de encontrar un conjunto de axiomas suficiente para toda ella o un proceso computable suficiente para absolver todas las preguntas en esta ciencia; los intentos más importantes para lograr estas suposiciones erradas fueron desarrollados durante casi 50 años por Gotlob Ferge a finales del siglo XIX, B. Russell y A. Whitehead con el *Principia Mathematica* y D. Hilbert con su formalismo logicista a inicios del siglo XX, plasmado en el segundo de sus aclamados 23 problemas en el año 1900 ("Probar que los axiomas de la aritmética son consistentes").

Debido fundamentalmente a la anexión de Austria por parte de Alemania (el *Anschluss*), la consideración de Gödel como apto para el servicio en el ejército y, el inicio de la Segunda Guerra Mundial, en 1940 Gödel y su esposa huyeron de Viena usando la ruta del Japón hacia Estados Unidos, país que antes había recibido a Gödel en sus conferencias en la American Mathematical Society, el Institute for Advanced Studies de Princeton y la Universidad de Notre Damme entre 1935 y 1938. En estas sus visitas conoció y se hizo buen amigo de Albert Einstein.

Los resultados que obtuvo Gödel durante su vida en Princeton fueron variados y profundos, citamos aquí algunos de ellos:

- La primera definición aceptada en el ámbito matemático de "función recursiva" y de "computabilidad," usando sus técnicas de numeración.
- La consistencia del axioma de elección y de la hipótesis generalizada del continuo, a través de una reformulación de la teoría de conjuntos en el que existen clases y conjuntos más simples. En esta teoría de conjuntos denominada NGB[2],

[2]Originalmente P.Bernays, alumno de D.Hilbert, había planteado una teoría de conjuntos, que había sido utilizada por J.Von Neumann en sus obras lógicas posteriores y K.Gödel se basó en estos trabajos.

el axioma de elección y la hipótesis generalizada del continuo son verdaderos, y por tanto deben ser consistentes con los axiomas de Zermelo-Fraenkel. Posteriormente P. Cohen construyó un modelo donde el axioma de elección y la hipótesis generalizada del continuo son falsos, concluyéndose que ambos son independientes de la teoría de conjuntos de Zermelo-Fraenkel.

- La existencia de soluciones paradójicas a las ecuaciones de campo de Einstein en Teoría de la Relatividad General, mediante universos que rotan, en lugar de expandirse. En este modelo de universo donde se presenta una métrica especial, se debe escoger cuidadosamente la constante cosmológica para que coincida con partículas de arena que giran en una distribución homogénea. Aquí existen Curvas Cerradas Temporales (*Closed Timelike Curves*) que permiten que los conos de luz (descripción futura de un evento) roten en cualquier dirección espacio-temporal, permitiendo un viaje redondo a través del tiempo, retornando al exacto punto del espacio-tiempo donde se partió.

- La existencia de Dios mediante una prueba ontológica, basada en la obra de San Anselmo (Anselmo de Canterbery) y de G. W. Leibniz. Usando lógica modal determinó 5 axiomas (luego complementadas por A. Anderson) que determinan el comportamiento de las propiedades "positivas" formando un ultrafiltro, de donde se define una propiedad Tipo-Dios (*Godlikeness*), luego se define la esencia y la existencia necesaria como propiedad. Llamamos "Dios" al único objeto en todas las realidades o mundos de la lógica modal, que tiene la propiedad Tipo-Dios.

- La existencia de una deficiencia en la Constitución de los Estados Unidos, que permitiría que un dictador tome el poder. Esto fue expresado por Gödel mismo el 5 de diciembre de 1947 al juez que le otorgó la nacionalidad estadounidense frente a sus amigos A. Einstein y O. Morgentern (co-creador de la teoría de juegos). Sin embargo la prueba de esta afirmación nunca fue publicada o detallada por Gödel, manteniéndose aún como un misterio.

- Varios comentarios filosóficos, expresando sus propios criterios basados en el Platonismo; estos comentarios fueron expresados de manera muy concisa en breves artículos, en general no publicados hasta varios años luego de su muerte.

La volatilidad de la nacionalidad de Gödel (austro-húngaro de nacimiento, checoslovaco en 1918, austriaco en 1929, alemán en 1938 y estadounidense en 1947), se refleja también en su inestabilidad psicológica y social. Desde muy niño fue extremadamente inteligente (le llamaban *Herr Warum*, señor "Por qué"), en 1912 sufrió de fiebre reumática, que aunque completamente curada le dejó con la convicción que sufrió daño permanente al corazón. Gödel era tímido, retraído y excéntrico, creía que permanentemente trataban de envenenarlo con gas venenoso que emitían los refrigeradores, creía que el General MacArthur fue substituido por un impostor (a partir

de mediciones de su nariz), veía fantasmas, creía de manera paranoica en fuerzas que trabajaban en el mundo que aplacaban al bien y solamente comía los alimentos preparados por su esposa, por temor a ser envenenado, ni siquiera comía los alimentos que él mismo preparaba. Este último fue el motivo de su muerte en Princeton el 14 de enero de 1978, al negarse a comer, pues su esposa estaba incapacitada de moverse por una enfermedad, murió de 33 kilos de peso por "malnutrición e inanición causadas por desordenes de personalidad."

A pesar de una vida trágica, Kurt Gödel recibió distinciones muy importantes para su época, harto merecidas en vista de su trayectoria intelectual, citaremos unas cuantas de ellas:

- Miembro del selecto Círculo de Viena.
- Profesor emérito del Instituto para Estudios Avanzados de Princeton en 1976.
- Merecedor del primero de los Premios Albert Einstein en 1951.
- Merecedor de la Medalla Nacional de Ciencia de Estados Unidos en 1974.
- Doctor Honorario de la Universidad de Harvard en 1952, donde se señaló al Teorema de Incompletitud de Gödel como "La verdad matemática más importante del siglo."

Para terminar con esta breve biografía, citamos algunos conceptos que tuvieron personalidades mundiales sobre Kurt Gödel:

Para el septuagésimo quinto aniversario de la Academia de Ciencia de Ohio, en Columbus, sede de la Universidad Estatal de Ohio, el 22 de abril de 1966, se celebraron el sexagésimo cumpleaños de Kurt Gödel y el trigésimo quinto aniversario de la publicación de sus teoremas de incompletitud, esta celebración tomó la forma de un simposio, (Festschrift Symposium o Gödel Symposium). En esa oportunidad, el Dr. J. Robert Oppenheimer expresó su salutación en los siguientes términos:

> "*Es un honor y un placer para mi colaborar en la celebración a Kurt Gödel, su aniversario y su gran trabajo, que no solamente profundizó y enriqueció de forma inconmensurable el conocimiento de la estructura lógica con importantes argumentos abstractos y matemáticos, sino iluminó el papel de la limitación del conocimiento humano en general. Yo saludo a los profesores, muchos con grandes distinciones, quienes se reunieron para honrar a Gödel, presentando sus descubrimientos y sus enfoques, y espero que las contribuciones en esta ocasión lleven gran placer al hombre que los inspiró.*"[3]

[3]Traducción libre [Jack J. Bulloff and Hahn, 1969] pág. VIII

En marzo de 1951 Kurt Gödel recibió el premio "Albert Einstein" y en esta ocasión John von Neumann realizó un tributo con las siguientes palabras:

> "*La hazaña de Kurt Gödel en lógica moderna es singular y monumental - de hecho es más que un monumento, es un hito histórico que permanecerá ampliamente visible en el espacio y el tiempo. Ora que nada comparable a ella ha ocurrido en la lógica de los tiempos modernos o no, pueda dar curso a debate; en todo caso, los aproximados concebibles son muy, muy pocos. El sujeto de la lógica ha ciertamente cambiado completamente su naturaleza y posibilidades con la hazaña de Gödel.*
>
> *El nombre de Gödel está asociado con muchos importantes logros en detalle y con dos absolutamente decisivos*[4]*. Esta ocasión se presta, pienso, para hablar solamente de estos últimos.*
>
> *La naturaleza del primero es sencilla de mencionar, aunque su carácter y ejecución técnicas exactas escaparían de una adecuada caracterización sin las técnicas especializadas e intrincadas de la lógica formal.*
>
> *Gödel fue el primero en demostrar que ciertos teoremas*[5] *matemáticos no pueden ser probados o refutados con los rigurosos y aceptados de la matemática. En otras palabras, él demostró la existencia de proposiciones matemáticas indecidibles. Más allá de este resultado, él probó que una proposición específica muy importante pertenecía a esta clase de problemas indecidibles: La pregunta de si la matemática está libre de contradicciones internas. El resultado es remarcable en su casi paradójica "auto-negación": Nunca será posible lograr con medios matemáticos la certidumbre que la matemática no contiene contradicciones. Debe hacerse énfasis que el punto importante es, que este no es un principio filosófico o una actitud intelectual plausible, sino el resultado de una prueba matemática rigurosa de tipo extremadamente sofisticado.*
>
> *La formulación que acabo de realizar sólo expuso toscamente el resultado y eliminó algunos de los finos aspectos de su rigurosa formulación, pero si uno quiere plantear el teorema sin recurrir al difícil lenguaje técnico de la lógica formal, pienso que esta es la mejor alternativa.*

[4]Se observa que son tres los resultados remarcables, donde el primero de ellos es el Teorema de Completitud, el segundo el Teorema de Incompletitud y el tercero la prueba de la consistencia del axioma de elección y la hipótesis del continuo (coincidiendo en los dos últimos con von Neumann).

[5]En rigor, debería señalarse que son ciertas proposiciones verdaderas, no ciertos teoremas.

> *De hecho, Gödel probó su teorema no respecto a la matemática solamente, sino para todos los sistemas que permitan una formalización, esta es una descripción rigurosa y exhaustiva, en términos de la lógica moderna: Ningún sistema puede probarse libre de contradicción, en términos del sistema mismo.*
>
> *El segundo*[6] *resultado decisivo de Gödel solamente puede ser expresado en la terminología de lógica formal y de la importante aunque recóndita disciplina matemática moderna: La teoría de conjuntos. Dos teoremas conjeturados de teoría de conjuntos, o mejor dos principios, el así llamado "Principio de Elección" y la así llamada "Hipótesis del Continuo" resistieron por 50 años todo intento de demostración. Gödel probó que ninguno de los dos puede refutarse por medios matemáticos. Para el primero de ellos sabemos que no puede ser probado tampoco, para el segundo, parece que ocurriera lo mismo, sin embargo no parece posible que alguien inferior a Gödel sea capaz de probarlo*[7].
>
> *No intentaré una evaluación detallada de estos logros, me limitaré a repetir: En la historia de la lógica, ellos son enteramente singulares. Antes de Gödel no se había establecido rigurosamente la indemostrabilidad propia dentro de la matemática. El objeto en la lógica nunca más será el mismo."*[8]

La amistad legendaria que unía a Gödel y Einstein se reflejaba en las largas caminatas que hacían en Princeton conversando sobre temas cuya naturaleza era un misterio para todos los demás miembros del Instituto. Oskar Morgenstern, economista y muy amigo de ambos en el Instituto para Estudios Avanzados de Princeton, indica que, al final de su vida, A. Einstein le confió que "*su obra ya no significaba mucho, que él venía al Instituto para tener el privilegio de poder regresar a casa con Gödel.*"[9]

1.1. Observaciones sobre Terminología

Se ha visto por conveniente introducir este punto, debido a la variedad existente en la terminología a emplear, específicamente sobre las palabras "Completitud" e "Incompletitud," sus sinónimos y algo de etimología.

---

[6] "Tercero."

[7] Gran halago para Paul Cohen, quien en 1963 logró la prueba.

[8] Traducción libre [Jack J. Bulloff and Hahn, 1969] págs. IX,X.

[9] De acuerdo a [Wang and trad. Pilar Castillo, 1987], pg.70

Gödel en sus obras usa los términos *Entscheidungsdefinitheit* en alemán y *Completeness* en inglés refiriéndose a la calidad y acción de completo, que en español tiene cuatro sinónimos: "Completitud," "Compleción," "Completud" y "Completez." Los cuatro se encuentran en el Diccionario de la Lengua Española[10] como sustantivos y sinónimos entre sí. En este trabajo se hará uso del primero de los cuatro términos señalados, aunque se ha podido observar que el tercero es usado de manera algo más frecuente en las traducciones.

Se entiende como "Completitud" la característica de un sistema formal —Completo— donde se puede determinar si una proposición o su negación son teoremas. En este sentido no deberíamos confundir "completo" con "lleno."

En relación al término *Entscheidungsdefinitheit*, desglosado en *Entscheidung* o decisión y *definieren* o determinar, más el sufijo *heit* expresa la característica intrínseca del concepto buscado. De esta manera, interpretamos el término *Entscheidungsdefinitheit* como la cualidad de determinar la decisión fundamental —en nuestro caso, si una proposición o su negación son teoremas—, dejando de lado el término análogo *vollständigkeit* que, rústicamente, significa completitud haciendo referencia al sinónimo "lleno" (*voll*) de "completo."[11]

En idiomas menos rigurosos como español o inglés se hace referencia a la definición en Lógica Matemática de "Teoría Completa" (donde se sabe que una proposición o su negación son teoremas), usando "Completitud" y *Completeness*.

Se entiende como "Incompletitud" la característica de un sistema formal incompleto, donde NO se puede determinar si una proposición o su negación son teoremas. En este sentido no deberíamos confundir "incompleto" con "no lleno."

Aunque en inglés se usa muy comúnmente el término *Uncompleteness*, siendo válido en el idioma de Shakespeare, en el idioma de Cervantes, al menos en el Diccionario de la Lengua Española [Espanola, 2001], no existen los términos "Incompletitud," "Incompleción," "Incompletud" ni "Incompletez,"[12] aunque las reglas (un tanto coloquiales) del prefijo "*in*" permiten el uso actual de estos términos, haciendo referencia correspondiente a la negación de los cuatro términos mencionados previamente.

Sobre el término "Indecidible,"[13] que hace referencia a proposiciones que aunque verdaderas no pueden ser probadas o refutadas en un sistema axiomático, este sí se encuentra en el Diccionario de la Lengua Española, como un adjetivo referido a filosofía. Se hace notar que Gödel utiliza los términos *Unentscheidbare* en alemán y

[10] Conforme [Espanola, 2001].

[11] Conforme se puede observar en [Ale, 1967]

[12] Se empleará en el trabajo cualquiera de los cuatro términos mencionados arriba.

[13] Para este término, no existe de dónde escoger.

undeceidable en inglés para esta expresión.

Se observa que a diferencia del término "Completitud," en los tres idiomas estas acepciones tienen la misma etimología y hacen referencia a la imposibilidad de una decisión, en nuestro caso decidir si la proposición puede o no ser probada.

En referencia al término "Indecidibilidad," que no existe formalmente en el Diccionario de la Lengua Española [Espanola, 2001], sin embargo se hace nuevamente uso coloquial de las reglas para el sufijo "*dad*" para convertir un adjetivo (Indecidible) en sustantivo abstracto derivado.

1.2. Contextualización

El presente trabajo tiene como objeto central al Teorema de Incompletitud de Gödel, sin embargo se amplía hasta el resultado de László Kalmar, donde se muestra que si el cálculo de predicados (lenguaje predicativo) contiene al menos una relación (constante predicativa) binaria, este lenguaje no permite la construcción de un algoritmo que determine si una fórmula es válida (demostrable) o no. Este resultado se conoce también por el Teorema de Church-Kalmar, pues su demostración se basa en el resultado de Alonzo Church, que indica el mismo resultado mencionado pero con relaciones cuaternarias.

Se observa que, para la prueba del Teorema de Incompletitud de Gödel, no se seguirá el camino usual, sino que se inicia en los resultados de Alan Turing, quien fue el primero en definir adecuadamente la noción de algoritmo, mediante las "máquinas de Turing" y solucionar el "problema de parada" (*halting problem*[14]), que básicamente señala que dada una descripción de un programa y una entrada finita, determinar si el programa con esta entrada termina o corre indefinidamente. La solución de este problema es negativa y más aún, la prueba del mismo es suficiente para dar pie a una prueba del teorema de incompletitud de Gödel.

Se entiende por Lógica Algebraica a la rama de la Lógica Matemática que toma los conceptos algebraicos para fundamentar la misma, convirtiendo al Álgebra casi paradójicamente en una "metateoría" para la Lógica Matemática, enfocando los resultados y problemas lógicos con herramientas y métodos ya establecidos en Álgebra.

Para el sustento de las demostraciones de los teoremas señalados, usaremos el enfoque de la Lógica Algebraica[15]. Este enfoque es usado —independientemente de la "paradoja" mencionada[16]— con el objetivo de exponer la rigurosidad matemática con

[14] "Dada la descripción de un programa y una entrada finita, decidir si el programa termina de correr o corre indefinidamente, dada esa entrada."

[15] Conforme [Barnes and trad. Xambó Descamps, 1978]

[16] Esta "paradoja" no es tal, pues no se intenta dar fundamento a la Lógica Matemática —filosófico o de otra índole—, solamente formular un mecanismo de construcción tan preciso de la misma, que inclusive admite la demostración de los Teoremas de Gödel y Kalmar.

que puede desarrollarse la teoría y demostrarse los teoremas mencionados, usando las poderosas aunque sutiles herramientas algebraicas.

Por otra parte, en el desarrollo del cálculo de proposiciones (enunciados), también se probará, haciendo uso de la Lógica Algebraica y los resultados de Adolf Lindenbaum, el Teorema de Completitud de Gödel, que establece que el cálculo de enunciados de primer orden es completo.

Con estos antecedentes y por su importancia en este trabajo, es adecuado conocer un poco de la vida de L. Kalmar.

László Kalmar, nacido el 27 de marzo de 1905 en Edde, Hungría, de donde se mudaron con su madre a Budapest, a la muerte de su padre. Allí terminó sus estudios universitarios en Matemática y Física en 1927, siendo sobresaliente en toda su carrera. Sus mentores József Kürschák y Lipót Fejér le llevaron hasta los límites de la investigación de su época, siendo importante también la colaboración de su discípula Rósa Péter.

Luego de su visita a Göttingen en 1929, su interés fundamental residió en la lógica matemática, que desarrolló en Szeged (ciudad a la que se trasladaron los mejores investigadores de Hungría luego del tratado de Trianon de 1920), donde fue a residir luego de su doctorado, bajo la tutela de Frigyes Riesz y Alfréd Haar. Kalmar obtuvo su profesorado en la Universidad de Szeged en 1947 e inauguró la primera cátedra de Fundamentos de la Matemática y Ciencias de la Computación, siendo su primer docente. Además fundó el Laboratorio de Cibernética y el grupo de investigación de Lógica Matemática y Teoría de Autómatas.

Trabajó en la solución de ciertos casos del problema de decisión para cálculo lógico de primer orden, simplificando los resultados de Paul Isaac Bernays y trabajó sobre ideas de Gödel y Church, siendo reconocido como el más prominente lógico de Hungría. Fue de su interés además la ciencia de la computación, en muchos aspectos, siendo el líder del uso de computadoras en su país.

Recibió muchos honores, como ser miembro de la Academia de Ciencias de Hungría en 1961, recibir el premio Kossuth en 1950 y el premio del estado de Hungría en 1975, siendo ambos los mayores galardones que su país podía imponerle. Además fue presidente honorario de la Sociedad Matemática Janos Bolyai y de la Sociedad para la Ciencia de la Computación John von Neumann. Murió junto a su esposa y sus cuatro hijos en Mátraháza, Hungría el 2 de agosto de 1976.

1.3. Teoremas de Gödel

El presente trabajo tiene como tema central la completitud, en base a los trabajos de Kurt Gödel. En las secciones anteriores se ha presentado una introducción a los teoremas de incompletitud, que se tratarán ahora con mayor detalle. Existen básicamente dos teoremas de completitud que fueron desarrollados por Gödel: la completitud de la lógica proposicional (1930) y la incompletitud de sistemas axiomáticos

que contengan aritmética (1931).

1.3.1. Teorema de completitud

Aunque eclipsado por el teorema de incompletitud, este resultado por sí mismo debería catapultar a Gödel como uno de los más importantes lógicos del siglo pasado. Con este resultado, logró obtener en 1929 su doctorado en matemática en la Universidad de Viena a los 25 años de edad. El resultado no es trivial y su demostración no pudo ser lograda previamente por los mejores lógicos y matemáticos, como observaron Hilbert y Ackerman en [Hilbert and trad.Víctor Sánchez, 1975] en p.68):

> "*El hecho que el sistema de axiomas sea completo, en el sentido que todos los predicados que son válidos para cada dominio de individuos pueden actualmente ser deducibles de ellos es aún un problema no resuelto.*"

Actualmente se presupone este resultado y es mencionado pocas veces, sin embargo es muy profundo y muy sencillo: "El cálculo de predicados de primer orden es completo." En el capítulo 5 se realizará la demostración formal, usando Lógica Algebraica, en el contexto ya señalado.

La demostración que hizo Gödel se basa en el siguiente argumento: Para todo predicado de primer orden P, o P es demostrable o su negación $\sim P$ es válida en el dominio de los naturales. Luego mostró en el estricto sentido de la teoría de prueba de Hilbert que si $\sim P$ es no válida, P es demostrable, usando una variación del Teorema de Löwenheim-Skolem (donde Thoraf Skolem extendió el argumento inicial de Leopold Löwenheim a un infinito numerable de proposiciones), que indica que si una proposición es válida en un dominio no vacío, también lo es en un dominio infinito contable, además de la propiedad de compacidad del cálculo de proposiciones.

Sin embargo el contexto del presente trabajo hace que la prueba más adecuada sea la empleada por Leon Henkin en 1949, donde se usa el teorema de satisfacibilidad, donde se demuestra la existencia de una interpretación o modelo que hace válido todo predicado.

Una observación colateral, que vincula la completitud de la lógica con resultados sobre incompletitud en sistemas axiomáticos, es la paradoja de Skolem (1922), que señala:

> "*Si la teoría axiomática de conjuntos, formulada en el cálculo de predicados de primer orden es consistente, todos los axiomas deben ser verdaderos para un dominio infinito numerable de conjuntos, sin embargo existe un teorema de la teoría que señala que existen innumerables conjuntos de conjuntos.*"

1.3.2. Teorema de incompletitud

Este es el resultado más conocido y comentado de Gödel, además de haber sido descrito como "La verdad matemática más importante del siglo" por la propia Universidad de Harvard, ha sido sido la primera ocasión en que se realizó una demostración enteramente metamatemática con el uso adecuado de mapeos entre sistemas formales.

En este acápite nos basaremos en el documento de Gödel *Uber formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, conforme las traducciones ulteriores y explicaciones de Feferman, Kleene, Dover,Hirzel, Nagel, Newman, Smullyan, Stewart, Wang, Mosterín y otros.[17]

Aunque Gödel conceptualizó este trabajo en una sola obra, existen tres resultados asociados a él, todos de importancia trascendental en la historia de la lógica matemática por el contenido y la forma de exposición.

El contexto en que los teoremas se demostraron inicialmente es el de *Principia Mathematica* (monumental obra de Russell y Whitehead) y sistemas relacionados, posteriormente el contexto se extendió formalmente a sistemas axiomáticos en general e inclusive a sistemas formales como veremos en el capítulo 10, aunque Gödel mismo lo había postulado con una diáfana claridad sobre el alcance y significado de sus descubrimientos.

El primer resultado (teorema de indecidibilidad) se refiere a la existencia de sentencias indecidibles en sistemas formales, que Gödel consideró más importante que los otros, al haber titulado su documento con estas palabras. El segundo resultado derivado de la existencia de indecidibles es que si el sistema de referencia es consistente, este no puede ser completo (teorema de incompletitud). El tercer resultado es derivado del segundo y establece que la consistencia de los axiomas de un sistema no puede ser probado dentro del mismo.

Para probar informalmente el primer resultado es necesario considerar que existe una función inyectiva entre los símbolos del lenguaje de la lógica de primer orden, las palabras y fórmulas que se forman a partir de ellos y finalmente las demostraciones, hacia los números naturales, mediante la aritmetización de los mismos, es decir contar con las operaciones de suma y multiplicación. Asumiendo esto, ordenamos todas las fórmulas $R_n(x)$ que tienen exactamente una variable libre por su número corres-

[17] Conforme [Avigad, 2005], [Barrow, 1998], [Barrow,], [Jack J. Bulloff and Hahn, 1969], [Cattabriga, 2007], [Davis, 2000], [Franzén, 2005], [Gödel and trad. Jesús Mosterín, 1989], [Gödel and trad. B.Meltzer, 1992], [Gödel and trad. B.Hirzel, 2000], [Goldstein, 2005], [Hintikka, 2000], [Hofstadter, 1979], [Kleene, 2000], [Manaster, 1975], [Mendelson, 1964], [Myers,], [Nagel and R.Newmann, 1960], [K.Podnieks, 1992], [Rylov, 2007], [Shanker, 1988], [Smith, 2005], [Smullyan, 1992], [Smullyan, 1987], [Stewart and trad. José María Fraile, 1977], [Tarski, 1971], [Wang and trad. Pilar Castillo, 1987]

pondiente y reemplazamos el número por su variable libre (n corresponde a $R_n(x)$, entonces $R_n(n)$).

Formamos el conjunto K de los números n tales que $R_n(n)$ no puede probarse en el sistema, la fórmula "n pertenece a K" es una de las fórmulas tipo R, la llamaremos S, entonces tenemos las siguientes equivalencias:

$$R_q(q) \Leftrightarrow S(q) \Leftrightarrow q \in K \Leftrightarrow R_q(q) \text{ no puede ser probada.}$$

Se observa que esto significa que sólo se puede establecer la demostrabilidad de $R_q(q)$ si y sólo si no es un teorema, lo que implica establecer una proposición correcta que establece su propia indemostrabilidad. Este tipo de proposiciones se llama indecidible.

La formalización rigurosa de este resultado requiere de la definición detallada y adecuada del sistema de numeración (la función inyectiva brevemente descrita), denominada *Gödelización*, la definición de recursividad primitiva y funciones recursivas, varios lemas sobre éstas, finalmente establecer 46 definiciones y resultados para llegar al teorema de indecidibilidad.

Observamos que el resultado del documento de Gödel solamente se cumple para sistemas ω-consistentes (consistencia en base a predicados sobre números), sin embargo la hipótesis fue debilitada para sistemas solamente consistentes en 1936 por John Barkley Rosser.

El segundo resultado se establece rápidamente observando que si el sistema de referencia es consistente, existen sentencias indecidibles, por tanto no se puede determinar la demostrabilidad o indemostrabilidad de todas las sentencias, así que no puede ser completo.

El tercer resultado que posiblemente sea el importante en términos generales para la lógica matemática (que fue el "golpe de gracia" para las aspiraciones del programa de Hilbert), establece lo siguiente:

> *En un cualquier teoría T formal recursivamente numerable que incluye verdades aritméticas básicas y también ciertas verdades sobre pruebas formales, T incluye una proposición de su propia consistencia si y sólo si T es inconsistente.*

La prueba de este resultado es interesante por su simplicidad, como indica el segundo resultado ya mencionado, si T es consistente entonces A no puede ser probado en T (A es el indecidible $R_q(q)$), pero "A no puede ser probado en T" es exactamente A, por tanto T es consistente implica A, así que no podremos tener en T una prueba de consistencia de T, pues si así fuera, concluiríamos que A es demostrable, lo que contradice la indecidibilidad de A, establecida en el primer resultado.

Se observa que en estos resultados confluyen los conceptos subyacentes en dos paradojas: la paradoja del mentiroso (o de Epimenides) y la paradoja de Richard, aunque ambas son básicamente juegos lógicos, la gran virtud de Gödel fue la formalización rigurosa de todos sus resultados.

La paradoja de Epimenides (o del mentiroso) en su versión original indica "todos los cretenses son mentirosos," frase que se dice repetía Epimenides, un filósofo cretense. Esta paradoja puede reproducirse en varias formas "estoy mintiendo," "nunca digo la verdad" o "este teorema es falso," afirmaciones que linguísticamente son erradas pues son afirmaciones sobre ellas mismas o tienen derivaciones erradas de generalización o temporales. Se puede ver que el concepto de indecidibilidad se basa en esta paradoja. Se ha convertido tan popular esta paradoja autorecurrente que el propio capitán James T. Kirk en un episodio del clásico "*Star Trek*" logró evitar la destrucción de su nave, usando la misma para "confundir" a una raza extra terrestre absolutamente "lógica."[18]

Por su parte la paradoja de Richard es algo más intrincada y describe tanto el procedimiento de la prueba del primer resultado establecido como llegar a un indecidible, primero se establece una correspondencia entre una propiedad lexicográfica de los números naturales (por ejemplo en español: "el primer número natural" es uno, "divisible entre si mismo y el uno" describe a un número primo, etc.), ordenamos estas descripciones en términos de cantidad de letras y su orden alfabético y le asignamos un natural. En caso que el natural asignado n no corresponda a la propiedad descrita, decimos que n es un número Ricardiano. La propiedad "es Ricardiano" es una propiedad asignada a un número natural, supongamos que sea k, nos hacemos la pregunta: ¿es k es Ricardiano? Si fuera así, no correspondería a la propiedad de serlo, por otra parte, si no lo fuera, tendría que serlo por definición. Se observa sin embargo que es una falacia, pues la propiedad "ser Ricardiano" no es lexicográfica sino establece una propiedad sobre la lexicografía usada.

1.3.3. Al grano...

Sin embargo de todo lo establecido, en el contexto que se desarrolla el presente trabajo, se mostrará en detalle las pruebas del Teorema de Completitud del cálculo proposicional de primer orden, de los tres resultados de Gödel y del Teorema de Kalmar, presuponiendo el álgebra para definir y establecer los resultados de lógica matemática.

Se observa nuevamente que en nuestro contexto de lógica algebraica, para mostrar el Teorema de Completitud es necesario establecer el Teorema de Satisfacibilidad y resultados en Álgebras de Lindenbaum. En este mismo contexto, los tres resultados de incompletitud requieren de definiciones y resultados de teorías matemáticas, máquinas de Turing, funciones recursivas, recursividad, resultados sobre satisfacibilidad, axiomas de Peano y aritmética contextualizadas.

[18]Obviamente esta raza alienígena no llegó a tener entre sus científicos a equivalentes de Gödel, Tarski, Turing, Kleene, Rosser, Church, Gentzen, Kalmar o varios de los que se mencionan en el presente estudio.

Es importante señalar que uno de los más importantes logros en este enfoque de la prueba de incompletitud de Gödel, es el resultado debido a Turing, quien en 1936 postuló el "problema de parada" que indica la imposibilidad de la existencia de un algoritmo que determine el comportamiento futuro de cualquier algoritmo, proposición ciertamente indecidible y autorecurrente. Para la prueba rigurosa de este resultado, se usa el Teorema de Incompletitud de Gödel; consiguientemente se observa que es equivalente al mismo.

Sin embargo aquí no se ha considerado suficiente llegar solamente a los resultados de Gödel, sino avanzar un poco más en la historia, mostrando los resultados de Church y Kalmar, los que generalizan los conceptos básicos de incompletitud hacia la lógica de primer orden, estableciéndola dependiente del orden de sus relaciones (si existe una relación binaria se muestra la incompletitud) y usando en el proceso comparación de teorías matemáticas.

En el último capítulo encontraremos nuevamente una discusión no exclusivamente técnica algebraica, donde se expondrán ejemplos, limitaciones, implicaciones, consecuencias y visiones diferentes en base a los resultados de incompletitud de sistemas formales de Gödel.

Capítulo 2

Preliminares Algebraicos

2.1. Álgebras

Definición 2.1.1. Un *tipo* $\mathcal{T}$ es un conjunto T provisto de una aplicación $\mathrm{ar}\colon T \to \mathbb{N}$ de T en el conjunto de los números enteros no negativos. Escribiremos $\mathcal{T} = (T, \mathrm{ar})$, o simplemente T, cuando no cause confusión. Es también conveniente escribir $T_n = \{t \in T : \mathrm{ar}(t) = n\}$, para $n \in \mathbb{N}$.

Definición 2.1.2. Un *álgebra A de tipo T*, o una *T-álgebra*, es un conjunto A provisto de una aplicación $t_A\colon A^{\mathrm{ar}(t)} \to A$ para cada $t \in T$. Los elementos $t \in T_n$ se llaman operaciones n-arias de T-álgebra.

Observación. Se observa que cada aplicación t_A depende tanto del tipo T como del conjunto A.

Definición 2.1.3. Dos T-álgebras A y B se llaman *iguales* si y sólo si $A = B$ y $t_A = t_B$ para todo $t \in T$.

Ejemplo 2.1.4. Sean $A = B = \{0, 1\}$ dos conjuntos y sea $A^0 = B^0 = \{\emptyset\}$. Consideremos las operaciones

$$\begin{array}{lll} +\colon A^2 \longrightarrow A & 0_A\colon A^0 \longrightarrow A & 0_B\colon B^0 \longrightarrow B \\ (a,b) \longmapsto a+b & \emptyset \longmapsto 0 & \emptyset \longmapsto 1. \end{array}$$

Si ponemos $\mathcal{T}_1 = (\{0_A, +\}, \mathrm{ar})$ y $\mathcal{T}_2 = (\{0_B, +\}, \mathrm{ar})$, donde $\mathrm{ar}(0_A) = \mathrm{ar}(0_B) = 0$ y $\mathrm{ar}(+) = 2$. Entonces A es una T_1-álgebra y una T_2-álgebra, siendo ambas T-álgebras distintas.

Ejemplo 2.1.5. Los anillos pueden ser considerados como álgebras de tipo $\mathcal{T} = (\{0, -, +, \cdot\}, \mathrm{ar})$, donde $\mathrm{ar}(0) = 0$, $\mathrm{ar}(-) = 1$, y $\mathrm{ar}(+) = \mathrm{ar}(\cdot) = 2$. Las operaciones están dadas por

$$\begin{array}{cccc} 0\colon \{\emptyset\} \longrightarrow A & -\colon A \longrightarrow A & +\colon A^2 \longrightarrow A & \cdot\colon A^2 \longrightarrow A \\ \emptyset \longmapsto 0 & a \longmapsto -a & (a,b) \longmapsto a+b & (a,b) \longmapsto a \cdot b. \end{array}$$

Ejemplo 2.1.6. Si A es un anillo, entonces todo A-módulo M puede ser considerado como un ejemplo de T-álgebra de tipo $\mathcal{T} = (\{0, -, +\} \cup A, \mathrm{ar})$, donde $\mathrm{ar}(0) = 0$, $\mathrm{ar}(-) = 1$, $\mathrm{ar}(+) = 2$, y $\mathrm{ar}(a) = 1$ para todo $a \in A$. Las operaciones están dadas por

$$\begin{array}{cccc} 0\colon \{\emptyset\} \longrightarrow M & -\colon M \longrightarrow M & +\colon M^2 \longrightarrow M & a\colon M \longrightarrow M \\ \emptyset \longmapsto 0 & m \longmapsto -m & (m,n) \longmapsto m+n & m \longmapsto am. \end{array}$$

Ejemplo 2.1.7. Sea A un anillo dado. Si B es anillo que contiene a A como un subanillo, B puede verse como una T-álgebra de tipo $\mathcal{T} = (\{0, -, +, \cdot\} \cup A, \mathrm{ar})$, donde $\mathrm{ar}(0) = 0$, $\mathrm{ar}(-) = 1$, $\mathrm{ar}(+) = \mathrm{ar}(\cdot) = 2$, y $\mathrm{ar}(a) = 0$ para todo $a \in A$. Las operaciones están dadas por

$$0\colon \emptyset \longmapsto 0 \in A, \qquad -\colon b \longmapsto -b, \qquad +\colon (b,c) \longmapsto b+c,$$
$$\cdot\colon (b,c) \longmapsto b \cdot c, \qquad a\colon \emptyset \longmapsto a.$$

Definición 2.1.8. Sea A una T-álgebra. Un subconjunto B de A se llama una T-*subálgebra* de A, si forma una T-álgebra dotándola de las operaciones que son restricción de las operaciones de A a B, denotándose $B \leq A$. Esto es, si para cada $t \in T$, se verifica que

$$t\colon A^{\mathrm{ar}(t)} \longrightarrow A \quad \text{implica} \quad t|_{B^{\mathrm{ar}(t)}}\colon B^{\mathrm{ar}(t)} \longrightarrow B.$$

Proposición 2.1.9. *Sea $\{B_i : i \in I\}$ una familia arbitraria de subálgebras de A, entonces su intersección $\bigcap_{i\in I} B_i$ es una subálgebra de A.*

Demostración. En efecto, sea $i \in I$ y

$$t|_{B_i^{\mathrm{ar}(t)}} \colon B_i^{\mathrm{ar}(t)} \longrightarrow B_i,$$

luego si $(b_{i_1}, b_{i_2}, \ldots, b_{i_{\mathrm{ar}(t)}}) \in B_i^{\mathrm{ar}(t)}$, entonces $t(b_{i_1}, b_{i_2}, \ldots, b_{i_{\mathrm{ar}(t)}}) \in B_i$. Sea

$$(b_1, b_2, \ldots, b_{\mathrm{ar}(t)}) \in \Big(\bigcap_{i\in I} B_i\Big)^{\mathrm{ar}(t)},$$

entonces para cada $j \in \{1, \ldots, \mathrm{ar}(t)\}$ se tiene que $b_j \in \bigcap_{i\in I} B_i$, de donde, para cada $i \in I$ tenemos que $b_j \in B_i$, luego para cada $i \in I$ tenemos $(b_1, b_2, \ldots, b_{\mathrm{ar}(t)}) \in B_i^{\mathrm{ar}(t)}$; así para cada $i \in I$ tenemos $t(b_1, b_2, \ldots, b_{\mathrm{ar}(t)}) \in B_i$, de donde $t(b_1, b_2, \ldots, b_{\mathrm{ar}(t)}) \in \bigcap_{i\in I} B_i$, esto prueba lo que queríamos. □

Observación. Se observa que la unión de dos T-álgebras no necesariamente es una T-álgebra, por ejemplo, sean los conjuntos $\mathbb{Z}(1) = \{-1, 0, 1\}$ y $\mathbb{Z}(2) = \{-2, 0, 2\}$ con $T = \{t\}$, $ar(t) = 2$, definido por $t(a, 0) = t(0, a) = a$, $t(a, -a) = t(-a, a) = 0$, $t(a, a) = a$. Se puede observar que $\mathbb{Z}(1)$ y $\mathbb{Z}(2)$ forman

Definición 2.1.10. Dado un subconjunto cualquiera X de una T-álgebra A, la menor subálgebra de A que contiene a X es

$$\bigcap\{U : U \text{ subálgebra de } A, U \supseteq X\}.$$

A esta subálgebra se la llama *subálgebra generada por* X y la denotamos por $\langle X\rangle_T$, o por $\langle X\rangle$ si no hay riesgo de confusión.

Ejemplo 2.1.11. Veremos que $\emptyset$ es una subálgebra de A si y sólo si $T_0 = \emptyset$. Por definición, $T_0 = \{t \in T : \mathrm{ar}(t) = 0\}$, luego $\emptyset$ es una subálgebra de A si y sólo si $t|_\emptyset \colon \emptyset^{\mathrm{ar}(t)} \to \emptyset$, para todo $t \in T$. Luego $\emptyset^{\mathrm{ar}(t)} = \emptyset$ si y sólo si $\mathrm{ar}(t) > 0$; si $\mathrm{ar}(t) = 0$ entonces $\emptyset^{\mathrm{ar}(t)} = \{\emptyset\}$. Sea $T = T_0 \cup T_0^*$, donde $T_0^* = \{t \in T : \mathrm{ar}(t) > 0\}$, entonces $T_0 \cap T_0^* = \emptyset$. Si $t \in T_0$, entonces $t|_\emptyset \colon \{\emptyset\} \to \emptyset$, una contradicción; luego $T_0 = \emptyset$. Si

$T_0 = \emptyset$, entonces $t \in T_0^*$ de donde $t|_\emptyset \colon \emptyset \to \emptyset$ lo que implica que $\emptyset$ es una subálgebra de A.

Si A es una T-álgebra y B es una subálgebra de A y $\emptyset \subset B$, entonces $\langle \emptyset \rangle$ es una subálgebra de B.

Ejemplo 2.1.12. Los grupos se pueden considerar como casos especiales de T-álgebras con $\mathcal{T} = (\{*\}, \mathrm{ar})$ donde $\mathrm{ar}(*) = 2$ y $* \colon G \times G \to G$, y también de T'-álgebras con $\mathcal{T}' = (\{e, i, *\}, \mathrm{ar})$ donde $\mathrm{ar}(e) = 0$, $\mathrm{ar}(i) = 1$, $\mathrm{ar}(*) = 2$, y $e \colon \{\emptyset\} \to G$, $i \colon G \to G$, y $* \colon G \times G \to G$. Probaremos primero que toda T'-subálgebra de un grupo es un subgrupo, pero no toda T-subálgebra no vacía es necesariamente un subgrupo. Veamos, sean G un grupo y una T'-álgebra y sea H una T'-subálgebra de G, entonces $e|_H \colon \{\emptyset\} \to H$, $i|_H \colon H \to H$, $*|_H \colon H \times H \to H$, luego H es un grupo. Por otro lado, sea $a \in G$ con $a \neq e$, entonces $\langle a \rangle_T$ es una T-subálgebra de G, donde

$$\langle a \rangle_T = \{a^n : n > 0\}, \qquad a^1 = a, \quad a^p = a^{p-1} * a.$$

Si existe $n > 0$ tal que $a^n = e$, entonces $\langle a \rangle_T$ es un grupo. Si para todo $n > 0$ se tiene que $a^n \neq e$, entonces $\langle a \rangle_T$ no es un grupo.

Ahora probaremos que si G es un grupo finito entonces toda T-subálgebra no vacía de G es ella misma un grupo. Entonces, sea H una T-subálgebra no vacía de G. $\bigcap_{a \in H} \langle a \rangle_T$ es una T-subálgebra de G. Para cada $a \in H$, como $\langle a \rangle_T$ es una T-subálgebra de H, entonces $\bigcap_{a \in H} \langle a \rangle_T$ es una T-subálgebra de H. Como para todo $a \in H$ se tiene que $a \in \langle a \rangle_T$, entonces H es una T-subálgebra de $\bigcap_{a \in H} \langle a \rangle_T$. Por lo tanto, $\bigcap_{a \in H} \langle a \rangle_T = H$.

Ejemplo 2.1.13. Asimismo, podemos mostrar un ejemplo de que la unión de dos subálgebras no es necesariamente un subálgebra:
Sean los grupos $\mathbb{Z}(1) = \{-1, 0, 1\}$ con la operación $\cdot$ y $\mathbb{Z}(2) = \{-2, 0, 2\}$ con la operación $\star$, definidas conforme las siguientes tablas:

$\cdot$	-1	0	1
-1	-1	-1	0
0	-1	0	1
1	0	1	1

$\star$	-2	0	2
-2	-2	-2	0
0	-2	0	2
2	0	2	2

Observamos que realmente ambas operaciones $\cdot$ y $\star$ son la misma y la llamamos $*$, definiendo de la siguiente manera:

$$\begin{aligned} *\colon \mathbb{Z}(1) \times \mathbb{Z}(1) &\longrightarrow \mathbb{Z}(1) \qquad *\colon \mathbb{Z}(2) \times \mathbb{Z}(2) \longrightarrow \mathbb{Z}(2) \\ (a,b) &\longmapsto a * b \qquad\qquad (a,b) \longmapsto a * b \end{aligned}$$

Tales que:

$$a * b = \begin{cases} b & \text{si } a = 0 \\ a & \text{si } b = 0 \\ 0 & \text{si } b = -a \vee a = -b \\ a & \text{si } a = b \\ a + b & \text{(suma usual) en otro caso} \end{cases}$$

Con esta nueva operación $*$, vemos que tanto $\mathbb{Z}(1)$, como $\mathbb{Z}(2)$ e inclusive $\mathbb{Z}$ forman grupos, donde $\mathbb{Z}(1)$ y $\mathbb{Z}(2)$ se convierten en $*$-subgrupos de $\mathbb{Z}$.
Sin embargo si consideramos $\mathbb{Z}(1) \cup \mathbb{Z}(2) = \{-2, -1, 0, 1, 2\}$ con la operación $*$ definida arriba, no es un subgrupo de $(\mathbb{Z}, *)$, ya que ni siquiera cumple la clausura, por ejemplo para $-2 * -1 = (-2) + (-1) = -3$ ó $2 * 1 = 2 + 1 = 3$.

Definición 2.1.14. Sean A y B T-álgebras. Un *homomorfismo* de A en B es una aplicación $\varphi\colon A \to B$ tal que para todo $t \in T$ y $a_1, \ldots, a_n \in A$ $(n = \mathrm{ar}(t))$, se tiene que

$$\varphi(t_A(a_1, \ldots, a_n)) = t_B(\varphi(a_1), \ldots, \varphi(a_n)).$$

Equivalentemente, el diagrama

$$\begin{array}{ccc} A^n & \xrightarrow{t_A} & A \\ {\scriptstyle \varphi^n}\downarrow & & \downarrow{\scriptstyle \varphi} \\ B^n & \xrightarrow[t_B]{} & B \end{array}$$

debe conmutar, i.e., $\varphi \circ t_A = t_B \circ \varphi^n$.

Sean $\varphi\colon A \to B$ y $\psi\colon B \to C$ dos homomorfismos, veamos que la composición $\psi \circ \varphi\colon A \to C$ es un homomorfismo. Si $n = \mathrm{ar}(t)$, entonces tenemos

$$\begin{array}{ll} \varphi^n\colon A^n \longrightarrow B^n & \psi^n\colon B^n \longrightarrow C^n \\ (a_i)_{i=1}^n \longmapsto (\varphi(a_i))_{i=1}^n & (b_i)_{i=1}^n \longmapsto (\psi(b_i))_{i=1}^n \end{array}$$

de donde

$$(\psi^n \circ \varphi^n)(a_i)_{i=1}^n = \psi^n(\varphi(a_i))_{i=1}^n = ((\psi \circ \varphi)(a_i))_{i=1}^n = (\psi \circ \varphi)^n(a_i)_{i=1}^n.$$

Luego tenemos el diagrama con cuadrados conmutativos

$$\begin{array}{ccc} A^n & \xrightarrow{t_A} & A \\ {\scriptstyle \varphi^n}\downarrow & & \downarrow{\scriptstyle \varphi} \\ B^n & \xrightarrow{t_B} & B \\ {\scriptstyle \psi^n}\downarrow & & \downarrow{\scriptstyle \psi} \\ C^n & \xrightarrow{t_C} & C \end{array}$$

entonces

$$\psi \circ \varphi \circ t_A = \psi \circ (t_B \circ \varphi^n) = (\psi \circ t_B) \circ \varphi^n = t_C \circ \psi^n \circ \varphi^n = t_C \circ (\psi \circ \varphi)^n.$$

Por tanto, $\psi \circ \varphi$ es un homomorfismo.

Además, si $\varphi\colon A \to B$ es inversible, entonces la aplicación $\varphi^{-1}\colon B \to A$ es un homomorfismo. En efecto, si existe φ^{-1} entonces

$$\begin{array}{ccc} B & \xrightarrow{\varphi^{-1}} & A \\ {\scriptstyle t_B}\uparrow & & \uparrow{\scriptstyle t_A} \\ B^n & \xrightarrow[\varphi^{-n}]{} & A^n \end{array}$$

donde $\varphi^{-n} = (\varphi^{-1})^n$, de donde $a = \varphi^{-1} \circ t_B(b_i)_{i=1}^n$ implica que

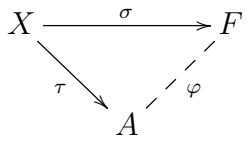
$$\varphi(a) = \varphi \circ \varphi^{-1} \circ t_B(b_i)_{i=1}^n = t_B(b_i)_{i=1}^n,$$

y $a' = t_A \circ \varphi^{-n}(b_i)_{i=1}^n = t_A(\varphi^{-1}(b_i))_{i=1}^n$ implica que

$$\varphi(a') = \varphi \circ t_A(\varphi^{-1}(b_i))_{i=1}^n = t_B \circ \varphi^n(\varphi^{-1}(b_i))_{i=1}^n = t_B(\varphi \circ \varphi^{-1}(b_i))_{i=1}^n = t_B(b_i)_{i=1}^n.$$

2.2. Álgebras Libres

Definición 2.2.1. Sea X un conjunto, F una T-álgebra y $\sigma\colon X \to F$ una aplicación. Diremos que F es una *T-álgebra libre* (estrictamente hablando sería preciso decir (F,σ)) con conjunto de *generadores libres* X si para toda T-álgebra A y toda aplicación $\tau\colon X \to A$, existe un único homomorfismo $\varphi\colon F \to A$ tal que $\varphi \circ \sigma = \tau$.

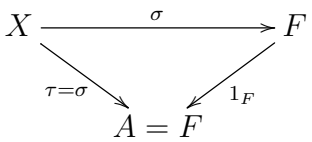


Proposición 2.2.2. *La aplicación σ es inyectiva.*

Demostración. En efecto, sean $x_1, x_2 \in X$ distintos, entonces existen $A = \langle\{x_1, x_2\}\rangle_T$ y $\tau\colon X \to A$ dada por $x \mapsto x$ tales que $\tau(x_1) \neq \tau(x_2)$. Por definición, existe un único homomorfismo $\varphi\colon F \to A$ tal que $\varphi \circ \sigma = \tau$, por lo que $\varphi \circ \sigma(x_1) \neq \varphi\sigma(x_2)$. Si fuera $\sigma(x_1) = \sigma(x_2)$, entonces sería $\varphi(\sigma(x_1)) = \varphi(\sigma(x_2))$ lo que es una contradicción. Por tanto, σ es inyectiva. □

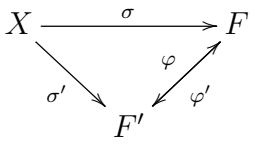
Teorema 2.2.3. *Dado un conjunto X y un tipo $\mathcal{T}$, existe una T-álgebra libre sobre X. Dicha T-álgebra libre sobre X es única salvo isomorfismos.*

Demostración. (a) `Unicidad`. Primero mostramos que si (F,σ) es libre sobre X y $\varphi\colon F \to F$ es un homomorfismo tal que $\varphi \circ \sigma = \sigma$, entonces $\varphi = 1_F$. En efecto, tomemos $A = F$ y $\tau = \sigma$ en la condición que define F.



Como $1_F\colon F \to F$ también resuelve el problema, de la unicidad requerida en la definición de F, se tiene que $\varphi = 1_F$.

Sean ahora (F, σ) y (F', σ') libres sobre X. Entonces existen homomorfismos $\varphi\colon F \to F'$ y $\varphi'\colon F' \to F$ tales que $\varphi \circ \sigma = \sigma'$ y $\varphi' \circ \sigma' = \sigma$, es decir, el diagrama



es conmutativo. De aquí se tiene que

$$\begin{array}{l} \sigma' = \varphi \circ \sigma = \varphi \circ \varphi' \circ \sigma' \\ \sigma = \varphi' \circ \sigma' = \varphi' \circ \varphi \circ \sigma \end{array} \quad \text{lo que implica que} \quad \begin{array}{l} \varphi \circ \varphi' = 1_{F'} \\ \varphi' \circ \varphi = 1_F. \end{array}$$

Así que φ y φ' son isomorfismos inversos y con ello la unicidad queda demostrada.

(b) `Existencia`. Construimos un álgebra F como la reunión de ciertos conjuntos F_n $(n \in \mathbb{N})$, definidos inductivamente como sigue:[1]

(i) $F_0 = X \cup T_0$.

(ii) Supuesto definido F_r para $0 < r < n$, definimos

$$F_n = \Big\{(t, a_1, \ldots, a_k) : t \in T,\ \mathrm{ar}(t) = k,\ a_i \in F_{r_i},\ \sum_{i=1}^{k} r_i = n - 1\Big\}.$$

(iii) Pongamos

$$F = \bigcup_{n \in \mathbb{N}} F_n.$$

Para definir en el conjunto F una estructura de T-álgebra tenemos que especificar la acción de las operaciones $t \in T$.

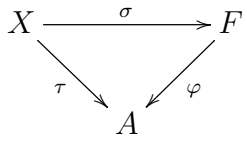
(iv) Si $t \in T_k$ y $a_1, \ldots, a_k \in F$, pongamos $t(a_1, \ldots, a_k) = (t, a_1, \ldots, a_k) \in F$. En particular, si $t \in T_0$, entonces $t\colon \{\emptyset\} \to F_0 \subset F$ está dada por $\emptyset \mapsto t_F$.

Esto convierte a F en una T-álgebra. Para completar la construcción, se tiene que definir una aplicación $\sigma\colon X \to F$.

[1] Recuérdese que $T_n = \{t \in T : \mathrm{ar}(t) = n\}$.

(v) Para cada $x \in X$, pondremos $\sigma(x) = x \in F_0$.

Para terminar tenemos que demostrar que F es libre sobre X, esto es, se tiene que ver que si A es una T-álgebra y $\tau\colon X \to A$ una aplicación de X en A, entonces existe un único homomorfismo $\varphi\colon F \to A$ tal que el diagrama



conmuta. Hacemos esto construyendo inductivamente la restricción φ_n de φ a F_n y viendo que φ_n está determinada completamente por τ y φ_k con $k < n$.

Tenemos que $F_0 = T_0 \cup X$. Por la condición de homomorfismo tendremos $\varphi_0(t_F) = t_A\colon \{\emptyset\} \to A$ para $t \in T_0$, mientras que $\varphi_0(x) = \tau(x)$ para todo $x \in X$. Así pues, $\varphi_0\colon F_0 \to A$ está definida unívocamente por las condiciones que ha de satisfacer φ.

Supongamos ahora que φ_k está unívocamente determinada para $k < n$. Un elemento de F_n $(n > 0)$ es de la forma $(t, a_1, \ldots, a_n)$, donde $t \in T_k$, $a_i \in F_{r_i}$ y $\sum_{i=1}^{k} r_i = n-1$. Como además $(t, a_1, \ldots, a_k) = t(a_1, \ldots, a_k)$ y φ ha de ser un homomorfismo, debe ser

$$\varphi(t, a_1, \ldots, a_k) = t(\varphi(a_1), \ldots, \varphi(a_k)),$$

luego existe un único homomorfismo $\varphi_n\colon F_n \to A$ definido por

$$\varphi_n(t, a_1, \ldots, a_k) = t(\varphi_{r_1}(a_1), \ldots, \varphi_{r_k}(a_k)),$$

lo cual determina unívocamente φ_n, pues $\varphi_{r_i}(a_i)$ están unívocamente definidos para $i = 1, \ldots, k$. Como todo elemento de F pertenece a un único F_n, poniendo $\varphi(\alpha) = \varphi_n(\alpha)$ si $\alpha \in F_n$ $(n \geq 0)$, se ve que φ es un homomorfismo de F en A que satisface la condición

$$\varphi(\sigma(x)) = \varphi_0(x) = \tau(x)$$

para todo $x \in X$ y φ es único con estas condiciones. □

Observación. Sea A una T-álgebra y sea F la T-álgebra libre sobre el conjunto $X_n = \{x_1, \ldots, x_n\}$. Para toda sucesión de elementos (no necesariamente distintos)

$a_1, \ldots, a_n \in A$, existe un único homomorfismo $\varphi\colon F \to A$ tal que $\varphi(x_i) = a_i$ $(i = 1, \ldots, n)$. Si $w \in F$, entonces $\varphi(w) \in A$ está unívocamente determinado por $a_1, \ldots, a_n$. Luego podemos definir una aplicación $w_A\colon A^n \to A$ dada por $(a_1, \ldots, a_n) \mapsto \varphi(w)$. Si en particular tomamos $A = F$ y $a_i = x_i$ $(i = 1, \ldots, n)$, entonces $\varphi = 1_F$ y $w(x_1, \ldots, x_n) = w$.

Definición 2.2.4. Una *T-palabra* en las *variables* $x_1, \ldots, x_n$ es un elemento de la T-álgebra libre sobre el conjunto $X_n = \{x_1, \ldots, x_n\}$, de generadores libres.

Definición 2.2.5. Una *palabra* en los elementos $a_1, \ldots, a_n$ de la T-álgebra A es un elemento $w(a_1, \ldots, a_n) \in A$, donde w es una T-palabra en las variables $x_1, \ldots, x_n$.

Definición 2.2.6. Una *variable de T-álgebra* es un elemento del conjunto de generadores libres de una T-álgebra libre.

Entre las palabras en las variables $x_1, \ldots, x_n$ figuran las palabras x_i $(i = 1, \ldots, n)$, que tienen la propiedad de que

$$x_i(a_1, \ldots, a_n) = a_i.$$

Ejemplo 2.2.7. Sea F la T-álgebra libre sobre $X = \{x\}$ donde $T = \{t\}$ y $\mathrm{ar}(t) = 1$. Entonces tenemos primero que

$$F_0 = T_0 \cup X = X = \{x\},$$

luego, tenemos que

$$F_n = \Big\{(t, a_1, \ldots, a_k) : t \in T_k,\ a_i \in F_{r_i},\ \sum_{i=1}^{k} r_i = n - 1\Big\},$$

de donde, en particular

$$F_1 = \{(t, a_1) : t \in T,\ a_1 \in F_0\} = \{(t, x)\}$$
$$F_2 = \{(t, a_1) : t \in T,\ a_1 \in F_1\} = \{(t, a_1)\},$$

por lo que $\#F_n = 1$ y $\#F = \#\mathbb{N}$.

Ejemplo 2.2.8. Sea $T = \emptyset$ y X un conjunto cualquiera. Entonces, $F_0 = X$ y

$$F_1 = \left\{(t, a_1, \ldots, a_k) : t \in T_k,\ a_i \in F_{r_i},\ \sum_{i=1}^{k} r_i = n - 1\right\} = \emptyset,$$

de donde, $F_n = \emptyset$ para $n > 0$. Por lo tanto, $F = F_0 = X$, es decir, la T-álgebra libre sobre X coincide con X.

Ejemplo 2.2.9. Sea ahora $T = \{t\}$ con $\text{ar}(t) = 2$ y sea $X = \{x\}$, entonces

$$F_0 = T_0 \cup X = \{x\}$$
$$F_1 = \{(t, a_1, a_2) : a_1 \in F_0,\ a_2 \in F_0,\ t \in T_2\} = \{(t, x, x)\}$$
$$F_2 = \{(t, a_1, a_2) : a_1 \in F_1,\ a_2 \in F_0,\ a_1 \in F_0,\ a_2 \in F_1\} = \{(t, a_1, x), (t, x, a_2)\},$$

de donde $\#F = \#\mathbb{N}$.

Ejemplo 2.2.10. Sea $T = \{t, u\}$ con $\text{ar}(t) = 0$ y $\text{ar}(u) = 2$ y sea $X = \emptyset$, entonces

$$F_0 = T_0 \cup X = \{t\} \cup \emptyset = \{t\} \quad \text{implica} \quad \#F_0 = 1$$
$$F_1 = \{(t, a_1, a_2) : a_1, a_2 \in F_0\} \quad \text{implica} \quad \#F_1 = 1$$
$$F_2 = \{(t, a_1, a_2) : a_1 \in F_0,\ a_2 \in F_1,\ a_1 \in F_1,\ a_2 \in F_0\} \quad \text{implica} \quad \#F_2 = 2 \cdot 1$$
$$F_3 = \{(t, a_1, a_2) : a_1 \in F_{r_1},\ a_2 \in F_{r_2},\ r_1 + r_2 = 2\} \quad \text{implica} \quad \#F_3 = 3 \cdot 2,$$

de donde se tiene que

$$\#F_n = n \cdot \#F_{n-1},$$

lo que implica

$$\#\bigcup_{n\in\mathbb{N}} F_n = \sum_{n\in\mathbb{N}} \#F_n = \sum_{n\in\mathbb{N}} n \cdot \#F_{n-1} = \#\mathbb{N}.$$

Ejemplo 2.2.11. Supongamos que T es contable (finito o numerable) y que existen $t \in T_0$ y $t' \in T_k$ para algún $k > 0$. Si $\#X = \#\mathbb{N}$, mostraremos que $\#F = \#\mathbb{N}$. Veamos, por definición

$$F_0 = T_0 \cup X,$$

lo que implica $\#F_0 = \#\mathbb{N} + 1 = \#\mathbb{N}$, luego

$$F_1 = \bigcup_{\ell=1}^{k} \Big\{ (t, a_1, \ldots, a_\ell) : \mathrm{ar}(t) = \ell,\ a_i \in F_0,\ \sum_{i=1}^{\ell} 0 = 0 \Big\},$$

lo que implica $\#F_1 = \#\mathbb{N}$, luego

$$F_2 = \bigcup_{\ell=1}^{k} \Big\{ ((t, a_1, \ldots, a_\ell) : \mathrm{ar}(t) = \ell,\ a_i \in F_{r_i},\ \sum_{i=1}^{\ell} r_i = 1 \Big\},$$

lo que implica $\#F_2 = \#\mathbb{N}$, luego

$$F_n = \bigcup_{\ell=1}^{k} \Big\{ ((t, a_1, \ldots, a_\ell) : \mathrm{ar}(t) = \ell,\ a_i \in F_{r_i},\ \sum_{i=1}^{\ell} r_i = n - 1 \Big\},$$

lo que implica $\#F_n = \#\mathbb{N}$, y finalmente

$$F = \bigcup_{n \in \mathbb{N}} F_n$$

y esto último implica $\#F = \#\mathbb{N}$.

2.3. Variedades de Álgebras

Sea F la T-álgebra libre sobre un conjunto numerable $X = \{x_1, x_2, \ldots\}$ de variables. Si w es un elemento de F, w es una palabra sobre algún conjunto finito $X_n = \{x_1, \ldots, x_n\} \subset X$.

Definición 2.3.1. Una *relación de identidad* para T-álgebras es un par $(u, v) \in F \times F$. Si existe un n tal que u, v pertenecen al álgebra libre sobre X_n, en este caso decimos que (u, v) es una *relación de identidad en n variables*.

Definición 2.3.2. Decimos que una T-álgebra A *satisface* la relación de identidad (u, v), o que (u, v) es una *ley* de A si $u(a_1, \ldots, a_n) = v(a_1, \ldots, a_n)$ cualesquiera que sean $a_1, \ldots, a_n \in A$. Equivalentemente, (u, v) es una ley de A si $\varphi(u) = \varphi(v)$ para todo homomorfismo $\varphi \colon F \to A$.

Definición 2.3.3. Sea L un conjunto de relaciones de identidad para T-álgebras. La clase

$$V = \{A \ T\text{-álgebra} : A \text{ satisface } (u, v) \quad \forall (u, v) \in L\}$$

se llama una *variedad de T-álgebras definida por L*. A las relaciones de identidad satisfechas por todas las álgebras de V se las llama *leyes de la variedad*. Obsérvese que

$$\{(u, v) : (u, v) \text{ es ley de la variedad } V\} \supset L,$$

pero puede ser distinto de L.

Ejemplo 2.3.4. Supongamos que $T = \{*\}$ con $\text{ar}(*) = 2$ y que

$$L = \{(u, v)\} = \{(x_1 * (x_2 * x_3), (x_1 * x_2) * x_3)\}.$$

Si A satisface (u, v), entonces para todo $a, b, c \in A$ se tiene que $a * (b * c) = (a * b) * c$. Por lo tanto, la variedad V definida por L es la clase de todos los semigrupos.

Ejemplo 2.3.5. Supongamos que $T = \{e, i, *\}$ con $\text{ar}(e) = 0$, $\text{ar}(i) = 1$, y $\text{ar}(*) = 2$, y que

$$L = \{(x_1 * (x_2 * x_3), (x_1 * x_2) * x_3), (e * x_1, x_1), (i(x_1) * x_1, e)\},$$

entonces las álgebras de la variedad V definida por L son grupos.

Ejemplo 2.3.6. Sea $T = \{*, i, e\}$ con $\text{ar}(*) = 2$, $\text{ar}(i) = 1$, y $\text{ar}(e) = 0$, además sea

$$L = \{(x_1 * (x_2 * x_3), (x_1 * x_2) * x_3), (x_1 * x_2, x_2 * x_1), (e * x_1, x_1), (i(x_1) * x_1, e)\},$$

entonces la variedad V definida por L es la clase de todos los grupos abelianos.

Ejemplo 2.3.7. Sea A un anillo con unidad y M un A-módulo unitario izquierdo. Supongamos que $T = \{*, i, e\} \cup A$, donde $\text{ar}(*) = 2$, $\text{ar}(i) = 1$, $\text{ar}(e) = 0$, y para cada $a \in A$ se tiene $a \colon M \to M$ dada por $m \mapsto a \cdot m$ ($\text{ar}(a) = 1$). Entonces M es una T-álgebra. M es un grupo abeliano, entonces

$$a(m * n) = am * an \qquad (a + b)m = am * an \qquad (ab)m = a(bm)$$

$$1m = m \qquad 0m = 0 \qquad (-a)m = i(am)y$$

y tenemos el diagrama conmutativo

$$\begin{array}{ccc} M & \xrightarrow{a} & M \\ {\scriptstyle *}\uparrow & & \uparrow{\scriptstyle *} \\ M^2 & \xrightarrow[(a,a)]{} & M^2 \end{array}$$

Si ponemos

$$L' = \{(a(m*n), a(m)*a(n)), ((a+b)(m), a(m)*b(m)), ((ab)(m), a(b(m))),$$
$$(1(m), m), (0(m), e), ((-a)(m), i(a(m)))\},$$

entonces la variedad V definida por $L \cup L'$ es la clase de todos los A-módulos unitarios izquierdos.

Ejemplo 2.3.8. Sea A un anillo conmutativo con unidad, y sea B un anillo conmutativo con unidad, A subanillo de B y $1_A = 1_B$. Supongamos que $T = \{0, i, +, \cdot, 1\} \cup A$ donde $\mathrm{ar}(0) = \mathrm{ar}(1) = 0$, $\mathrm{ar}(i) = 1$, $\mathrm{ar}(+) = \mathrm{ar}(\cdot) = 2$, y para todo $a \in A$ ($\mathrm{ar}(a) = 0$) $a\colon \{\emptyset\} \to B$ está dada por $\emptyset \mapsto a$. Entonces B es una T-álgebra. B es un grupo abeliano con $a(bc) = (ab)c$, $a(b+c) = ab + ac$, $ab = ba$, $1a = a$, $0a = 0$, y $i(a)b = i(ab)$.

Ejemplo 2.3.9. ¿Es la clase de los grupos finitos una variedad? Sea $T = \{*, i, e\}$, y pongamos

$$L = \{(x_1 * (x_2 * x_3), (x_1 * x_2) * x_3), (e * x_1, x_1), (i(x_1) * x_1, e), (x_1 * e, x_1), (x_1 * i(x_1), e)\},$$

entonces la clase de los grupos finitos es una variedad, definida por L.

2.4. Álgebras Relativamente Libres

Sea V la variedad de T-álgebras definida por el conjunto de leyes L.

Definición 2.4.1. Una T-álgebra A de la variedad V, es un *álgebra (relativamente) libre* en V sobre un conjunto X de *generadores (relativamente) libres* (donde se supone dada una aplicación $\sigma\colon X \to A$, usualmente inyectiva) si para toda aplicación $\tau\colon X \to B$ de X en una T-álgebra B de V existe un único homomorfismo $\varphi\colon A \to B$ tal que $\varphi \circ \sigma = \tau$.

Definición 2.4.2. Una T-álgebra A se llama *relativamente libre* si existe una variedad V con $A \in V$ tal que A es relativamente libre en V.

Teorema 2.4.3. *Sea T un tipo arbitrario, L cualquier conjunto de leyes y V la variedad de T-álgebras definido por L. Para todo conjunto X existe una T-álgebra de V libre en V sobre X.*

Demostración. Sea (F, ρ) la T-álgebra libre sobre X. Definamos una relación de congruencia en F poniendo $u \sim v$ (donde $u, v \in F$) si y sólo si $\varphi(u) = \varphi(v)$ para todo homomorfismo $\varphi\colon F \to A$ donde $A \in V$. Esta relación es de equivalencia. Sea ahora $t \in T_k$ y $u_i \sim v_i$ $(i = 1, \ldots, k)$, entonces para todo homomorfismo $\varphi\colon F \to A$ con $A \in V$ tendremos $\varphi(u_i) = \varphi(v_i)$, y, por tanto

$$\varphi(t(u_1, \ldots, u_k)) = t(\varphi(u_1), \ldots, \varphi(u_k)) = t(\varphi(v_1), \ldots, \varphi(v_k)) = \varphi(t(v_1, \ldots, v_k))$$

lo que implica que $t(u_1, \ldots, u_n) \sim t(v_1, \ldots, v_m)$, es decir, $\sim$ es una relación de congruencia.

Sea

$$R = \{\overline{u} : u \in F\} \quad \text{donde} \quad \overline{u} = \{v \in F : u \sim v\},$$

podemos definir $t\colon R^k \to R$ $(t \in T_k)$ poniendo

$$t(\overline{u}_1, \ldots, \overline{u}_k) = \overline{t(u_1, \ldots, u_k)}.$$

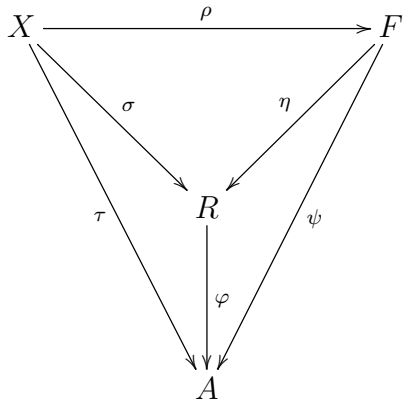
Como lo anterior está bien definido, R es una T-álgebra. La aplicación $u \mapsto \overline{u}$ es un homomorfismo $\eta\colon F \to R$. En efecto, si $t \in T_k$, entonces

$$\begin{aligned} \eta(t(u_1, \ldots, u_k)) &= \overline{t(u_1, \ldots, u_k)} = t(\overline{u}_1, \ldots, \overline{u}_k) \\ &= t(\eta(u_1), \ldots, \eta(u_k)). \end{aligned}$$

Definamos finalmente $\sigma\colon X \to R$ por $\sigma(x) = \overline{\rho(x)} = \eta(\rho(x))$.

Vamos a demostrar que (R, σ) es relativamente libre sobre X. Sea una T-álgebra $A \in V$ y $\tau\colon X \to A$. Como (F, ρ) es libre sobre X, entonces existe un único $\psi\colon F \to A$

homomorfismo tal que $\varphi \circ \rho = \tau$.



Sea $\varphi\colon R \to A$ dada por $\overline{u} \mapsto \psi(u)$. Esta aplicación está bien definida porque si $\overline{u} = \overline{v}$, entonces $\eta(u) = \eta(v)$ lo que implica $u \sim v$ y esto implica que $\psi(u) = \psi(v)$. Por otro lado, la aplicación φ es un homomorfismo, pues si $t \in T_k$, entonces

$$\begin{aligned}\varphi(t(\overline{u}_1, \ldots, \overline{u}_n)) &= \varphi(\overline{t(u_1, \ldots, u_n)}) = \psi(t(u_1, \ldots, u_n)) = t(\psi(u_1), \ldots, \psi(u_n)) \\ &= t(\varphi(\overline{u}_1), \ldots, \varphi(\overline{u}_n)),\end{aligned}$$

además

$$\varphi \circ \sigma = \varphi \circ \eta \circ \rho = \psi \circ \rho = \tau.$$

Si $\varphi'\colon R \to A$ es otro homomorfismo tal que $\varphi'\sigma = \tau$, entonces $\varphi'\eta\rho = \tau = \psi\rho$ y como ρ es inyectiva se tiene que $\varphi'\eta = \psi$. De lo cual resulta que, para todo $\overline{u} \in R$

$$\varphi'(\overline{u}) = \varphi'\eta(u) = \psi(u) = \varphi(\overline{u})$$

y por consiguiente $\varphi' = \varphi$. □

Observación. x es una V-*variable* si $x \in X$ y existe F T-álgebra libre sobre X con $F \in V$. w es una V-*palabra* en las V-variables $x_1, \ldots, x_n$ si $w \in F$ y $F \in V$ es una T-álgebra libre sobre $\{x_1, \ldots, x_n\}$.

Capítulo 3

Cálculo de Proposiciones

3.1. Álgebras de Proposiciones

Definición 3.1.1. Sea $T = \{F, \Rightarrow\}$ donde $\text{ar}(F) = 0$ y $\text{ar}(\Rightarrow) = 2$. Llamaremos *álgebra de proposiciones* a cualquier T-álgebra.

Definición 3.1.2. Sea X un conjunto y $P(X)$ la T-álgebra libre sobre X. X es un conjunto de *variables proposicionales* y llamamos a $P(X)$ el *álgebra de proposiciones del cálculo de proposiciones*.

Ejemplo 3.1.3. El álgebra $\mathbb{Z}_2 = \{0, 1\}$ (enteros módulo 2), donde

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

es un álgebra de proposiciones definiendo $F_{\mathbb{Z}_2} = 0$ y $m \Rightarrow n = 1 + m(1 + n)$.

En cualquier álgebra de proposiciones se introducen operaciones adicionales $\sim$, $\vee$, $\wedge$, $\Leftrightarrow$, poniendo

$$\begin{aligned}
\sim p &= p \Rightarrow F \\
p \vee q &= (\sim p) \Rightarrow q = (p \Rightarrow F) \Rightarrow q \\
p \wedge q &= \sim (\sim p \vee \sim q) = [((p \Rightarrow F) \Rightarrow F) \Rightarrow (q \Rightarrow F)] \Rightarrow F \\
p \Leftrightarrow q &= (p \Rightarrow q) \wedge (q \Rightarrow p) = [(((p \Rightarrow q) \Rightarrow F) \Rightarrow F) \Rightarrow ((q \Rightarrow p) \Rightarrow F)] \Rightarrow F.
\end{aligned}$$

Ejemplo 3.1.4. Las definiciones de $\sim$, $\vee$, $\wedge$, $\Leftrightarrow$ dadas arriba están de acuerdo con su uso habitual. Veamos:

p	$\sim p$	$p \Rightarrow F$
V	F	F
F	V	V

p	q	$\sim p$	$p \vee q$	$(\sim p) \Rightarrow q$
V	V	F	V	V
V	F	F	V	V
F	V	V	V	V
F	F	V	F	F

p	q	$p \wedge q$	$\sim$	$(\sim p$	$\vee$	$\sim q)$
V	V	V	V	F	F	F
V	F	F	F	F	V	V
F	V	F	F	V	V	F
F	F	F	F	V	V	V

p	q	$p \Leftrightarrow q$	$(p \Rightarrow q)$	$\wedge$	$(q \Rightarrow p)$
V	V	V	V	V	V
V	F	F	F	F	V
F	V	F	V	F	F
F	F	V	V	V	V

Ejemplo 3.1.5. Expresemos $\sim$, $\vee$, $\wedge$, y $\Leftrightarrow$ en $\mathbb{Z}_2$ en términos de suma y producto. Sean m y n en $\mathbb{Z}_2$, entonces

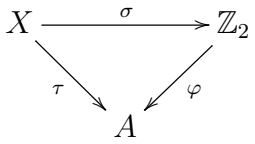
$$\sim m = \sim m \Rightarrow F = m \Rightarrow 0 = 1 + m(1+0) = 1 + m$$

$$\begin{aligned} m \vee n &= (\sim m) \Rightarrow n = (1+m) \Rightarrow n = 1 + (1+m)(1+n) \\ &= 1 + 1 + m + n + mn = (m+n) + (mn) = m(1+n) + n \\ &= n + m(1+n) \end{aligned}$$

$$\begin{aligned} m \wedge n &= \sim (\sim m \vee \sim n) = \sim ((1+m) \vee (1+n)) = 1 + [(1+m) \vee (1+n)] \\ &= 1 + [1 + (1 + (1+m))(1 + (1+n))] = 1 + 1 + (1 + 1 + m)(1 + 1 + n) \\ &= 0 + (0+m)(0+n) \\ &= m \cdot n \end{aligned}$$

$$\begin{aligned} m \Leftrightarrow n &= (m \Rightarrow n) \wedge (n \Rightarrow m) = (m \Rightarrow n)(n \Rightarrow m) \\ &= (1 + m(1+n))(1 + n(1+m)) \\ &= 1 + m(1+n) + n(1+m) + mn(1+n)(1+m) \\ &= 1 + m + nm + n + nm + mn(1 + n + m + mn) \\ &= 1 + m + n + mn + mnn + mmn + mmnn \\ &= 1 + m + n + mn + mn + mn + mn \\ &= 1 + m + n \end{aligned}$$

Ejemplo 3.1.6. Sea $X = \{0, 1\}$ y $\sigma \colon x \to \mathbb{Z}_2$ dada por $m \mapsto m$



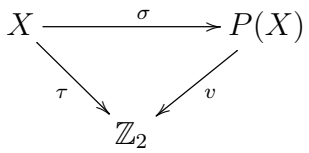
existe un único homomorfismo $\varphi \colon \mathbb{Z}_2 \to A$ dado por $m \mapsto \tau(m)$, entonces $\varphi \circ \sigma = \varphi = \tau$. Por lo tanto, $\mathbb{Z}_2$ es una T-álgebra libre sobre X.

3.2. Verdad en el Cálculo de Proposiciones

Definición 3.2.1. Una *valuación* de $P(X)$ es un homomorfismo de álgebras de proposiciones $v \colon P(X) \to \mathbb{Z}_2$. Diremos que $p \in P(X)$ es *verdadera respecto de* v si $v(p) = 1$, y que p es *falsa respecto de* v si $v(p) = 0$.

Observación. Sea X un conjunto y supongamos que $\tau \colon X \to \mathbb{Z}_2$ está dada por $x \mapsto$

$\tau(x)$. Si $\sigma\colon x \mapsto x$



existe una única $v\colon P(X) \to \mathbb{Z}_2$ determinada unívocamente tal que $v \circ \sigma = \tau$.

Definición 3.2.2. Sea $A \subset P(X)$ y $q \in P(X)$. Diremos que q es una *consecuencia* del conjunto A de hipótesis, o que A *implica semánticamente* q, si $v(q) = 1$ para toda valuación v tal que $v(p) = 1$ para todo $p \in A$. Escribiremos $A \vDash q$, y el conjunto de todas las consecuencias de A lo denotaremos por

$$\mathrm{Con}(A) = \{p \in P(X) : A \vDash p\}.$$

Definición 3.2.3. Sea $p \in P(X)$. Diremos que p es *válida*, o que es una *tautología*, si $v(p) = 1$ para toda valuación v de $P(X)$.

Observación. Entonces $p \in P(X)$ es una tautología si $\emptyset \vDash p$. Escribiremos simplemente $\vDash p$.

Ejemplo 3.2.4. Tenemos que $\{q\} \vDash p \Rightarrow q$, pues si v es una valuación tal que $v(q) = 1$, entonces

$$v(p \Rightarrow q) = v(p) \Rightarrow v(q) = v(p) \Rightarrow 1 = 1 + v(p)(1 + 1) = 1.$$

Ejemplo 3.2.5. Por otro lado, tenemos que $\vDash p \Rightarrow p$, pues si v es una valuación, entonces

$$v(p \Rightarrow p) = v(p) \Rightarrow v(p) = 1 + v(p)(1 + v(p)) = 1.$$

Ejemplo 3.2.6. Ahora mostramos que $F \vDash p$ para todo $p \in P(X)$. Si v es una valuación de $P(X)$, $v(F) = 1$ contradice $v(p) = 1$ para todo $p \in P(X)$.

Ejemplo 3.2.7. Demostremos que $\{p, p \Rightarrow q\} \vDash q$ y que $\{p, \sim q \Rightarrow \sim p\} \vDash q$ para todo $p, q \in P(X)$. Si $v(p) = 1$, entonces

$$1 = v(p \Rightarrow q) = v(p) \Rightarrow v(q) = 1 + v(p)(1 + v(q)) = 1 + (1 + v(q)) = v(q),$$

por lo tanto $\{p, p \Rightarrow q\} \vDash q$. Por otro lado, si $v(p) = 1$, entonces

$$\begin{aligned}
1 &= v(\sim q \Rightarrow \sim p) = v(\sim q) \Rightarrow v(\sim p) = v(q \Rightarrow F) \Rightarrow v(p \Rightarrow F) \\
&= (v(q) \Rightarrow v(F)) \Rightarrow (v(p) \Rightarrow v(F)) = (v(q) \Rightarrow 0) \Rightarrow (v(p) \Rightarrow 0) \\
&= [1 + v(q)(1 + 0)] \Rightarrow [1 + v(p)(1 + 0)] = [1 + v(q)] \Rightarrow [1 + v(p)] \\
&= 1 + (1 + v(q))(1 + 1 + v(p)) = 1 + (1 + v(q))v(p) = 1 + 1 + v(q) \\
&= v(q),
\end{aligned}$$

y por lo tanto $\{p, \sim q \Rightarrow \sim p\} \vDash q$.

Ejemplo 3.2.8. Sea $v\colon P(X) \to \mathbb{Z}_2$ una valuación, entonces

$$\begin{aligned}
v(p \Rightarrow (q \Rightarrow p)) = v(p) \Rightarrow (v(q) \Rightarrow v(p)) &= v(p) \Rightarrow [1 + v(q)(1 + v(p))] \\
&= 1 + v(p)[1 + 1 + (v(q)(1 + v(p))] \\
&= 1 + v(p)v(q)(1 + v(p)) = 1;
\end{aligned}$$

por otro lado

$$\begin{aligned}
v(p \Rightarrow (q \Rightarrow r) \Rightarrow [(p \Rightarrow q) \Rightarrow (p \Rightarrow r)]) &= \\
&= [v(p) \Rightarrow (v(q) \Rightarrow v(r)] \Rightarrow [[v(p) \Rightarrow v(q)] \Rightarrow [v(p) \Rightarrow v(r)]] \\
&= [v(p) \Rightarrow [1 + v(q)(1 + v(r))]] \Rightarrow [[1 + v(p)(1 + v(q))] \Rightarrow \\
&\qquad [1 + v(p)(1 + v(r))]] \\
&= [1 + v(p)[v(q)(1 + v(r))]] \Rightarrow [1 + [1 + v(p)(1 + v(q))][v(p)(1 + v(r))]] \\
&= [1 + v(p)v(q)(1 + v(r))] \Rightarrow [1 + [1 + v(p) + v(p)v(q)][v(p)(1 + v(r))]] \\
&= [1 + v(p)v(q) + v(p)v(q)v(r)] \Rightarrow [1 + v(p)(1 + v(r)) \\
&\qquad + v(p)v(p)(1 + v(r)) + v(p)v(p)v(q)(1 + v(r))] \\
&= [1 + v(p)v(q) + v(p)v(q)v(r)] \Rightarrow [1 + v(p)v(q)(1 + v(r))] \\
&= [1 + v(p)v(q) + v(p)v(q)v(r)] \Rightarrow [1 + v(p)v(q) + v(p)v(q)v(r)] = 1
\end{aligned}$$

finalmente

$$\begin{aligned} v(\sim\sim p \Rightarrow p) &= v(\sim\sim p) \Rightarrow v(p) = [1 + v(\sim p)] \Rightarrow v(p) \\ &= [1 + 1 + v(p)] \Rightarrow v(p) = v(p) \Rightarrow v(p) = 1. \end{aligned}$$

Así $p \Rightarrow (q \Rightarrow p)$, $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$ y $\sim\sim p \Rightarrow p$ son tautologías cualesquiera que sean $p, q, r \in P(X)$.

Lema 3.2.9. Con *es una operación de clausura en* $P(X)$*, esto es, tiene las siguientes propiedades:*

(i) $A \subset \mathrm{Con}(A)$.

(ii) *Si* $A_1 \subset A_2$ *entonces* $\mathrm{Con}(A_1) \subset \mathrm{Con}(A_2)$.

(iii) $\mathrm{Con}(\mathrm{Con}(A)) = \mathrm{Con}(A)$.

Demostración. (i) Para todo $a \in A$, $v(a) = 1$ implica $v(a) = 1$, luego $A \vDash a$.

(ii) Supongamos que $q \in \mathrm{Con}(A)$ y sea v una valuación tal que $v(A_2) \subset \{1\}$. Entonces $v(A_1) \subset \{1\}$ y por lo tanto $v(q) = 1$ pues $q \in \mathrm{Con}(A_1)$. Es decir, $q \in \mathrm{Con}(A_2)$.

(iii) Supongamos que $q \in \mathrm{Con}(\mathrm{Con}(A))$ y sea v una valuación tal que $v(A) \subset \{1\}$. Si $p \in \mathrm{Con}(A)$ entonces $v(p) = 1$ por definición de $\mathrm{Con}(A)$. Así que $v(\mathrm{Con}(A)) \subset \{1\}$ y, por tanto, $v(q) = 1$. Es decir, $q \in \mathrm{Con}(A)$. □

3.3. Demostraciones en el Cálculo de Proposiciones

Para el cálculo de proposiciones sobre un conjunto X tomamos como axiomas los elementos del subconjunto $\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3$ de $P(X)$ donde

$$\begin{aligned} \mathcal{A}_1 &= \{p \Rightarrow (q \Rightarrow p) : p, q \in P(X)\}, \\ \mathcal{A}_2 &= \{(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r)) : p, q, r \in P(X)\}, \\ \mathcal{A}_3 &= \{\sim\sim p \Rightarrow p : p \in P(X)\}. \end{aligned}$$

Definición 3.3.1. Sea $q \in P(X)$ y sea $A \subset P(X)$. En el cálculo de proposiciones sobre el conjunto X, una *demostración de q a partir de las hipótesis A* es una sucesión finita $p_1, p_2, \ldots, p_n$ de elementos de $P(X)$ tales que $p_n = q$ y, para todo i, o bien $p_i \in \mathcal{A} \cup A$, o existen $j, k < i$ tales que $p_k = (p_j \Rightarrow p_i)$.

Definición 3.3.2. Sea $q \in P(X)$ y $A \subset P(X)$. Se dice que q es *deducible* de A, o que q es *demostrable* a partir de A, o que A *implica sintácticamente* q, si existe una demostración de q a partir de A. Escribiremos $A \vdash q$ y el conjunto de todas las proposiciones deducibles a partir de A será denotado por:

$$\mathrm{Ded}(A) = \{q \in P(X) : A \vdash q\}.$$

Definición 3.3.3. Sea $p \in P(X)$. Diremos que p es un *teorema* del cálculo proposicional sobre X si existe una demostración de p a partir de $\emptyset$.

Así que p es un teorema si $\emptyset \vdash p$, lo que escribiremos abreviadamente $\vdash p$.

Lema 3.3.4. (i) *Si $q \in \mathrm{Ded}(A)$, entonces existe $A' \subset A$ finito tal que $q \in \mathrm{Ded}(A')$.*

(ii) Ded *es una operación de clausura en $P(X)$.*

Demostración. (i) Supongamos que $q \in \mathrm{Ded}(A)$, entonces tenemos que $A \vdash a$, es decir, existe $\{p_1, \ldots, p_n\} \subset P(X)$ una demostración de q a partir de A. Pongamos $D_{q,n} = \{p_1, \ldots, p_n\}$, con $\#D_{q,n} = n - 1$. Sea $p_i \in D_{q,n} \setminus \{q\}$, entonces $p_i \in \mathcal{A} \cup A$ o existen $j, k < i$ tales que $p_k = (p_j \Rightarrow p_i)$. Entonces existe $\{p_1, \ldots, p_n\} \subset P(X)$ tal que $p_n = q$ donde $p_i \in \mathcal{A} \cup (A \cap D_{q,n})$ o existen $j, k < i$ tales que $p_k = (p_j \Rightarrow p_i)$, por lo tanto $q \in \mathrm{Ded}(A \cap D_{q,n})$ y $\#(A \cap D_{q,n}) \leq \#D_{q,n} < \aleph_0$.

(ii) (a) $A \subset \mathrm{Ded}(A)$, pues si $p \in A$, $\{p\}$ es demostración de p a partir de A, entonces $p \in \mathrm{Ded}(A)$.

(b) Si $A_1 \subset A_2$ entonces $\mathrm{Ded}(A_1) \subset \mathrm{Ded}(A_2)$. En efecto, sea $q \in \mathrm{Ded}(A_1)$ de donde $A_1 \vdash q$, entonces existe $D_{q,n}$ una demostración de q a partir de A tal que $q = p_n$ y $p_i \in \mathcal{A} \cup A_1$ o existen $j, k < i$ tales que $p_k = (p_j \Rightarrow p_i)$. Entonces existe $D_{q,n}$ tal que $q = p_n$ y $p_i \in \mathcal{A} \cup A_2$ o existen $j, k < i$ tales que $p_k = (p_j \Rightarrow p_i)$ lo que implica $A_2 \vdash q$, es decir, $q \in \mathrm{Ded}(A_2)$.

(c) Veamos que $\mathrm{Ded}(\mathrm{Ded}(A)) = \mathrm{Ded}(A)$. Sea $q \in \mathrm{Ded}(\mathrm{Ded}(A))$ entonces existe $\{p_1, \ldots, p_n\} \subset P(X)$ una demostración de q a partir de $\mathrm{Ded}(A)$. Supongamos que $\{p_{i_1}, \ldots, p_{i_r}\} = \{p_1 \ldots, p_n\} \cap \mathrm{Ded}(A)$. Luego para todo $j \in \{1, 2, \ldots, r\}$ existe $\{p_{i_j,1}, p_{i_j,2}, \ldots, p_{i_j,r_j}\}$ demostración de p_{i_j} a partir de A, es decir, $p_{i_j,r_j} = p_{i_j}$ y $p_{i_j,k} \in \mathcal{A} \cup A$ o existen $\ell, m < k$ tales que $p_{i_j,m} = (p_{i_j,\ell} \Rightarrow p_{i_j,k})$. Substituimos p_{i_j} por $\{p_{i_j,1}, p_{i_j,2}, \ldots, p_{i_j,r_j}\}$, entonces existe $\{p_1, \ldots, p_n\} \subset P(X)$ una demostración de q a partir de A. □

Ejemplo 3.3.5. $\vdash p \Rightarrow p$. En efecto, para todo $p \in P(X)$

$$
\begin{aligned}
p_1 &= p \Rightarrow ((p \Rightarrow p) \Rightarrow p) && (\mathcal{A}_1)\\
p_2 &= (p \Rightarrow ((p \Rightarrow p) \Rightarrow p)) \Rightarrow ((p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p)) && (\mathcal{A}_2)\\
p_3 &= (p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p) && (p_2 = p_1 \Rightarrow p_3)\\
p_4 &= p \Rightarrow (p \Rightarrow p) && (\mathcal{A}_1)\\
p_5 &= p \Rightarrow p && (p_3 = p_4 \Rightarrow p_5),
\end{aligned}
$$

entonces $\{p_1, p_2, p_3, p_4, p_5\}$ es una demostración de $p \Rightarrow p$.

Ejemplo 3.3.6. $\{q\} \vdash p \Rightarrow q$. En efecto,

$$
\begin{aligned}
p_1 &= q \Rightarrow (p \Rightarrow q) && (\mathcal{A}_1)\\
p_2 &= q && (q \in \{q\})\\
p_3 &= p \Rightarrow q && (p_1 = p_2 \Rightarrow p_3).
\end{aligned}
$$

Ejemplo 3.3.7. $\vdash F \Rightarrow q$. Para todo $q \in P(X)$, la siguiente sucesión es una demos-

tración:

$$p_1 = (\sim\sim q \Rightarrow q) \Rightarrow (F \Rightarrow (\sim\sim q \Rightarrow q)) \qquad (\mathcal{A}_1)$$

$$p_2 = \sim\sim q \Rightarrow q \qquad (\mathcal{A}_3)$$

$$p_3 = F \Rightarrow (\sim\sim q \Rightarrow q) \qquad (p_1 = p_2 \Rightarrow p_3)$$

$$p_4 = [F \Rightarrow (\sim\sim q \Rightarrow q)] \Rightarrow [(F \Rightarrow \sim\sim q) \Rightarrow (F \Rightarrow q)] \qquad (\mathcal{A}_2)$$

$$p_5 = (F \Rightarrow \sim\sim q) \Rightarrow (F \Rightarrow q) \qquad (p_4 = p_3 \Rightarrow p_5)$$

$$p_6 = F \Rightarrow (\sim q \Rightarrow F) = F \Rightarrow \sim\sim q \qquad (\mathcal{A}_1, \text{definici\"{i}}\frac{1}{2} \text{ de } \sim)$$

$$p_7 = F \Rightarrow q \qquad (p_5 = p_6 \Rightarrow p_7).$$

Ejemplo 3.3.8. $\vdash \sim p \Rightarrow (p \Rightarrow q)$. Tomando la sucesión $p_1, \ldots, p_7$ del Ejemplo 3.3.7 seguida por

$$p_8 = (F \Rightarrow q) \Rightarrow (p \Rightarrow (F \Rightarrow q)) \qquad (\mathcal{A}_1)$$

$$p_9 = p \Rightarrow (F \Rightarrow q) \qquad (p_8 = p_7 \Rightarrow p_9)$$

$$p_{10} = [p \Rightarrow (F \Rightarrow q)] \Rightarrow [(p \Rightarrow F) \Rightarrow (p \Rightarrow q)] \qquad (\mathcal{A}_2)$$

$$p_{11} = (p \Rightarrow F) \Rightarrow (p \Rightarrow q) = \sim p \Rightarrow (p \Rightarrow q) \qquad (p_{10} = p_9 \Rightarrow p_{11}, \text{definici\"{i}}\frac{1}{2} \text{ de } \sim)$$

obtenemos una demostración de $\sim p \Rightarrow (p \Rightarrow q)$.

Observación. Como $\vdash F \Rightarrow q$ entonces $\{F \Rightarrow q\} \vdash \sim p \Rightarrow (p \Rightarrow q)$. Luego $\sim p \Rightarrow (p \Rightarrow q) \in \text{Ded}(\{F \Rightarrow q\}) \subset \text{Ded}(\text{Ded}(\emptyset)) = \text{Ded}(\emptyset)$ de donde $\vdash \sim p \Rightarrow (p \Rightarrow q)$.

Esta es una demostración de la existencia de una demostración en el cálculo proposicional, pero no es una demostración en el cálculo proposicional.

Ejemplo 3.3.9. Sea $D \subset P(X)$ tal que $A \cup \mathcal{A} \subset D$ y $p, p \Rightarrow q \in D$ implica que $q \in D$, entonces $\text{Ded}(A) \subset D$. En efecto, supongamos que $(p_i)_{i=1}^n \in \text{Ded}(A)$, entonces para todo $i = 1, \ldots, n$ $p_i \in A \cup \mathcal{A}$ o existen $j, k < i$ tales que $p_j = p_k \Rightarrow p_i$. Si $q \in A$ y $q' \in \mathcal{A}$, entonces $\{q\} \in \text{Ded}(A)$ y $\{q'\} \subset \text{Ded}(A)$, es decir, $A \vdash q$ y $A \vdash q'$, por lo tanto $A \cup \mathcal{A} \subset \text{Ded}(A)$.

Supongamos que $p, p \Rightarrow q \in \mathrm{Ded}(A)$. Si suponemos que $q \in A \cup \mathcal{A}$, entonces $q \in \mathrm{Ded}(A)$. Si $q \notin A \cup \mathcal{A}$, entonces existen $(p_i)_{i=1}^n$ una deducción de p y $(q_i)_{i=1}^m$ una deducción de $p \Rightarrow q$, donde $p_n = p$ y $q_m = p \Rightarrow q$; por lo tanto

$$(p_1, p_2, \ldots, p_n, q_1, q_2, \ldots, q_m, q) \in \mathrm{Ded}(A)$$

es una deducción de q con $q_m = p_n \Rightarrow q$.

Ejemplo 3.3.10. Sea $A = \{p \Rightarrow q, q \Rightarrow r\}$, la siguiente sucesión es una demostración de $p \Rightarrow r$:

$$\begin{aligned}
p_1 &= [p \Rightarrow (q \Rightarrow r)] \Rightarrow [(p \Rightarrow q) \Rightarrow (p \Rightarrow r)] && (\mathcal{A}_2)\\
p_2 &= (q \Rightarrow r) \Rightarrow [p \Rightarrow (q \Rightarrow r)] && (\mathcal{A}_1)\\
p_3 &= q \Rightarrow r && (A)\\
p_4 &= p \Rightarrow (q \Rightarrow r) && (p_2 = p_3 \Rightarrow p_4)\\
p_5 &= (p \Rightarrow q) \Rightarrow (p \Rightarrow r) && (p_1 = p_4 \Rightarrow p_5)\\
p_6 &= p \Rightarrow q && (A)\\
p_7 &= p \Rightarrow r && (p_5 = p_6 \Rightarrow p_7).
\end{aligned}$$

Teorema 3.3.11 (Teorema de Sustitución)**.** *Sean X, Y conjuntos y $\varphi\colon P(X) \to P(Y)$ un homomorfismo del álgebra de proposiciones (libre) sobre X en el álgebra de proposiciones (libre) sobre Y. Sea $w = w(x_1, \ldots, x_n) \in P(X)$ y $A \subset P(X)$. Pongamos $a_i = \varphi(x_i)$.*

(a) *Si $A \vdash w$, entonces $\varphi(A) \vdash w(a_1, \ldots, a_n)$.*

(b) *Si $A \vDash w$, entonces $\varphi(A) \vDash w(a_1, \ldots, a_n)$.*

Demostración. (a) Supongamos que $p_1, \ldots, p_r$ es una demostración de w en $P(X)$ a partir de A. Si $p_i \in A$ entonces $\varphi(p_i) \in \varphi(A)$. Luego, como φ es un homomorfismo, si $p_i \in \mathcal{A}_X$, entonces $\varphi(p_i) \in \mathcal{A}_Y$. Por la misma razón, si $k, j < i$ tales que $p_k = (p_j \Rightarrow p_i)$, entonces $\varphi(p_k) = \varphi(p_j) \Rightarrow \varphi(p_i)$. Así $\varphi(p_1), \ldots, \varphi(p_r)$ es una demostración

de $\varphi(w)$ en $P(Y)$ a partir de $\varphi(A)$. Como $\varphi(w) = w(a_1, \ldots, a_n)$, el resultado queda probado.

(b) Supongamos que $A \vDash w$. Sea $v\colon P(Y) \to \mathbb{Z}_2$ una valuación de $P(Y)$ tal que $v(\varphi(A)) \subset \{1\}$. Entonces $v \circ \varphi\colon P(X) \to \mathbb{Z}_2$ es una valuación de $P(X)$ tal que $(v \circ \varphi)(A) \subset \{1\}$. Como $A \vDash w$, tendremos que $v \circ \varphi(w) = 1$, es decir, que $v(\varphi(w)) = 1$. O sea, $\varphi(A) \vDash \varphi(w)$. □

Capítulo 4

Propiedades del Cálculo de Proposiciones

4.1. Introducción

Definición 4.1.1. Una *lógica* $\mathcal{L}$ es un sistema $\mathcal{L} = (P, \mathcal{V}, \mathcal{D})$ que consiste en un conjunto P (de proposiciones), un conjunto

$$\mathcal{V} = \{v\colon P \to W : v \text{ es una valuación}\}$$

(W conjunto de valores), y para cada $A \subset P$, un conjunto

$$\mathcal{D} = \{\{p_1, \ldots, p_n\}_A \subset P : n \in \mathbb{N}\},$$

donde $\{p_1, \ldots, p_n\}_A$ es una deducción de $p_n \in P$ a partir de $A \subset P$.

Ejemplo 4.1.2. La lógica del cálculo proposicional sobre un conjunto X, que de ahora en adelante denotaremos por $\mathrm{Prop}(X)$, es el sistema $\mathrm{Prop}(X) = (P(X), \mathcal{V}, \mathcal{D})$, donde

$$\mathcal{V} = \{v\colon P(X) \to \mathbb{Z}_2 : v \text{ valuación}\}$$
$$\mathcal{D} = \{\{p_1, \ldots, p_n\}_{\mathcal{A}} \subset P(X) : n \in \mathbb{N}, \mathcal{A} \subset P\}$$

conjunto de deducciones en $P(X)$ a partir de los axiomas $\mathcal{A}$.

Observación. Sean $w_0 \in W$, $A \subset P$, $q \in P$ y $\mathcal{L} = (P, \mathcal{V}, \mathcal{D})$ una lógica. Si para toda $v \in \mathcal{V}$ y todo $p \in A$ se tiene que $v(p) = w_0$ implica que $v(q) = w_0$ entonces decimos que "p es una consecuencia de A" y lo denotamos por $A \vDash q$; en particular, si $\emptyset \vDash p$ entonces p es una *tautología* en $\mathcal{L}$. Si existe $(d_i)_{i=1}^n \in \mathcal{D}$ con $d_n = q$, decimos que "q se puede deducir a partir de A" y lo denotamos por $A \vdash q$; en particular, si $\emptyset \vdash q$ entonces q es un *teorema* en $\mathcal{L}$.

Definición 4.1.3. Una lógica $\mathcal{L}$ se llama *coherente* si $A \vdash p$ implica que $A \vDash p$, para todo $A \subset P$ y $p \in P$.

Definición 4.1.4. Una lógica $\mathcal{L}$ se llama *consistente* si $A \nvdash F$, para todo $A \subset P$.

Definición 4.1.5. Una lógica $\mathcal{L}$ se llama *adecuada* si $A \vDash p$ implica que $A \vdash p$, para todo $A \subset P$ y $p \in P$.

Observación. Si $A = \emptyset$ y $\mathcal{L}$ es una lógica coherente, p teorema implica p válido. Y si $\mathcal{L}$ es adecuada, p válido implica p teorema.

Definición 4.1.6. Diremos que la lógica $\mathcal{L}$ es *decidible en validez* si existe un algoritmo que determina, para cada proposición p, y en un número finito de pasos, si p es o no es válida.

Definición 4.1.7. Una la lógica $\mathcal{L}$ es *decidible en deductibilidad* si existe un algoritmo que determina, para cada proposición p, y en un número finito de pasos, si p es o no es un teorema.

4.2. Coherencia y Adecuación de $\mathrm{Prop}(X)$

Teorema 4.2.1 (Teorema de Coherencia)**.** *Sea $A \subset P(X)$ y $p \in P(X)$. Si $A \vdash p$ entonces $A \vDash p$.*

Demostración. Supongamos que existe $\{p_1, \ldots, p_n\}_A \in \mathcal{D}$, con $p_n = p$. Sea $v\colon P(X) \to \mathbb{Z}_2$ una valuación tal que $v(A) \subset \{1\}$. Procedemos por inducción sobre n, la longitud

de la demostración de p. Supongamos que $n = 1$, entonces $p \in A \cup \mathcal{A}$, de donde $v(p) = 1$.

Ahora supongamos que $n > 1$ y que $v(q) = 1$ para todo $q \in P$ tal que $A \vdash q$ y $\#\mathcal{D}(q) < n$. Entonces tendremos $v(p_1) = v(p_2) = \cdots = v(p_{n-1}) = 1$. Por otra parte, o bien $p_n \in A \cup \mathcal{A}$ lo que implica que $v(p_n) = 1$, o bien existen $i, j < n$ tales que $p_i = p_j \Rightarrow p_n$ lo que implica que

$$v(p_i) = v(p_j) \Rightarrow v(p_n) = 1 + v(p_j)(1 + v(p_n)) = 1$$

y esto implica que $v(p_j)(1+v(p_n)) = 0$ de donde $1+v(p_n) = 0$ por lo que, finalmente, $v(p_n) = 1$. □

Corolario 4.2.2 (Teorema de Consistencia)**.** $\nvdash F$ *en* $\mathrm{Prop}(X)$.

Demostración. Supongamos que $\vdash F$, entonces $\vDash F$ por el Teorema de Coherencia. Como los axiomas son tautologías, $v(F) = 1$ para toda $v \in \mathcal{V}$, esto implica que $\mathcal{V} = \emptyset$. Pero si $X \to \mathbb{Z}_2$ es una aplicación con $X \neq \emptyset$, entonces existe un homomorfismo $v\colon P(X) \to \mathbb{Z}_2$ (valuación) pues $P(X)$ es libre sobre X. □

Ejemplo 4.2.3. Supongamos que $p, p \Rightarrow q \in \mathrm{Con}(A)$, mostraremos que $q \in \mathrm{Con}(A)$. Como $A \vDash p$ y $A \vDash p \Rightarrow q$, sea $v \in \mathcal{V}$ tal que para todo $a \in A$ $v(a) = 1$, $v(p) = 1$, y $v(p \Rightarrow q) = 1$ luego $1 = v(p) \Rightarrow v(q)$ lo que implica que

$$1 = 1 + v(p)(1 + v(q)) = 1 + (1 + v(q))$$

de donde $0 = 1 + v(q)$ luego $v(q) = 1$, así $A \vdash q$. Si $A \subset \mathrm{Con}(A)$ y $\mathcal{A} \subset \mathrm{Con}(A)$, entonces $A \cup \mathcal{A} \subset \mathrm{Con}(A)$. Si ponemos

$$\mathcal{D} = \{D \subset P(X) : A \cup \mathcal{A} \subset D, p, p \Rightarrow q \in D\}$$

entonces $\mathrm{Ded}(A) \in \mathcal{D}$, $\mathrm{Con}(A) \in \mathcal{D}$, luego para todo $D \in \mathcal{D}$, $\mathrm{Ded}(A) \subset D$ implica $\mathrm{Ded}(A) \subset \mathrm{Con}(A)$.

Teorema 4.2.4 (Teorema de Deducción)**.** *Sea* $A \subset P(X)$ *y* $p, q \in P(X)$. *Entonces* $A \vdash p \Rightarrow q$ *si y sólo si* $A \cup \{p\} \vdash q$.

Demostración. (a) Supongamos que $A \vdash p \Rightarrow q$. Entonces existe $(q_i)_{i=1}^n \in \mathrm{Ded}(A)$ tal que $q_n = p \Rightarrow q$. Luego $(q_1, \ldots, q_n, p, q) \in \mathrm{Ded}(A \cup \{p\})$ con $p \in A \cup \{p\}$ y $q_n = p \Rightarrow q$, por lo tanto, $A \cup \{p\} \vdash q$.

(b) Supongamos que $A \cup \{p\} \vdash q$ entonces existe $(p_i)_{i=1}^n \in \mathrm{Ded}(A \cup \{p\})$ con $p_n = q$. Por inducción sobre n, la longitud de la demostración.

Si $n = 1$, entonces $q \in \mathcal{A} \cup A \cup \{p\}$, es decir $q \in \mathcal{A} \cup A$ entonces $(q, q \Rightarrow (p \Rightarrow q), p \Rightarrow q) \in \mathrm{Ded}(A)$, es decir, $A \vdash p \Rightarrow q$; si $q = p$, entonces $\vdash p \Rightarrow p$.

Supongamos ahora que $n > 1$. Por inducción $A \vdash p \Rightarrow p_i$ para $i = 1, \ldots, n-1$. Podemos suponer que $q \notin \mathcal{A} \cup A \cup \{p\}$, entonces existen $i, j < n$ tales que $p_i = p_j \Rightarrow q$. Supongamos que (por hipótesis de inducción) $A \vdash p \Rightarrow p_j$ y que $A \vdash p \Rightarrow (p_j \Rightarrow q)$, entonces existe una deducción $q_1, q_2, \ldots, q_k, q_{k+1}$ a partir de A tal que

$$q_k = p \Rightarrow p_j$$
$$q_{k+1} = p \Rightarrow (p_j \Rightarrow q).$$

Pongamos

$$q_{k+2} = (p \Rightarrow (p_j \Rightarrow q)) \Rightarrow ((p \Rightarrow p_j) \Rightarrow (p \Rightarrow q)) \qquad (\mathcal{A}_2)$$
$$q_{k+3} = (p \Rightarrow p_j) \Rightarrow (p \Rightarrow q) \qquad (q_{k+2} = q_{k+1} \Rightarrow q_{k+3})$$
$$q_{k+4} = p \Rightarrow q \qquad (q_{k+3} = q_k \Rightarrow q_{k+4})$$

entonces $q_1, \ldots, q_k, \ldots, q_{k+4}$ es una demostración de $p \Rightarrow q$ a partir de A. □

Ejemplo 4.2.5. Vamos a probar que $\{p \Rightarrow q, q \Rightarrow r\} \vdash p \Rightarrow r$. Primero vemos que $\{p, p \Rightarrow q, q \Rightarrow r\} \vdash r$: he aquí una demostración p, $p \Rightarrow q$, q, $q \Rightarrow r$, r. Finalmente, del Teorema de Deducción resulta que $\{p \Rightarrow q, q \Rightarrow r\} \vdash p \Rightarrow r$.

Ejemplo 4.2.6. Probaremos que $p \Rightarrow r \in \mathrm{Ded}(\{p \Rightarrow q, p \Rightarrow (q \Rightarrow r)\})$. La sucesión p, $q \Rightarrow r$, $p \Rightarrow q$, r es una demostración de r, entonces $\{p, p \Rightarrow q, p \Rightarrow (q \Rightarrow r)\} \vdash r$, de donde, por el Teorema de Deducción, $\{p \Rightarrow q, p \Rightarrow (q \Rightarrow r)\} \vdash p \Rightarrow r$. De otra

forma:

$$(p \Rightarrow (q \Rightarrow r)) \Rightarrow [(p \Rightarrow q) \Rightarrow (p \Rightarrow r)] \qquad (\mathcal{A}_2)$$

$$(p \Rightarrow q) \Rightarrow (p \Rightarrow r) \qquad \text{(MP)}$$

$$p \Rightarrow r \qquad \text{(MP)}$$

Así si $p \Rightarrow q, p \Rightarrow (q \Rightarrow r) \in \text{Ded}(A)$ entonces $p \Rightarrow r \in \text{Ded}(A)$.

Ejemplo 4.2.7. Tenemos que $\vdash p \Rightarrow \sim\sim p$ pues $\{p, \sim p\} \vdash F$ y aplicando dos veces el Teorema de Deducción, obtenemos lo propuesto.

Ejemplo 4.2.8. Las siguientes expresiones son teoremas de $\text{Prop}(X)$:

(a) $p \Rightarrow p \vee q$, (b) $q \Rightarrow p \vee q$,

(c) $(p \vee q) \Rightarrow (q \vee p)$, (d) $p \wedge q \Rightarrow p$,

(e) $p \wedge q \Rightarrow q$, (f) $(p \wedge q) \Rightarrow (q \wedge p)$.

Definición 4.2.9. Sea $A \subset P(X)$. Diremos que A es *consistente* si $F \notin \text{Ded}(A)$. Diremos que A es *consistente maximal* si A es consistente y todo subconjunto $T \subset P(X)$ que contiene propiamente a A, $A \subsetneq T$, es inconsistente.

Lema 4.2.10. *Un subconjunto $A \subset P(X)$ es consistente maximal si y sólo si:*

(i) $F \notin A$.

(ii) $A = \text{Ded}(A)$.

(iii) *Para todo $p \in P(X)$, $(p \in A) \vee (\sim p \in A)$.*

Demostración. ($\Rightarrow$) Supongamos que A es consistente maximal. Entonces $F \notin \text{Ded}(A)$, pues A es consistente, y en consecuencia $F \notin A$.

Por otra parte $\text{Ded}(A)$ es consistente, pues $\text{Ded}(\text{Ded}(A)) = \text{Ded}(A)$; como $A \subset \text{Ded}(A)$, tendremos que $A = \text{Ded}(A)$, pues A es consistente maximal.

Finalmente, si $p \notin A$, entonces $F \in \text{Ded}(A \cup \{p\})$ o, equivalentemente, $A \cup \{p\} \vdash F$. Por el Teorema de Deducción, $A \vdash p \Rightarrow F$, es decir, $\sim p \in \text{Ded}(A) = A$.

($\Leftarrow$) Supongamos que A cumple (i), (ii), y (iii). Entonces $F \notin \mathrm{Ded}(A) = A$. Si $A \subset T$ pero $A \neq T$, entonces existe $p \in T$ tal que $p \notin A$. Por (iii), $\sim p \in A$ y en consecuencia $p, \sim p \in T$, de donde $p, \sim p, F$ es una demostración de F a partir de T. Esto prueba que A es consistente maximal. □

Lema 4.2.11. *Sea $A \subset P(X)$ un subconjunto consistente. Entonces existe un subconjunto consistente maximal M tal que $A \subset M$.*

Demostración. Sea

$$\Sigma = \{T \subset P(X) : T \supset A, F \notin \mathrm{Ded}(T)\}.$$

Como $A \in \Sigma$, $\Sigma \neq \emptyset$. Supongamos que $\{T_\alpha\}$ es una familia totalmente ordenada de miembros de Σ y pongamos $T = \bigcup_\alpha T_\alpha$. Está claro que $T \subset P(X)$ y $A \subset T$. T es consistente, pues si fuera que $T \vdash F$, entonces existiría un subconjunto inconsistente T_α, lo que implica que $T_\alpha \vdash F$, esto contradice que $T_\alpha \in \Sigma$. Así que Σ es un conjunto ordenado inductivo. Por el Lema de Zorn existe M un elemento maximal en Σ tal que $M \subset P(X)$, y por tanto $A \subset M$ y $F \notin \mathrm{Ded}(M)$. □

Teorema 4.2.12 (Teorema de Satisfacibilidad)**.** *Sea $A \subset P(X)$ un subconjunto consistente. Existe una valuación $v\colon P(X) \to \mathbb{Z}_2$ tal que $v(A) \subset \{1\}$.*

Demostración. Sea $M \subset P(X)$ consistente maximal tal que $A \subset M$. Dado $p \in P(X)$ definimos v por

$$v(p) = \begin{cases} 1 & \text{si } p \in M \\ 0 & \text{si } p \notin M. \end{cases}$$

Probaremos que v es una valuación (un homomorfismo).

Está claro que $v(F) = 0$, pues $F \notin \mathrm{Ded}(M)$.

Resta probar que $v(p \Rightarrow q) = v(p) \Rightarrow v(q)$, realizaremos la prueba tomando casos para p y q.

Si $q \in M$, entonces $p \Rightarrow q \in M$ pues por $\mathcal{A}_1$ se tiene $\vdash q \Rightarrow (p \Rightarrow q)$ de donde

$\{q\} \vdash p \Rightarrow q$, entonces $p \Rightarrow q \in \mathrm{Ded}(\{q\}) \subset \mathrm{Ded}(M) = M$ pues M es consistente maximal, luego $p \Rightarrow q \in M$. Así

$$\begin{aligned} v(p \Rightarrow q) = 1 &= 1 + v(p)(0) = 1 + v(p)(1+1) \\ &= 1 + v(p)(1 + v(q)) = v(p) \Rightarrow v(q). \end{aligned}$$

Si $p \notin M$, entonces $\sim p \in M$, puesto que M es consistente maximal, además, como $\{p, \sim p\} \vdash q$ se tiene que $\{\sim p\} \vdash p \Rightarrow q$, entonces $p \Rightarrow q \in \mathrm{Ded}(\{\sim p\}) \subset \mathrm{Ded}(M) = M$ ya que M es consistente maximal. Así

$$v(p \Rightarrow q) = 1 = 1 + 0 = 1 + v(p)(1 + v(q)) = v(p) \Rightarrow v(q).$$

Si $p \in M$ y $q \notin M$, entonces $p \Rightarrow q \notin M$ (si fuera el caso que $p \Rightarrow q \in M$, se tendría que $q \in M$ que contradice $M = \mathrm{Ded}(M)$). Así

$$\begin{aligned} v(p \Rightarrow q) = 0 &= 1 + 1 = 1 + v(p)(1+0) = 1 + v(p)(1 + v(q)) \\ &= v(p) \Rightarrow v(q). \end{aligned}$$

□

Teorema 4.2.13 (Teorema de Adecuación)**.** *Sea $A \subset P(X)$ y $p \in P(X)$. Si $A \vDash p$ en* $\mathrm{Prop}(X)$*, entonces $A \vdash p$ en* $\mathrm{Prop}(X)$.

Demostración. Supongamos que $A \vDash p$. Si v es una valuación y $v(A) \subset \{1\}$, entonces $v(p) = 1$. Si $A \cup \{\sim p\}$ fuese consistente, entonces existiría una valuación $v\colon P(X) \to \mathbb{Z}_2$ tal que $v(A \cup \{\sim p\}) \subset \{1\}$ lo que implicaría que

$$1 = v(\sim p) = v(p \Rightarrow F) = v(p) \Rightarrow v(F) = 1 + v(p)(1+0) = 1 + v(p) = 0$$

lo que es una contradicción. Entonces $F \in \mathrm{Ded}(A \cup \{\sim p\})$ luego $A \cup \{\sim p\} \vdash F$ lo que implica $A \vdash \sim p \Rightarrow F$ y esto implica que $A \vdash \sim\sim p$. Si $(d_i)_{i=1,\ldots,n}^{A}$ es una deducción de $\sim\sim p$, poniendo

$$\begin{aligned} d_{n+1} &= \sim\sim p \Rightarrow p \\ d_{n+2} &= p \end{aligned}$$

tenemos que $(d_i)_{i=1,\ldots,n+2}^{A}$ es una deducción de p, entonces $A \vdash p$. □

Ejemplo 4.2.14. Si $A \vDash p$, entonces existe $A_0 \subset A$ con $\#A = \aleph_0$ tal que $A_0 \vDash p$. En efecto, si $A \vDash p$, entonces $A \vdash p$ lo que implica que existe $A_0 \subset A$ finito tal que $A_0 \vdash p$ lo que implica que $A_0 \vDash p$. (A este resultado se le conoce con el nombre de Teorema de Compacidad.)

4.3. Funciones de Verdad y Decidibilidad de $\mathrm{Prop}(X)$

Observación. Supongamos que v es una valuación de $P(X)$ y $r_v \subset P(X)^2$. Si definimos pr_vq si y sólo si $v(p) = v(q)$, r_v es una relación de equivalencia. Si pr_vp_1 y qr_vq_1, entonces $v(p) = v(p_1)$ y $v(q) = v(q_1)$, esto implica que $v(p) \Rightarrow v(q) = v(p_1) \Rightarrow v(q_1)$ lo que implica $v(p \Rightarrow q) = v(p_1 \Rightarrow q_1)$, de donde $(p \Rightarrow q)r_v(p_1 \Rightarrow q_1)$ y r_v es una relación de congruencia para toda v.

Definición 4.3.1. Si $\mathcal{V} = \{v\colon P(X) \to \mathbb{Z}_2 : v \text{ valuación}\}$ y ponemos

$$r = \bigcap_{v \in \mathcal{V}} r_v,$$

r es una relación de congruencia en $P(X)$ que llamaremos *equivalencia semántica* y la denotaremos por $\models\!\!\models$. Como $p \models\!\!\models q$ si y sólo si $v(p) = v(q)$ para toda $v \in \mathcal{V}$, entonces $p \models\!\!\models q$ si y sólo si $\{p\} \vDash q$ y $\{q\} \vDash p$.

Definición 4.3.2. El conjunto de clases de $P(X)$ respecto de la relación $\models\!\!\models$, $L(X) = P(X)/\models\!\!\models$, es la $\{F, \Rightarrow\}$-álgebra llamada *álgebra de Lindenbaum* sobre X.

Si $\overline{p}, \overline{q} \in L(X)$, entonces $\overline{p} \Rightarrow \overline{q} = \overline{p \Rightarrow q}$ pues $v \in \mathcal{V}$ es un homomorfismo.
Sea $F_0\colon \{\emptyset\} \to L(X)$ dada por $\emptyset \mapsto \overline{F}$, donde $\overline{F} = \{q \in P(X) : q \models\!\!\models F\}$ y $q \models\!\!\models F$ si y sólo si $v(q) = 0$ para toda v.
Además sea $\varphi\colon P(X) \to L(X)$ dada por $p \mapsto \overline{p}$, φ es un homomorfismo pues $\varphi(p \Rightarrow q) = \overline{p \Rightarrow q} = \overline{p} \Rightarrow \overline{q} = \varphi(p) \Rightarrow \varphi(q)$.

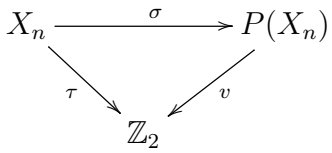
Observación. Sea $X_n = \{x_1, \ldots, x_n\}$. Si $w = w(x_1, \ldots, x_n)$ es una palabra en $P(X_n)$, entonces $\overline{w} = \overline{w}(x_1, \ldots, x_n) = \{p \in P(X_n) : p \models\!\!\models w\}$.

Observación. Sea $\overline{w}(x_1, \ldots, x_n) \in L(X_n)$, escojamos un representante $w \in \overline{w}$.

Sea $(z_1, \ldots, z_n) \in \mathbb{Z}_2^n$, esta n-upla de valores en $\mathbb{Z}_2$ define una función $\tau\colon X_n \to \mathbb{Z}_2$

tal que $\tau(x_i) = z_i$

Así existe una única valuación $v\colon P(X_n) \to \mathbb{Z}_2$ tal que $v(x_i) = \tau(x_i) = z_i$, $i = 1, \ldots, n$, pues



Definamos $\overline{w}(z_1, \ldots, z_n) = v(w(x_1, \ldots, z_n))$, que es independiente de la elección del representante w de $\overline{w}$. En efecto, si $w_1 \in \overline{w}$, entonces $w_1 \models\!\models w$ lo que implica que $v(w) = v(w_1)$ para toda valuación v, y esto implica que $\overline{w}_1 = \overline{w}$.

Podemos entonces definir

$$\overline{w}\colon \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2$$
$$(z_1, \ldots, z_n) \longmapsto v(w(x_1, \ldots, x_n)).$$

Lo anterior está bien definido pues: Supongamos que $\overline{w}(z_1, \ldots, z_n) = \overline{w}_1(z_1, \ldots, z_n)$ para todo $(z_1, \ldots, z_n) \in \mathbb{Z}_2^n$, entonces

$$\overline{w}(z_1, \ldots, z_n) = v(w) \qquad \text{con} \qquad v(x_i) = z_i$$
$$\overline{w}_1(z_1, \ldots, z_n) = v(w) \qquad \text{con} \qquad v(x_i) = z_i$$

$(i = 1, \ldots, n)$, luego $v(w) = v(w_1)$ para toda $v \in \mathcal{V}$, esto implica que $w \models\!\models w_1$ de donde $\overline{w} = \overline{w}_1$. Así

$$L(X_n) \subset \{f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2 : f \text{ función}\}.$$

Definición 4.3.3. Una función $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2$ se llama una *función de verdad.*

Teorema 4.3.4. *$L(X_n)$ es el conjunto de las funciones de verdad $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2$.*

Demostración. Como $0 = \overline{F}$ y $1 = \overline{F \Rightarrow F}$, entonces las funciones constantes $0, 1 \in L(X_n)$. Así que el resultado es cierto para $n = 0$.

Si $f, g\colon \mathbb{Z}_2^n \to \mathbb{Z}_2$ son funciones de verdad, definimos la función de verdad

$$f \Rightarrow g\colon \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2$$
$$(z_1, \ldots, z_n) \longmapsto f(z_1, \ldots, z_n) \Rightarrow g(z_1, \ldots, z_n).$$

Sea $u_i(x_1, \ldots, x_n) = x_i \in L(X_n)$ la i-ésima función de coordenadas.

Supongamos ahora que $n > 0$; vamos a completar la prueba procediendo por inducción sobre n. Sea $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2$ una función de verdad (en n variables). Pongamos

$$g(u_1, \ldots, u_{n-1}) = f(u_1, \ldots, u_{n-1}, 0)$$
$$h(u_1, \ldots, u_{n-1}) = f(u_1, \ldots, u_{n-1}, 1),$$

entonces $g, h \in L(X_{n-1}) \subset L(X_n)$. La función

$$\begin{aligned} k\colon \mathbb{Z}_2^n &\longrightarrow \mathbb{Z}_2 \\ (u_1, \ldots, u_n) &\longmapsto \big(\sim u_n \Rightarrow g(u_1, \ldots, u_{n-1})\big) \wedge \big(u_n \Rightarrow h(u_1, \ldots, u_{n-1})\big) \end{aligned}$$

pertenece a $L(X_n)$ y

$$\begin{aligned} k(u_1, \ldots, u_{n-1}, 0) &= (1 \Rightarrow g(u_1, \ldots, u_{n-1})) \wedge (0 \Rightarrow h(u_1, \ldots, u_{n-1})) \\ &= g(u_1, \ldots, u_{n-1}) \wedge 1 \\ &= g(u_1, \ldots, u_{n-1}) \\ &= f(u_1, \ldots, u_{n-1}, 0). \end{aligned}$$

De forma similar se obtiene que $k(u_1, \ldots, u_{n-1}, 1) = f(u_1, \ldots, u_{n-1}, 1)$. Entonces $k = f$ y, por tanto, $f \in L(X_n)$. □

Lema 4.3.5. *Sea $w = w(x_1, \ldots, x_n) \in P(X)$. Entonces $\vDash w$ si y sólo si su función de verdad asociada $\overline{w}\colon \mathbb{Z}_2^n \to \mathbb{Z}_2$ es la constante* 1.

Demostración. Supongamos que $\overline{w} = 1$. Sea $v\colon P(X) \to \mathbb{Z}_2$ una valuación de $P(X)$ y pongamos $a_i = v(x_i)$, entonces $v|_{P(X_n)}\colon P(X_n) \to \mathbb{Z}_2$ es una valuación de $P(X_n)$ tal que $v(w) = \overline{w}(a_1, \ldots, a_n) = 1$. Entonces $v(w) = 1$ para toda valuación v, lo que significa que $\vDash w$.

Recíprocamente, supongamos que $\vDash w$. Sea $(a_1, \ldots, a_n) \in \mathbb{Z}_2^n$. Entonces existe una valuación $v\colon P(X) \to \mathbb{Z}_2$ tal que $v(x_i) = a_i$. (Asignamos valores arbitrarios a los elementos de $X \setminus \{x_1, \ldots, x_n\}$.) De este modo $v|_{P(X_n)}\colon P(X_n) \to \mathbb{Z}_2$, la restricción

de v a $P(X_n)$, es una valuación de $P(X_n)$ tal que $\overline{w}(a_1, \ldots, a_n) = v(w) = 1$. Así que $\overline{w} = 1$. □

Teorema 4.3.6. Prop(X) *es decidible en validez.*

Demostración. Vamos a dar un algoritmo para decidir si $w \in P(X)$ es válida. El elemento w es una palabra $w(x_1, \ldots, x_n)$ en un conjunto finito $x_1, \ldots, x_n$ de variables. Sea $\overline{w} = w(u_1, \ldots, u_n)$ la función de verdad asociada a w. Para cada $(a_1, \ldots, a_n) \in \mathbb{Z}_2^n$ se puede calcular $\overline{w}(a_1, \ldots, a_n)$. Por el Lema 4.3.5, si para todo $(a_1, \ldots, a_n) \in \mathbb{Z}_2^n$ se tiene que $\overline{w}(a_1, \ldots, a_n) = 1$, entonces $\vDash w$. □

Teorema 4.3.7. Prop(X) *es decidible en validez.*

Demostración. Sea $p \in P(X)$. $\vdash p$ si y sólo si $\vDash p$. □

Corolario 4.3.8. Prop(X) *es decidible en deductibilidad.*

Capítulo 5

Cálculo de Predicados y Propiedades

5.1. Álgebras de Predicados

Las álgebras de proposiciones se construyen sobre conjuntos subyacentes de variables proposicionales. Aquí empezaremos con un conjunto infinito V a cuyos elementos llamaremos variables individuales y un conjunto $\mathcal{R}$ (cuyos elementos serán llamados símbolos de relación o de predicado), junto con una aplicación $\mathrm{ar}\colon \mathcal{R} \to \mathbb{N}$.

Definición 5.1.1. Sea $\widetilde{P}(V, \mathcal{R})$ el álgebra libre, sobre el conjunto $X = \{(r, x_1, \ldots, x_n) : r \in \mathcal{R},\ x_i \in V,\ n = \mathrm{ar}(r)\}$ de generadores libres, de tipo $\mathcal{T} = \{F, \Rightarrow, (\forall x) | x \in V\}$, donde $\mathrm{ar}(F) = 0$, $\mathrm{ar}(\Rightarrow) = 2$, y para todo $x \in V$ $\mathrm{ar}(\forall x) = 1$. Diremos que $\widetilde{P} = \widetilde{P}(V, \mathcal{R})$ es el *álgebra total de primer orden* sobre $(V, \mathcal{R})$. Utilizaremos la notación $r(x_1, \ldots, x_n) = (r, x_1, \ldots, x_n) \in X$ y pondremos $\mathcal{R}_n = \{r \in \mathcal{R} : \mathrm{ar}(r) = n\}$.

Observación. Si $w \in \widetilde{P}$, w es una palabra en los generadores libres de $\widetilde{P}$, cada uno de los cuales es de la forma $r(x_1, \ldots, x_n)$. Si $x_1, \ldots, x_m$ son las distintas variables individuales que intervienen en w, podemos pensar que $w = w(x_1, \ldots, x_m)$ es una función de estas variables.

Observación. Se considera que las dos expresiones

$$(\forall x_1) w(x_1, \ldots, x_m) \qquad \text{y} \qquad (\forall y) w(y, x_2, \ldots, x_m)$$

son iguales si $y \notin \{x_2, \ldots, x_m\}$.

Definición 5.1.2. Sea $w \in \widetilde{P}$. Se llama conjunto de *variables que ocurren* en w, escrito $V(w)$, a

$$V(w) = \bigcap\{U : U \subset V,\ w \in \widetilde{P}(U, \mathcal{R})\}.$$

Ejemplo 5.1.3. (i) $V(F) = \emptyset$. Pues $F \in \widetilde{P}(\emptyset, \mathcal{R})$, $\widetilde{P}(\emptyset, \mathcal{R})$ es $\{F, \Rightarrow\}$-álgebra y $F\colon \{\emptyset\} \to \widetilde{P}(\emptyset, \mathcal{R})$ está dada por $\emptyset \mapsto F$, entonces $\emptyset \in \{U : U \subset V, w \in \widetilde{P}(U, \mathcal{R})\}$ lo que implica $\bigcap\{U : U \subset V, w \in \widetilde{P}(U, \mathcal{R})\} = \emptyset$.

(ii) Si $r \in \mathcal{R}$, $\mathrm{ar}(r) = n$, $x_1, \ldots, x_n \in V$ entonces $V(r(x_1, \ldots, x_n)) = \{x_1, \ldots, x_n\}$. En efecto, para todo $i = 1, \ldots, n$ se tiene que $x_i \in \widetilde{P}(U, \mathcal{R})$ para todo $U \subset V$, luego $\{x_1, \ldots, x_n\} \subset V(r(x_1, \ldots, x_n))$. Recíprocamente, si $x \in V(r(x_1, \ldots, x_n))$, entonces para todo $U \subset V$ se tiene que $r(x_1, \ldots, x_n) \in \widetilde{P}(U, \mathcal{R})$ y $x \in U$; como $r(x_1, \ldots, x_n) \in \widetilde{P}(\{x_1, \ldots, x_n\}, \mathcal{R})$, entonces $x \in \{x_1, \ldots, x_n\}$.

(iii) Si $w_1, w_2 \in \widetilde{P}$, entonces $V(w_1 \Rightarrow w_2) = V(w_1) \cup V(w_2)$. Veamos:

(a) Supongamos que $w_1, w_2 \in \widetilde{P}$. Supongamos que $x \in V(w_1 \Rightarrow w_2)$ entonces para todo $U \subset V$ tenemos que $w_1 \Rightarrow w_2 \in \widetilde{P}(U, \mathcal{R})$ con $x \in U$. Supongamos que existen $U_1, U_2 \subset V$ tales que $w_1 \in \widetilde{P}(U_1, \mathcal{R})$ con $x \notin U_1$ y, $w_2 \in \widetilde{P}(U, \mathcal{R})$ con $x \notin U_2$. Entonces existe $U_1 \cup U_2 \subset V$ tal que $w_1, w_2 \in \widetilde{P}(U_1 \cup U_2, \mathcal{R})$ con $x \notin U_1 \cup U_2$; luego, existe $U_1 \cup U_2 \subset V$ tal que $w_1 \Rightarrow w_2 \in \widetilde{P}(U_1 \cup U_2, \mathcal{R})$ lo que implica $x \in U_1 \cup U_2$, una contradicción. Por tanto, para todo $U_1, U_2 \subset V$ se tiene que $w_1 \in \widetilde{P}(U_1, \mathcal{R})$ con $x \in U_1$ y, $w_2 \in \widetilde{P}(U_2, \mathcal{R})$ con $x \in U_2$, así $x \in V(w_1) \cup V(w_2)$.

(b) Supongamos que $x \in V(w_1) \cup V(w_2)$ entonces para todo $U_1 \subset V$ se tiene que $w_1 \in \widetilde{P}(U_1, \mathcal{R})$ con $x \in U_1$, o para todo $U_2 \subset V$ se tiene que $w_2 \in \widetilde{P}(U_2, \mathcal{R})$ con $x \in U_2$. Supongamos que existe $U \subset V$ tal que $w_1 \Rightarrow w_2 \in \widetilde{P}(U, \mathcal{R})$. Si ponemos $w = w_1 \Rightarrow w_2$, entonces $w = w(x_1, \ldots, x_n)$ con $\{x_i\}_{i=1}^n \subset U$. Si $w_1 = w_1(y_1, \ldots, y_k)$ y $\{y_i\}_{i=1}^k \subset \{x_i\}_{i=1}^n \subset U$, entonces $\{y_i\}_{i=1}^k \subset V$ tal que $w_1 \in \widetilde{P}(\{y_i\}_{i=1}^k, \mathcal{R})$, o, si $w_2 = w_2(z_1, \ldots, z_\ell)$ y $\{z_i\}_{i=1}^\ell \subset \{x_i\}_{i=1}^n \subset U$, entonces $\{z_i\}_{i=1}^\ell \subset V$ tal que $w_2 \in \widetilde{P}(\{z_i\}_{i=1}^\ell, \mathcal{R})$. Entonces $x \in \{y_i\}_{i=1}^k$ o $x \in \{z_i\}_{i=1}^\ell$, de donde $x \in \{x_i\}_{i=1}^n$ o $x \in \{x_i\}_{i=1}^n$, entonces $x \in U$ y esto implica que $x \in V(w_1 \Rightarrow w_2)$.

(iv) Si $x \in V$ y $w \in \widetilde{P}$, entonces $V((\forall x)w) = \{x\} \cup V(w)$. Veamos:
(a) Sean $x \in V$ y $w \in \widetilde{P}$. Supongamos que $y \in V((\forall x)w)$, entonces para todo $U \subset V$ se tiene que $(\forall x)w \in \widetilde{P}(U, \mathcal{R})$ con $y \in U$. Supongamos que $x \neq y$ y que $y \notin V(w)$, entonces existe $U_1 \subset V$ tal que $w \in \widetilde{P}(U_1, \mathcal{R})$ con $y \notin U_1$. Entonces existe $U_1 \cup \{x\} \subset V$ tal que $(\forall x)w \in \widetilde{P}(U_1 \cup \{x\}, \mathcal{R})$ con $y \notin U_1 \cup \{x\}$, y esto implica que existe $U_1 \cup \{x\} \subset V$ tal que $(\forall x)w \in \widetilde{P}(U_1 \cup \{x\}, \mathcal{R})$ con $y \in U_1 \cup \{x\}$, una contradicción. Por tanto, $y = x$ o $y \in V(w)$, de donde $y \in \{x\} \cup V(w)$.
(b) Supongamos que $y \in \{x\} \cup V(w)$, entonces $y = x$ o para todo $U \subset V$ se tiene que $w \in \widetilde{P}(U, \mathcal{R})$ con $y \in U$. Supongamos que existe $U \subset V$ tal que $(\forall x)w \in \widetilde{P}(U, \mathcal{R})$. Si ponemos $w_1 = (\forall x)w$, entonces $w_1 = w_1(x_1, \ldots, x_n)$ y $\{x_i\}_{i=1}^n \subset U$. Luego $y = x$ o $w = w(y_1, \ldots, y_k)$ con $\{y_i\}_{i=1}^k \subset \{x_i\}_{i=1}^n \subset U$ lo que implica $\{y_i\}_{i=1}^k \subset V$ tal que $w \in \widetilde{P}(\{y_i\}_{i=1}^k, \mathcal{R})$. Entonces $y = x$ o $y \in \{y_i\}_{i=1}^k$. Si $(\forall x)w \in \widetilde{P}(U, \mathcal{R})$, entonces $x \in U$ y $\{y_i\}_{i=1}^k \subset U$, entonces $y \in U$, de donde $y \in V((\forall x)w)$.

Observación. Resumiendo el ejemplo:

i) $V(F) = \emptyset$.

ii) Si $r \in \mathcal{R}$, $\text{ar}(r) = n$, $x_1, \ldots, x_n \in V$ entonces $V(r(x_1, \ldots, x_n)) = \{x_1, \ldots, x_n\}$.

iii) Si $w_1, w_2 \in \widetilde{P}$, entonces $V(w_1 \Rightarrow w_2) = V(w_1) \cup V(w_2)$.

iv) Si $x \in V$ y $w \in \widetilde{P}$, entonces $V((\forall x)w) = \{x\} \cup V(w)$.

(i), (ii), (iii), y (iv), se pueden tomar como definición de $V(w)$.

Definición 5.1.4. Sea $w \in \widetilde{P}$. La *profundidad de cuantificación* de w, escrita $d(w)$, se define por

(i) $d(F) = 0$, $d(r(x_1, \ldots, x_n)) = 0$ para todo generador libre de $\widetilde{P}$.

(ii) $d(w_1 \Rightarrow w_2) = \text{máx}(d(w_1), d(w_2))$.

(iii) $d((\forall x)w) = 1 + d(w)(x \in V)$.

Ahora podemos definir en $\widetilde{P}$ la relación de congruencia siguiente.

Definición 5.1.5. Sean $w_1, w_2 \in \widetilde{P}$. Definimos la relación $w_1 \approx w_2$ por

(a) $d(w_1) = d(w_2) = 0$ y $w_1 = w_2$, ó

(b) $d(w_1) = d(w_2) > 0$, $w_1 = a_1 \Rightarrow b_1$, $w_2 = a_2 \Rightarrow b_2$, $a_1 \approx a_2$, y $b_1 \approx b_2$, ó

(c) $w_1 = (\forall x)a$, $w_2 = (\forall y)b$ y, o bien

(i) $x = y$ y $a \approx b$, o bien

(ii) existe $c = c(x)$ tal que $c(x) \approx a$, $c(y) \approx b$ e $y \notin V(c)$.

Observación. Se observa que la notación $c = c(x)$ en la parte (c)(ii) indica el modo cómo el elemento en cuestión depende de la variable x, pero no la posible dependencia de otras variables. La utilizamos para poder representar la sustitución de toda ocurrencia de x por y.

La relación $\approx$ es una relación de congruencia en $\widetilde{P}(V, \mathcal{R})$, puesto que es una relación de equivalencia que es claramente compatible con las operaciones del álgebra.

Definición 5.1.6. El *álgebra de primer orden (reducida)* sobre $\widetilde{P}(V, \mathcal{R})$, indicada por $P(V, \mathcal{R})$, es el álgebra cociente de $\widetilde{P}(V, \mathcal{R})$ por la relación de congruencia $\approx$.

Los elementos de $P = P(V, \mathcal{R})$ son las clases de congruencia. Si $w \in \widetilde{P}$ y $[w]$ es la clase de congruencia de w, entonces

$$(\forall x)[w] = [(\forall x)w]$$
$$[w_1] \Rightarrow [w_2] = [w_1 \Rightarrow w_2].$$

Definición 5.1.7. Sea $w \in P$. Se define el conjunto $\mathrm{var}(w)$ de *variables (libres)* de w poniendo $\mathrm{var}(w) = \mathrm{var}(\widetilde{w})$, donde $\widetilde{w}$ es un representante de la clase de congruencia de w y donde $\mathrm{var}(\widetilde{w})$ se define inductivamente por

(i) $\mathrm{var}(F) = \emptyset$,

(ii) $\mathrm{var}(r(x_1, \ldots, x_n)) = \{x_1, \ldots, x_n\}$ si $r \in \mathcal{R}$ y $x_1, \ldots, x_n \in V$,

(iii) $\mathrm{var}(\widetilde{w}_1 \Rightarrow \widetilde{w}_2) = \mathrm{var}(\widetilde{w}_1) \cup \mathrm{var}(\widetilde{w}_2)$,

(iv) $\mathrm{var}((\forall x)\widetilde{w}) = \mathrm{var}(\widetilde{w}) \setminus \{x\}$.

Definición 5.1.8. Dado $A \subset P$, pondremos

$$\mathrm{var}(A) = \bigcup_{p \in A} \mathrm{var}(p).$$

5.2. Interpretaciones

Definición 5.2.1. Dado un conjunto $U \neq \emptyset$ y las aplicaciones $\varphi\colon V \to U$, $\psi\colon \mathcal{R}_V \to \mathcal{R}_U$, y $v\colon P \to \mathbb{Z}_2$, donde $\mathcal{R}_U$, $\mathcal{R}_V$, $P = P(V, \mathcal{R}_V)$, y si $r \in \mathcal{R}_{V_n}$, entonces $\psi(r) \in \mathcal{R}_{U_n}$. La cuaterna (U, φ, ψ, v) es una *interpretación* de P en el dominio U si satisface:

(a) Si $r \in \mathcal{R}_n$ y $x_1, \ldots, x_n \in V$, entonces $v(r(x_1, \ldots, x_n)) = 1$ si $(\varphi x_1, \ldots, \varphi x_n) \in \psi r$, y $v(r(x_1, \ldots, x_n)) = 0$ si $(\varphi x_1, \ldots, \varphi x_n) \notin \psi r$.

(b) v es un $\{F, \Rightarrow\}$-homomorfismo.

(c_k) Sea $P_k(V, \mathcal{R}) = \{p \in P(V, \mathcal{R}) : d(p) \leq k\}$. Supongamos que $p = (\forall x)q(x)$ tal que $d(p) = k$. Sea $V' = V \cup \{t\}$ con $t \notin V$. Si para toda $\varphi'\colon V' \to U$ extensión de φ y para toda $v'_{k-1}\colon P_{k-1}(V, \mathcal{R}) \to \mathbb{Z}_2$ tal que $(\varphi', \psi, v'_{k-1})$ satisfacen (a), (b), y (c_i), para $i < k$ ocurre que $v'_{k-1}(q(t)) = 1$, entonces $v(p) = 1$. Si $v'_{k-1}(q(t)) = 0$, entonces $v(p) = 0$.

Observación. Dados U, φ, ψ, existe una única aplicación $v\colon P \to \mathbb{Z}_2$ que satisface (a), (b) y (c_i) para todo i.

Observación. Sea $A \subset P$ y $p \in P$. Para toda v interpretación de P tal que $v(A) \subset \{1\}$, entonces $v(p) = 1$ y $A \vDash p$. Tenemos que

$$\mathrm{Con}(A) = \{p \in P : A \vDash p\}.$$

Si $\emptyset \vDash p$, escribimos $\vDash p$ y decimos que p es una *proposición válida*.

5.3. Demostraciones en $\mathrm{Pred}(V, \mathcal{R})$

Definición 5.3.1. El *conjunto de axiomas* de $\mathrm{Pred}(V, \mathcal{R})$ es el conjunto $\mathcal{A} = \mathcal{A}_1 \cup \cdots \cup \mathcal{A}_5$ donde

$$\mathcal{A}_1 = \{p \Rightarrow (q \Rightarrow p) : p, q \in P(V, \mathcal{R})\},$$
$$\mathcal{A}_2 = \{(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r)) : p, q, r \in P(V, \mathcal{R})\},$$
$$\mathcal{A}_3 = \{\sim\sim p \Rightarrow p : p \in P(V, \mathcal{R})\},$$
$$\mathcal{A}_4 = \{(\forall x)(p \Rightarrow q) \Rightarrow (p \Rightarrow ((\forall x)q)) : p, q \in P(V, \mathcal{R}), x \notin \mathrm{var}(p)\},$$
$$\mathcal{A}_5 = \{(\forall x)p(x) \Rightarrow p(y) : p(x) \in P(V, \mathcal{R}), y \in V\}.$$

Definición 5.3.2. Sea $A \subset P$, $p \in P$. Una *demostración de longitud* n de p a partir de A es una sucesión $p_1, \ldots, p_n$ de n elementos de A tales que $p_n = p$, la sucesión $p_1, \ldots, p_{n-1}$ es una demostración de longitud $n-1$ de p_{n-1} a partir de A y

(a) $p_n \in \mathcal{A} \cup A$,

(b) existen $i, j < n$ tales que $p_i = p_j \Rightarrow p_n$,

(c) existe una subsucesión $p_{k_1}, \ldots, p_{k_r}$ de $p_1, \ldots, p_{n-1}$ que es una demostración (de longitud $< n$) de $w(x)$ a partir de un subconjunto $A_0 \subset A$ con $x \notin \mathrm{var}(A_0)$ tal que $p_n = (\forall x)w(x)$.

Observación. Si existe $\{p_i\}_{i=1,\ldots,n}^{A}$ una deducción de p escribiremos, como antes, $A \vdash p$. Tendremos el conjunto

$$\mathrm{Ded}(A) = \{p \in P : A \vdash p\}.$$

De igual manera, $\emptyset \vdash p$ se escribirá $\vdash p$, y en este caso p se llamará un teorema de $\mathrm{Pred}(V, \mathcal{R})$.

Observación. Se define $(\exists x)$ como $\sim (\forall x) \sim$

Ejemplo 5.3.3. Vamos a demostrar que $\{\sim(\exists x)(\sim p)\} \vdash (\forall x)p$, cualquiera que sea $p \in P$. Veamos

$$p_1 = \sim\sim(\forall x)(\sim\sim p) \Rightarrow (\forall x)(\sim\sim p) \qquad (\mathcal{A}_3)$$

$$p_2 = \sim\sim(\forall x)(\sim\sim p) \qquad \text{(hipótesis)}$$

$$p_3 = (\forall x)(\sim\sim p) \qquad (p_1 = p_2 \Rightarrow p_3)$$

$$p_4 = (\forall x)(\sim\sim p(x)) \Rightarrow \sim\sim p(y) \qquad (\mathcal{A}_5)$$

$$p_5 = \sim\sim p(y) \qquad (p_4 = p_3 \Rightarrow p_5, y \notin \mathrm{var}(\sim(\exists x)(\sim p(x))))$$

$$p_6 = \sim\sim p(y) \Rightarrow p(y) \qquad (\mathcal{A}_3)$$

$$p_7 = p(y) \qquad (p_6 = p_5 \Rightarrow p_7)$$

$$p_8 = (\forall y)p(y) \qquad (\text{generalización}, y \notin \mathrm{var}(\sim(\exists x)(\sim p(x))))$$

5.4. Propiedades de $\mathrm{Pred}(V, \mathcal{R})$

Definición 5.4.1. Sea $P_1 = P(V_1, \mathcal{R}^{(1)})$ y $P_2 = P(V_2, \mathcal{R}^{(2)})$. Un *semihomomorfismo* $(\alpha, \beta)\colon (P_1, V_1) \to (P_2, V_2)$ es un par de aplicaciones $\alpha\colon P_1 \to P_2$ y $\beta\colon V_1 \to V_2$ tales que

(a) $\#(\beta(V_1)) \geq \aleph_0$,

(b) α es un $\{F, \Rightarrow\}$-homomorfismo, y

(c) $\alpha((\forall x)p) = (\forall x')\alpha(p)$, donde $x' = \beta(x)$.

Lema 5.4.2. *Sea $(\alpha, \beta)\colon (P_1, V_1) \to (P_2, V_2)$ un semihomomorfismo. Sea $p \in P_1$ y supongamos que $x \in V_1 \setminus \mathrm{var}(p)$. Entonces $\beta(x) \notin \mathrm{var}(\alpha(p))$.*

Demostración. Primero, si $x \neq y$, entonces $(\forall x)p = (\forall y)p$ si y sólo si $x, y \notin \mathrm{var}(p)$.

Como $\#\beta(V_1) \geq \aleph_0$, existe $y' \in \beta(V_1)$ tal que $y' \neq \beta(x)$ e $y' \notin \beta(\mathrm{var}(p))$. Seleccionando $y \in V_1$ tal que $\beta(y) = y'$, resulta que $(\forall x)p = (\forall y)p$. Si $x' = \beta(x)$, entonces tenemos que

$$(\forall x')\alpha(p) = \alpha((\forall x)p) = \alpha((\forall y)p) = (\forall y')\alpha(p),$$

y por tanto, $x' \notin \text{var}(\alpha(p))$. □

Teorema 5.4.3 (Teorema de Sustitución)**.** *Sea* $(\alpha, \beta)\colon (P_1, V_1) \to (P_2, V_2)$ *un semihomomorfismo. Sea* $A \subset P_1$, $p \in P_1$.

(a) *Si* $A \vdash p$ *entonces* $\alpha(A) \vdash \alpha(p)$.

(b) *Si* $A \vDash p$ *entonces* $\alpha(A) \vDash \alpha(p)$.

Demostración. (a) Sea $\{p_i\}_{i=1,\ldots,n}^{A}$ una demostración de p. Vamos a proceder por inducción sobre n para demostrar que $\{\alpha(p_i)\}_{i=1,\ldots,n}^{\alpha(A)}$ es una deducción de $\alpha(p)$.

Si $a = ((\forall x)(p \Rightarrow q)) \Rightarrow (p \Rightarrow (\forall x)q)$ es un axioma del tipo $\mathcal{A}_4$ con $x \notin \text{var}(p)$ entonces $\beta(x) \notin \text{var}(\alpha(p))$, entonces $\alpha(p)$ es un axioma de tipo $\mathcal{A}_4$, así por $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_3$ y, $\mathcal{A}_5$ si $p \in \mathcal{A}^{(1)} \cup A$ entonces $\alpha(p) \in \mathcal{A}^{(2)} \cup \alpha(A)$ con $\mathcal{A}^{(i)}$ axioma en $\text{Pred}(V_i, \mathcal{R}^{(i)})$. Es decir, el resultado es válido para $n = 1$.

Para $n > 1$ podemos suponer, por inducción, que $\{\alpha(p_i)\}_{i=1,\ldots,n-1}^{\alpha(A)}$ es una deducción de $\alpha(p_n)$. Si $p_i = p_j \Rightarrow p_n$ para algún $i, j < n$, entonces $\alpha(p_i) = \alpha(p_j) \Rightarrow \alpha(p_n)$. Si $p_n = (\forall x)q$ donde $\{q_j\}_{i=1,\ldots,k}^{A_0} \subset \{p_i\}_{i=1,\ldots,n}^{A}$ donde $A_0 \subset A$, $q_k = q$ y $x \notin \text{var}(A_0)$, entonces $\{\alpha(q_i)\}_{i=1,\ldots,k}^{\alpha(A_0)}$ es una deducción de $\alpha(q)$. Si $w \in A_0$, $x \notin \text{var}(w)$ y, $x' = \beta(x) \notin \text{var}(\alpha(w))$, así que $x' \notin \text{var}(\alpha(A_0))$ y $\{\alpha(p_1), \ldots, \alpha(p_{n-1}), (\forall x')\alpha(q)\}$ es una deducción de $(\forall x')\alpha(q)$ a partir de $\alpha(A)$ tal que $(\forall x')\alpha(q) = \alpha((\forall x)q) = \alpha(p)$. □

Teorema 5.4.4 (Teorema de Coherencia)**.** *Sea* $A \subset P(V, \mathcal{R})$ *y* $p \in P(V, \mathcal{R})$. *Si* $A \vdash p$, *entonces* $A \vDash p$.

Demostración. Sea $\{p_i\}_{i=1,\ldots,n}^{A}$ una deducción de p. Sea (U, φ, ψ, v) una interpretación de $P(V, \mathcal{R})$ tal que $v(A) \subset \{1\}$. Queremos demostrar que $v(p) = 1$, para lo cual procederemos por inducción sobre n. Si $n = 1$, $p \in \mathcal{A} \cup A$ y entonces $v(p) = 1$. Supongamos que el resultado es cierto para deducciones de longitud menor que $n > 1$. Si $p_i = p_j \Rightarrow p_n$ para algún $i, j < n$, entonces $v(p_i) = v(p_j) = 1$ y de ello se sigue que $v(p) = 1$.

Supongamos ahora que $p_n = (\forall x)q(x)$ y que $\{q_i(x)\}_{i=1,\dots,k}^{A_0}$ es una deducción de $q(x)$ con $A_0 \subset A$ tal que $x \notin \text{var}(A_0)$. En la definición de interpretación tenemos que utilizar la condición (c_r). Supongamos que $d(p) = r$ y $V' = V \cup \{t\}$ con $t \notin V$ y consideremos extensiones $\varphi' \colon V' \to U$ de φ y aplicaciones $v'_{r-1} \colon P_{r-1}(V', \mathcal{R}) \to \mathbb{Z}_2$ como las dadas en la condición (c_r). Tenemos que demostrar que en todos los casos $v'_{r-1}(q_k(t)) = 1$. Existe una extensión $v' \colon P(V', \mathcal{R}) \to \mathbb{Z}_2$ (valuación) con (U, φ', ψ, v') una interpretación de $P(V', \mathcal{R})$. Por el Teorema de Sustitución, $\{q_i(t)\}_{i=1,\dots,k}^{A_0}$ es una deducción de $q(t)$ y entonces $v(q(t)) = 1$ (por hipótesis de inducción), luego $v((\forall x)q(x)) = 1$. □

Corolario 5.4.5 (Teorema de Consistencia)**.** *F no es un teorema de* $\text{Pred}(V, \mathcal{R})$.

Demostración. Sea U un conjunto no vacío, $\varphi \colon V \to U$ una aplicación, $r \in \mathcal{R}_n$ tal que $\psi(r)$ en U con $\text{ar}(\psi(r)) = n$. Entonces existe $v \colon P(V, \mathcal{R}) \to \mathbb{Z}_2$ tal que (U, φ, ψ, v) es una interpretación, entonces $v(F) = 0$ de donde $\not\models F$ lo que implica que $\not\vdash F$. □

Teorema 5.4.6 (Teorema de Deducción)**.** *Sea $A \subset P = P(V, \mathcal{R})$ y $p, q \in P$. Entonces $A \vdash p \Rightarrow q$ si y sólo si $A \cup \{p\} \vdash q$.*

Demostración. (a) Si $A \vdash p \Rightarrow q$, entonces $\{p \Rightarrow q, p, q\}$ es una deducción de q a partir de $A \cup \{p\}$, entonces $A \cup \{p\} \vdash q$.

(b) Supongamos que $A \cup \{p\} \vdash q$, entonces $\{q_i\}_{i=1,\dots,n}^{A \cup \{p\}}$ de $q = q_n$. Por inducción sobre n.

Si $n = 1$, $q \in A \cup \mathcal{A}$, entonces $\{q, q \Rightarrow (p \Rightarrow q), p \Rightarrow q\}$ es una deducción de $p \Rightarrow q$ a partir de A; si $q = p$ entonces $\vdash p \Rightarrow p$ entonces $A \vdash p \Rightarrow q$.

Sea $n > 1$ y $A \vdash p \Rightarrow q_i$ con $i = 1, \dots, n-1$, supongamos que $q \notin \mathcal{A} \cup A \cup \{p\}$ entonces existen $i, j < n$ tales que $q_i = q_j \Rightarrow q$, así $A \vdash p \Rightarrow q_j$ y $A \vdash p \Rightarrow (q_j \Rightarrow q)$.

Existe $\{p_i\}^A_{i=1,\ldots,k+1}$ tal que

$$\begin{aligned} p_k &= p \Rightarrow q_j \\ p_{k+1} &= p \Rightarrow (q_j \Rightarrow q) \\ p_{k+2} &= [p \Rightarrow (q_j \Rightarrow q)] \Rightarrow [(p \Rightarrow q_j) \Rightarrow (p \Rightarrow q)] && (\mathcal{A}_2) \\ p_{k+3} &= (p \Rightarrow q_j) \Rightarrow (p \Rightarrow q) && (\text{MP}) \\ p_{k+4} &= p \Rightarrow q && (\text{MP}) \end{aligned}$$

entonces $\{p_i\}^A_{i=1,\ldots,k+4}$ es una deducción de $p \Rightarrow q$ entonces $A \vdash p \Rightarrow q$.

Ahora vemos (c_r). Supongamos que $q = (\forall x)r(x)$, $A_0 \vdash r(x)$, $A_0 \subset A \cup \{p\}$ y, $x \notin \text{var}(A_0)$. (i) Si $p \notin A_0$ entonces $A_0 \subset A$ y existe $\{p_i\}^{A_0}_{i=1,\ldots,k}$ una deducción de q a partir de A_0, entonces $\{p_1, \ldots, p_k, p_k \Rightarrow (p \Rightarrow p_k), p \Rightarrow p_k\}$ es una deducción de $p \Rightarrow q$ a partir de A. (ii) Si $p \in A_0$ existe $\{p_i\}^{A_0}_{i=1,\ldots,k}$ una deducción de $r(x)$ a partir de A_0. Sea $k < n$ entonces por la hipótesis de inducción $A_1 \vdash p \Rightarrow r(x)$ con $A_1 = A_0 \setminus \{p\}$ entonces (?) $(\forall x)(p \Rightarrow r(x))$ con $p \in A_0$, $x \notin \text{var}(A_0)$ implica $x \notin \text{var}(p)$, entonces $(\forall x)(p \Rightarrow r(x)) \Rightarrow (p \Rightarrow (\forall x)r(x))$ es un axioma de tipo $\mathcal{A}_4$ luego $p \Rightarrow (\forall x)r(x)$ por MP. □

Lema 5.4.7. *Sea A un subconjunto consistente de $P(V, \mathcal{R})$. Supongamos que $(\exists x)p(x) \in A$ y que $t \notin \text{var}(A)$. Entonces $F \notin \text{Ded}(A \cup \{p(t)\})$.*

Demostración. Supongamos que $F \in \text{Ded}(A \cup \{p(t)\})$. Entonces $\sim p(t) \in \text{Ded}(A)$, por el Teorema de Deducción. Como $t \notin \text{var}(A)$ entonces $(\forall x) \sim p(x) \in \text{Ded}(A)$ y $(\exists x)p(x) = \sim (\forall x) \sim p(x) \in A$ entonces $F \in \text{Ded}(A)$, una contradicción. □

Lema 5.4.8. *Sea A un subconjunto consistente de $P(V, \mathcal{R})$. Entonces existen $V^* \supset V$, y $A^* \supset A$, donde $A^* \subset P(V^*, \mathcal{R})$, tales que*

(i) *$F \notin \text{Ded}(A^*)$,*

(ii) *para todo $p \in P(V^*, \mathcal{R})$, o bien $p \in A^* \sim p \in A^*$,*

(iii) *si $(\exists x)p(x) \in A^*$ entonces $p(t) \in A^*$ para algún $t \in V^*$.*

Demostración. Pongamos $V_0 = V$, $A_0 = A$, y $P_0 = P(V, \mathcal{R})$. Construiremos inductivamente V_i, $P_i = P(V_i, \mathcal{R})$, A'_i y A_i, $i > 0$. Para cada $p \in A$ sea $t_p^{(i)} \in \text{var}(A_i)$ y pongamos

$$V_{i+1} = V_i \cup \{t_p^{(i)} : p \in A_i,\ p = (\exists x)q(x) \text{ para algún } q(x)\},$$
$$A'_{i+1} = A_i \cup \{q(t_p^{(i)}) : p \in A,\ p = (\exists x)q(x),\ q(x) \in P_i\}.$$

Supongamos que $F \notin \text{Ded}(A_i)$. Si $F \in \text{Ded}(A'_{i+1})$, entonces existe r tal que $F \in \text{Ded}(A_i \cup \{q_1(t_{p_1}^{(i)}), \ldots, q_r(t_{p_r}^{(i)})\})$, lo que contradice el Lema 5.4.7. Entonces $F \notin \text{Ded}(A'_{i+1})$ y esto implica que existe $A_{i+1} \supset A'_{i+1}$ tal que $F \notin \text{Ded}(A_{i+1})$, por el lema sobre conjuntos consistentes maximales. Así para todo $p \in P$, $p \in A_{i+1}$ ó $\sim p \in A_{i+1}$.

Si $i > 0$ escogemos un A_{i+1} con esas características y ponemos

$$V^* = \bigcup_i V_i, \qquad A^* = \bigcup_i A_i.$$

Si $(\exists x)p(x) \in A^*$, entonces existe i tal que $(\exists x)p(x) \in A_i \supset A'_i \supset A_{i+1} \supset \cdots \supset A_0$. □

Teorema 5.4.9 (Teorema de Satisfacibilidad)**.** *Sea A un subconjunto consistente de $P(V, \mathcal{R})$. Entonces existe una interpretación (U, φ, ψ, v) de $P(V, \mathcal{R})$ tal que $v(A) \subset \{1\}$.*

Demostración. Supongamos que A es un subconjunto consistente de $P(V, \mathcal{R})$.
Por el Lema 5.4.8 existen $V^* \supset V$ y $P(V^*, \mathcal{R}) \supset A^* \supset A$, que cumplen los puntos (i), (ii) y, (iii) del Lema.
Luego, cualquier interpretación de $P(V^*, \mathcal{R})$ con $v(A^*) \subset \{1\}$, restringida a $P(V, \mathcal{R})$ resulta en una interpretación tal que $v(A) \subset \{1\}$. Por consiguiente, no perdemos generalidad si suponemos que los mismos A, V satisfacen (i), (ii) y, (iii) del Lema 5.4.8, además podemos suponer, como se vió en la demostración del Lema mencionado, que A sea consistente maximal.
Construyamos la interpretación buscada: supongamos que $U = V$ y que $\varphi\colon V \to U$

es la aplicación identidad.

Sea $r \in \mathcal{R}_n$, entonces definimos:

$$\psi r = \{(x_1, \ldots, x_n) \in V^n : r(x_1, \ldots, x_n) \in A\}.$$

Si $p \in P(V, \mathcal{R})$, sea $v\colon P(V, \mathcal{R}) \to \mathbb{Z}_2$ tal que $v(p) = 1$ si $p \in A$ y $v(p) = 0$ si $p \notin A$.

De esta manera tenemos la cuaterna (U, φ, ψ, v), que es candidata a ser la interpretación buscada, veamos:

(a) Si $r \in \mathcal{R}_n$ y $(x_1, \ldots, x_n) \in V^n$, entonces $\varphi x_i = x_i$ pues φ es la identidad.

Si $(\varphi x_1, \ldots, \varphi x_n) = (x_1, \ldots, x_n) \in \psi r$, entonces $r(x_1, \ldots, x_n) \in A$, luego $v(r(x_1, \ldots, x_n)) = 1$. Si $(\varphi x_1, \ldots, \varphi x_n) = (x_1, \ldots, x_n) \notin \psi r$, entonces $r(x_1, \ldots, x_n) \notin A$, de donde $v(r(x_1, \ldots, x_n)) = 0$.

(b) Como $F \notin A$ pues A es consistente, entonces $v(F) = 0$.

Si $p, q \in P(V, \mathcal{R})$, entonces $v(p) \Rightarrow v(q) = 1 + v(p)(1 + v(q))$ en $\mathbb{Z}_2$, esta última expresión solo puede ser 0 si $v(p) = 1$ y $v(q) = 0$, es decir, cuando $p \in A$ y $q \notin A$, por el teorema de consistencia maximal tenemos que $A = Ded(A)$, si suponemos que $p \Rightarrow q \in A$, tendríamos que $q \in A$, esta contradicción indica que $p \Rightarrow q \notin A$, luego $v(p \Rightarrow q) = 0$ en $\mathbb{Z}_2$. Finalmente se obtiene que $v(p \Rightarrow q) = v(p) \Rightarrow v(q)$.

(c_{k+1}) Sea t una nueva variable tal que $t \notin V$ y supongamos que $p = (\forall x)q(x)$ con $d(p) = k + 1$, tenemos los siguientes casos:

a) $p = (\forall x)q(x) \in A$: Sea $V' = V \cup \{t\}$ con φ' la extensión de φ a V' y sea $v'_k\colon P_k(V', \mathcal{R}) \to \mathbb{Z}_2$. Por definición de interpretación, sabemos que v'_k satisface (c_i) para $i \leq k$ (hipótesis de inducción). Entonces para todo $w(x) \in P_k(V', \mathcal{R})$, $v'(w(t)) = v(w(y))$ con $y = \varphi'(t)$.

   Como $(\forall x)q(x) \in A$, como A es consistente maximal, tenemos que $q(y) \in Ded(A) = A$

   Así, para todo $y \in V$, $q(y) \in A$, entonces $v'(q(t)) = v(q(y)) = 1$ satisfaciendo la condición (c_{k+1}) para este caso.

b) $p = (\forall x)q(x) \notin A$: Como $\{\sim (\exists x)(\sim q(x))\} \vdash (\forall x)q(x)$, entonces si $\sim (\exists x)(\sim$

$q(x)) \in A$, tendríamos que $(\forall x)q(x) \in Ded(A) = A$, pues A es consistente maximal, de aquí concluimos que $\sim (\exists x)(\sim q(x)) \notin A$.

Por teorema de consistencia maximal, tenemos que $(\exists x)(\sim q(x)) \in A$ luego, para algún $y \in V$ se tiene que $(\sim q(y)) \in A$, de aquí $q(y) \notin A$ pues A por el teorema de consistencia maximal.

Ahora consideremos la extensión φ' de φ a $V' = V \cap \{t\}$ donde t es tal que $\varphi'(t) = y$, además tomamos $v'_k \colon P_k(V', \mathcal{R}) \to \mathbb{Z}_2$.

De aquí tenemos que $v'(q(t)) = v(q(y)) = 0$, que satisface la condición (c_{k+1}) también para este caso.

□

Teorema 5.4.10 (Teorema de Adecuación)**.** *Sea $A \subset P(V, \mathcal{R})$ y $p \in P(V, \mathcal{R})$. Si $A \models p$ entonces $A \vdash p$.*

Demostración. Sea $A \subset P(V, \mathcal{R})$ y $p \in P(V, \mathcal{R})$, con $A \models p$.

Supongamos que $F \notin Ded(A \cup \{\sim p\})$, por tanto existe una interpretación (U, φ, ψ, v) de $P(V, \mathcal{R})$ tal que $v(A \cup \{\sim p\}) = 1$ por el Teorema de Satisfacibilidad, esto contradice $A \models p$.

Así tenemos que $A \cup \{\sim p\}) \vdash F$, de donde $A \vdash \sim\sim p$, por el teorema de deducción, por tanto $A \vdash p$. □

Corolario 5.4.11 (Teorema de Compacidad)**.** *Si $A \models p$, entonces existe un subconjunto finito A_0 de A tal que $A_0 \models p$.*

Demostración. Si $A \models p$, entonces $A \vdash p$ por el teorema de Adecuación. Tomamos el subconjunto finito A_0 de A que resulta de escoger en A solamente los elementos que han sido necesarios para demostrar P, así tenemos que $A_0 \vdash p$, de donde $A_0 \models p$ por el teorema de Coherencia. □

Capítulo 6

Teorías Matemáticas de Primer Orden y Modelos

6.1. Cálculo de Predicados con Identidad

Sea $\mathcal{I} \in \mathcal{R}_2$, con $\text{ar}(\mathcal{I}) = 2$. Como axiomas de identidad tomaremos el conjunto $I \subset P(V, \mathcal{R})$ consistente en

$$(\forall x)\mathcal{I}(x, x), \tag{$A_{\mathcal{I}_1}$}$$

y para todo n, todo $j \leq n$, para todo $r \in \mathcal{R}_n$

$$(\forall x_1)(\forall x_2)\dots(\forall x_n)(\forall y)\big[\mathcal{I}(x_j, y) \Rightarrow [r(x_1, \dots, x_n) \Rightarrow r(x_1, \dots, x_{j-1}, y, x_{j+1}, \dots, x_n)]\big]. \tag{$A_{\mathcal{I}_2}$}$$

Ejemplo 6.1.1. Probaremos que $I \vdash \mathcal{I}(x, y) \Rightarrow \mathcal{I}(y, x)$. Sean $x, y \in V$, $x_1, x_2, x_3 \in V$ y sea $I \cup \{\mathcal{I}(x, y)\}$, entonces

$$(\forall x_1)(\forall x_2)(\forall x_2)[\mathcal{I}(x_1, x_2) \Rightarrow [\mathcal{I}(x_1, x_3) \Rightarrow \mathcal{I}(x_2, x_3)]] \qquad (A_{\mathcal{I}_2})$$

$$(\forall x_1)(\forall x_2)[\mathcal{I}(x_1, x_2) \Rightarrow (\forall x_3)[\mathcal{I}(x_1, x_3) \Rightarrow \mathcal{I}(x_2, x_3)]] \qquad (\mathcal{A}_4,\ \text{MP})$$

además $x_3 \notin \text{var}(\mathcal{I}(x_1, x_2))$

$$(\forall x_3)[\mathcal{I}(x_1, x_3) \Rightarrow \mathcal{I}(x_2, x_3)] \Rightarrow [\mathcal{I}(x_1, x_1) \Rightarrow \mathcal{I}(x_2, x_1)]. \qquad (x_1 \in V)$$

Así

$$(\forall x_1)(\forall x_2)[\mathcal{I}(x_1, x_2) \Rightarrow [\mathcal{I}(x_1, x_1) \Rightarrow \mathcal{I}(x_2, x_3)]] \qquad \text{(MP)}$$

$$(\forall x_1)I(x, y) \Rightarrow [\mathcal{I}(x_1, x_1) \Rightarrow \mathcal{I}(y, x_1)] \qquad (\mathcal{A}_5)$$

$$I(x, y) \Rightarrow [\mathcal{I}(x, x) \Rightarrow \mathcal{I}(y, x)] \qquad (\mathcal{A}_3)$$

$$\mathcal{I}(x, x) \Rightarrow \mathcal{I}(y, x). \qquad \text{(MP)}$$

Luego

$$(\forall x_1)\mathcal{I}(x_1, x_1) \Rightarrow \mathcal{I}(x, x) \qquad (\mathcal{A}_5)$$

$$(\forall x_1)I(x_1, x) \qquad (A_{\mathcal{I}_1})$$

$$\mathcal{I}(x, x) \qquad \text{(MP)}$$

$$\mathcal{I}(y, x). \qquad \text{(MP)}$$

Entonces $I \cup \{\mathcal{I}(x, y)\} \vdash \mathcal{I}(y, x)$, de donde se obtiene lo que queríamos probar.

Ejemplo 6.1.2. Mostraremos ahora que $I \vdash \mathcal{I}(x, y) \Rightarrow (\mathcal{I}(y, z) \Rightarrow \mathcal{I}(x, z))$. Sea $I \cup \{\mathcal{I}(x, y), \mathcal{I}(y, z)\}$, entonces

$$(\forall x_1)(\forall x_2)(\forall x_3)[\mathcal{I}(x_2, x_1) \Rightarrow [\mathcal{I}(x_2, x_3) \Rightarrow \mathcal{I}(x_1, x_3)]]$$

$$\mathcal{I}(y, x) \Rightarrow [\mathcal{I}(y, z) \Rightarrow \mathcal{I}(x, z)]$$

$$\mathcal{I}(y, x), \qquad \mathcal{I}(y, z) \Rightarrow \mathcal{I}(x, z), \qquad \mathcal{I}(x, z),$$

es decir, $I \cup \{\mathcal{I}(x, y)\} \vdash \mathcal{I}(y, z) \Rightarrow \mathcal{I}(x, z)$, de donde se obtiene lo que queríamos.

Definición 6.1.3. Supongamos que $\mathcal{I} \in \mathcal{R}_2$. Una *interpretación propia* de $P(V, \mathcal{R})$ es una interpretación (U, φ, ψ, v) tal que $\psi\mathcal{I}$ es la relación de identidad en U.

Definición 6.1.4. $\mathrm{Pred}_{\mathcal{I}}(V, \mathcal{R})$ es la *lógica* cuya álgebra de proposiciones es $P(V, \mathcal{R} \cup \{\mathcal{I}\})$, cuyas valuaciones son las dadas por interpretaciones propias y en la que se define una demostración de p a partir de A como una demostración en $\mathrm{Pred}_{\mathcal{I}}(V, \mathcal{R} \cup \{\mathcal{I}\})$ de p a partir de $I \cup A$.

Supondremos que $\mathcal{I} \in \mathcal{R}$, así $P(V, \mathcal{R} \cup \{\mathcal{I}\}) = P(V, \mathcal{R})$. Escribiremos $A \vdash_{\mathcal{I}} p$ y $p \in \mathrm{Ded}_{\mathcal{I}}(A)$ para indicar que p es demostrable a partir de A en $\mathrm{Pred}_{\mathcal{I}}(A, \mathcal{R})$, es decir, que $A \cup I \vdash p$ o equivalentemente, que $p\,\mathrm{Ded}(A \cup I)$. Diremos que p es una *consecuencia propia* de A, y escribiremos $A \vDash_{\mathcal{I}} p$, o $p \in \mathrm{Con}_{\mathcal{I}}(A)$ si $v(p) = 1$ para toda interpretación propia de $P(V, \mathcal{R})$ tal que $v(A) \subset \{1\}$.

Teorema 6.1.5 (Teorema de Satisfacibilidad)**.** *Supongamos que $F \notin \mathrm{Ded}_{\mathcal{I}}(A)$. Entonces existe una interpretación propia de $P(V, \mathcal{R})$ tal que $v(A) \subset \{1\}$.*

Demostración. Como $F \notin \mathrm{Ded}(A \cup I)$, existe una interpretación (U, φ, ψ, v) de $P(V, \mathcal{R})$ tal que $v(A \cup I) = \{1\}$. La relación $\psi\mathcal{I}$ es una relación de equivalencia en U. Dado $u \in U$, su clase de equivalencia es $\overline{u} = \{u' \in U : (u, u') \in \psi\mathcal{I}\}$ y sea $\overline{U} = \{\overline{u} : u \in U\}$ el conjunto de estas clases de equivalencia. Definamos $\overline{\varphi}\colon V \to \overline{U}$ dada por $x \mapsto \overline{\varphi(x)}$. Para cada $r \in \mathcal{R}_n$, si $(u_i, u_i') \in \psi\mathcal{I}$ para todo $i = 1, \ldots,$, entonces $(u_1, \ldots, u_n) \in \psi r$ si y sólo si $(u_1', \ldots, u_n') \in \psi r$. Por ello podemos definir una relación $\overline{\psi}r$ en $\overline{U}$ poniendo $(\overline{u}_1, \ldots, \overline{u}_n) \in \overline{\psi}r$ si y sólo si $(u_1, \ldots, u_n) \in \psi r$, entonces $\mathrm{ar}(\overline{\psi}r) = \mathrm{ar}(\psi r) = \mathrm{ar}(r)$. Luego $(\overline{U}, \overline{\varphi}, \overline{\psi}, v)$ es una interpretación propia de $P(V, \mathcal{R})$. En efecto,

(a) Sea $r \in \mathcal{R}_n$ y $x_1, \ldots, x_n \in V$, entonces $(\varphi(x_1), \ldots, \varphi(x_n)) \in \psi r$ si y sólo si $v(r(x_1, \ldots, x_n)) = 1$. Luego $(\varphi(x_1), \ldots, \varphi(x_n)) \in \psi r$ si y sólo si $(\overline{\varphi(x_1)}, \ldots, \overline{\varphi(x_n)}) \in \overline{\psi}r$ si y sólo si $(\overline{\varphi}(x_1), \ldots, \overline{\varphi}(x_n)) \in \overline{\psi}r$.

(b) v es un $\{F, \Rightarrow\}$-homomorfismo.

(c_k) Sea $p = (\forall x)q(x)$, $V' = V \cup \{t\}$ con $t \notin V$, para toda $\varphi'\colon V' \to U$, $\varphi'|_V = \varphi$, para toda $v'_{k-1}\colon P_{k-1}(V', \mathcal{R}) \to \mathbb{Z}_2$. $(\varphi', \psi, v'_{k-1})$ satisface (a), (b) y (c_i) para $i < k$, entonces $v'_{k-1}(q(t)) = 1$ si y sólo si $v(p) = 1$ (v no se altera).

(d) Si $\overline{u} \in \overline{U}$ y $(u, u) \in \psi\mathcal{I}$ y $(\overline{u}, \overline{u}) \in \overline{\psi}\mathcal{I}$, entonces $(\overline{u}, \overline{v}) \in \overline{\psi}\mathcal{I}$ si y sólo si $(u, v) \in \psi\mathcal{I}$ entonces $\overline{u} = \overline{v}$. Así v no se altera y $v(A) \subset \{1\}$. □

Corolario 6.1.6. (i) $\mathrm{Con}_{\mathcal{I}}(A) = \mathrm{Con}(A \cup I)$.

(ii) *Si $A \vDash_{\mathcal{I}} p$ entonces $A \vdash_{\mathcal{I}} p$.*

Demostración. Si $p \in \mathrm{Con}_{\mathcal{I}}(A)$, entonces existe una interpretación propia tal que $v(A) \subset \{1\}$, entonces $v(p) = 1$ y $V(\mathcal{I}) \subset \{1\}$.

Si $p \in \mathrm{Con}(A \cup \mathcal{I})$, entonces $A \cup \mathcal{I} \vDash p$. □

6.2. Teorías Matemáticas de Primer Orden

Definición 6.2.1. Una *teoría matemática de primer orden* es una terna $\mathcal{T} = (\mathcal{R}, A, C)$ tal que $\mathcal{I} \in \mathcal{R}$, $A \subset P(V, \mathcal{R})$ donde $C = \mathrm{var}(A) \subset V$ tal que $V \setminus C$ es finito. El conjunto A se llama conjunto de *axiomas* de $\mathcal{T}$ y a los elementos de C se les llama *constantes individuales* de $\mathcal{T}$; el *lenguaje* de $\mathcal{T}$ es el subconjunto $\mathcal{L}(\mathcal{T}) = \{p \in P(V, \mathcal{R}) : \mathrm{var}(p) \subset C\}$ de $P(V, \mathcal{R})$. Un *teorema* de $\mathcal{T}$ es un elemento $p \in \mathcal{L}(\mathcal{T})$ tal que $A \vdash_{\mathcal{I}} p$.

Observación. V es independiente de $\mathcal{T}$ y de $\mathcal{L}(\mathcal{T})$.

Definición 6.2.2. El conjunto $V_0 = C \cup \{x_i : i \in \mathbb{N}\}$ con $x_i \notin C$ es el conjunto de *variables estándar*.

Definición 6.2.3. El *álgebra* de $\mathcal{T}$ es el conjunto $P(\mathcal{T}) = P(V_0, \mathcal{R})$. Un elemento $p \in P(\mathcal{T})$ con $\mathrm{var}(p) \subset \{x_1, \ldots, x_n\} \cup C$ se llama una *fórmula en n-variables* de $\mathcal{T}$.

Observación. Sea $U \subset P(V, \mathcal{R})$ y $p \in P(V, \mathcal{R})$, entonces escribiremos $U \vdash_{\mathcal{T}} p$ para indicar que $A \cup U \vdash_{\mathcal{I}} p$; $\mathcal{T} \vdash p$ (o $\vdash_{\mathcal{T}} p$) en lugar de $A \vdash_{\mathcal{I}} p$; $U \vDash_{\mathcal{T}} p$ en lugar de $A \cup U \vdash_{\mathcal{I}} p$; y $\mathcal{T} \vDash p$ (o $\vDash_{\mathcal{T}} p$) en lugar de $A \vDash_{\mathcal{I}} p$.

Ejemplo 6.2.4. (Geometría proyectiva plana de primer orden.) Sean $p, \ell \in \mathcal{R}$, $\in\in \mathcal{R}_2$, donde interpretamos $p(x)$ como "x es un punto", $\ell(x)$ como "x es una recta" y $\in (x, y)$ como "x pertenece a y" ($\mathrm{ar}(p) = \mathrm{ar}(\ell) = 1$ y $\mathrm{ar}(\in) = 2$). Ponemos $\mathcal{R} = \{p, \ell, \in, \mathcal{I}\}$, $A = \{a_1, \ldots, a_6\}$ y $C = \emptyset$.

Observación. $(\exists! x)w(x)$ es $(\exists x)(w(x) \wedge (\forall y)(w(y) \Rightarrow \mathcal{I}(x, y)))$ con $w \in P(V, \mathcal{R})$.

Ejemplo 6.2.5. (Teoría de grupos elemental.) Ponemos $\mathcal{R} = \{\mathcal{I}, m\}$, donde $\mathrm{ar}(m) = 3$ y $m(x, y, z)$ es "$xy = z$"; $A = \{a_1, \ldots, a_4\}$ y $C = \{e\}$.

Definición 6.2.6. Un *modelo* de una teoría de primer orden $\mathcal{T} = (\mathcal{R}, A, C)$ es un conjunto M y dos aplicaciones $\nu\colon C \to M$ y $\psi\colon \mathcal{R} \to \mathrm{rel}(M)$ tales que para algún conjunto V de variables ($V \supset C$, $V \setminus C$ infinito) existe una interpretación propia (M, φ, ψ, v) de $P(V, \mathcal{R})$ tal que $\varphi|_C = \nu$ y $v(A) \subset \{1\}$.

Observación. La restricción $v|_{\mathcal{L}(\mathcal{T})}$ está completamente determinada por ν y ψ y es independiente de la elección de V y de la valuación propia. Si elegimos (M, ν, ψ) de $\mathcal{T}$, existe en correspondencia una valuación propia v de $\mathcal{L}(\mathcal{T})$; decimos que $p \in \mathcal{L}(\mathcal{T})$ es *verdadera* respecto del modelo (M, ν, ψ) de $\mathcal{T}$ si $v(p) = 1$.

Ejemplo 6.2.7. Sea $(G, \cdot)$ un grupo, 1 su neutro. Sea $\nu(e) = 1$, $\psi m = \{(x, y, z) \in G^3 : x \cdot y = z\}$, $\psi\mathcal{I}$ la relación de identidad. Entonces (G, ν, ψ) es un modelo de la teoría de grupos elemental.

Observación. Dado un modelo (M, ν, ψ) de una teoría $\mathcal{T}$. Sea $p(x_1, \ldots, x_n)$ una fórmula de $\mathcal{T}$ en n variables. Dados elementos $m_1, \ldots, m_n \in M$ cualesquiera, entonces existe v valuación de $P(V_0, \mathcal{R})$ y (M, ν, ψ, v) una interpretación de $P(V_0, \mathcal{R}) = P(\mathcal{T})$ tal que $\varphi|_C = \nu$ y $\varphi(x_i) = m_i$. Si $v(p) = 1$, entonces diremos que $(m_1, \ldots, m_n)$ satisface $p(x_1, \ldots, x_n)$ o que $p(m_1, \ldots, m_n)$ es *verdadera* en M. Definimos

$$\psi(p) = \{(m_1, \ldots, m_n) \in M^n : p(m_1, \ldots, m_n) \text{ es verdadera en } M\} \subset \mathrm{rel}(M).$$

Definición 6.2.8. Diremos que una relación n-aria ρ en un modelo M de $\mathcal{T}$ es *definible* en $\mathcal{T}$ si existe p fórmula en n variables de $\mathcal{T}$ tal que $\rho = \psi(p)$. Una aplicación $f\colon M^n \to M$ se llama una *aplicación definible* si existe p fórmula de $\mathcal{T}$ en $n + 1$ variables tal que:

(i) para todo $a_1, \ldots, a_n, b \in M$, $f(a_1, \ldots, a_n) = b$ si y sólo si $p(a_1, \ldots, a_n, b)$ es verdadera, y

(ii) $\mathcal{T} \vdash (\forall x_1) \cdots (\forall x_n)(\exists! y) p(x_1, \ldots, x_n, y)$.

Ejemplo 6.2.9. La conjugación es una relación definible en la teoría de grupos elemental. Viene definida por la fórmula

$$p(x_1, x_2) = (\exists x_3)(\exists x_4)(\exists x_5)[m(x_3, x_3, e) \wedge m(x_3, x_1, x_5) \wedge m(x_5, x_4, x_2)].$$

El paso al elemento inverso es una función definible, definida por la fórmula

$$q(x_1, x_2)m(x_2, x_1, e).$$

6.3. Propiedades de las Teorías de Primer Orden

Definición 6.3.1. Una teoría $\mathcal{T}$ de primer orden se llama *consistente* si $\mathcal{T} \nvdash F$.

Teorema 6.3.2. *La teoría $\mathcal{T}$ es consistente si y sólo si existe un modelo de $\mathcal{T}$.*

Demostración. Supongamos que $\mathcal{T}$ es consistente, entonces $F \notin \text{Ded}(\mathcal{T})$, entonces por el Teorema de Satisfacibilidad existe una interpretación propia (M, ν, ψ, v_M) de $P(V, \mathcal{R})$ tal que $v_M(A) \subset \{1\}$. Sean las aplicaciones $\varphi\colon V \to M$ y $\psi\colon \mathcal{R} \to \text{rel}(M)$. Si $C \subset V$ tal que $V \setminus C$ es infinito y $\nu = \varphi|_C$, entonces (M, ν, ψ) es un modelo de $\mathcal{T}$.

Recíprocamente, supongamos ahora que existe un modelo (M, ν, ψ) de $\mathcal{T}$ tal que (M, φ, ψ, v) es una interpretación propia con $\varphi|_C = \nu$ y $v_M(A) \subset \{1\}$. Supongamos que $\vdash_{\mathbf{T}} F$, entonces por el Teorema de Coherencia $\vDash_{\mathcal{T}} F$, luego $A \vDash F$ de donde $v_M(F) = 1$, una contradicción; entonces $\mathcal{T} \nvdash F$. □

Definición 6.3.3. La teoría $\mathcal{T}$ se llama *completa* si y sólo si para todo $p \in \mathcal{L}(\mathcal{T})$, o $\mathcal{T} \vdash p$ o $\mathcal{T} \vdash \sim p$.

Ejemplo 6.3.4. La teoría de grupos elemental no es completa. Sea $p = (\forall x)\mathcal{I}(x, e) \in \mathcal{L}(\mathcal{T})$. Supongamos que $\vdash p$ entonces $\vDash p$ para todo modelo de $\mathcal{T}$ pero si $\text{or}(G) = 1$ entonces $\vDash p$; si $\text{or}(G) \neq 1$ entonces $\nvDash p$. Supongamos que $\vdash \sim p$, entonces $\vDash \sim p$, pero si $\text{or}(G) = 1$ entonces $\vdash p$. Así $\nvdash p$ y $\nvdash \sim p$ en la teoría de grupos elemental.

Teorema 6.3.5. *Una teoría de primer orden $\mathcal{T}$ es completa si y sólo si todo $p \in \mathcal{L}(\mathcal{T})$ que es verdadero en un modelo de $\mathcal{T}$ es verdadero en cualquier otro modelo de $\mathcal{T}$.*

Demostración. Si $\mathcal{T} \vdash F$, entonces no existe un modelo de $\mathcal{T}$ y el resultado es trivial inconsistente. Si $\mathcal{T}$ es consistente, entonces supongamos que $\mathcal{T}$ es completa, y sean M_0 un modelo de $\mathcal{T}$ y $p \in \mathcal{L}(\mathcal{T})$ tales que $v_{M_0}(p) = 1$, entonces $v_{M_0}(\sim p) = 0$ lo que

implica $\nvDash\sim p$ y esto implica que $\nvdash p$ entonces $\vdash p$ ($\mathcal{T}$ es completa). Así $\vDash p$ luego $v_M(p) = 1$ donde v_M es una valuación propia de un modelo M.

Recíprocamente, supongamos para todo $p \in \mathcal{L}(\mathcal{T})$ y supongamos que M_0 es un modelo de $\mathcal{T}$ tal que si $v_{M_0}(p) = 1$, entonces $v_M(p) = 1$ donde M es un modelo de $\mathcal{T}$, entonces $\mathcal{T} \vDash p$, lo que implica por el Teorema de Adecuación que $\mathcal{T} \vdash p$. Si $v_{M_0}(p) = 0$ entonces $v_{M_0}(\sim p) = 1$ de donde $\mathcal{T} \vdash\sim p$ lo que implica que $\mathcal{T}$ es completa. □

Teorema 6.3.6. *Sea $\mathcal{T} = (\mathcal{R}, A, C)$ una teoría consistente. Entonces existe $A' \subset \mathcal{L}(\mathcal{T})$ tal que $A \subset A'$ y tal que $(\mathcal{R}, A', C)$ es consistente y completa.*

Demostración. Si $\mathcal{T}$ es consistente entonces existe M modelo de $\mathcal{T}$. Sea $A' = \{p \in \mathcal{L}(\mathcal{T}) : v_M(p) = 1\}$, entonces $\mathcal{T}' = (\mathcal{R}, A', C)$ es consistente pues $F \notin A'$. Como $v_M(A) \subset \{1\}$ entonces $A \subset A'$ y $\mathcal{L}(\mathcal{T}') = \mathcal{L}(\mathcal{T})$, pues $p \in \mathcal{L}(\mathcal{T}')$ y $\mathrm{var}(p) \subset C$. Si M' es un modelo de $\mathcal{T}'$, entonces M' es un modelo de $\mathcal{T}$ pues $v_{M'}(A) \subset \{1\}$, y M es un modelo de $\mathcal{T}'$ pues $v_M(A') \subset \{1\}$. Sea $p \in \mathcal{L}(\mathcal{T}')$ tal que $v_M(p) = 1$ entonces $p \in A'$ tal que si M' es un modelo de $\mathcal{T}'$ entonces $v_{M'}(A') \subset \{1\}$ entonces $v_{M'}(p) = 1$. Así $\mathcal{T}'$ es completa. □

Definición 6.3.7. Sean (M_1, ν_1, ψ_1) y (M_2, ν_2, ψ_2) modelos de la teoría $\mathcal{T}$. Diremos que M_1 es *isomorfo* a M_2 si existe una aplicación biyectiva $\alpha\colon M_1 \to M_2$ tal que $\alpha\nu_1 = \nu_2$ y $(m_1, \ldots, m_n) \in \psi_1 r$ si y sólo si $(\alpha(m_1), \ldots, \alpha(m_n)) \in \psi_2 r$ para todo $r \in \mathcal{R}_n$ y cualesquiera que sean $m_1, \ldots, m_n \in M_1$, y $n \in \mathbb{N}$.

Definición 6.3.8. Una teoría $\mathcal{T}$ se llama *categórica* si todos los modelos de $\mathcal{T}$ son isomorfos.

Ejemplo 6.3.9. Sea $\mathcal{G}$ la teoría de grupos elemental. Dos modelos G_1 y G_2 de $\mathcal{G}$ son isomorfos si y sólo si son isomorfos en el sentido de la teoría de grupos, entonces $\mathcal{G}$ no es categórica.

Ejemplo 6.3.10. Pongamos el conjunto de axiomas de $\mathcal{G}'$ igual a los axiomas de $\mathcal{G}$ reunido con $\{(\forall x)\mathcal{I}(x, e)\}$. $\mathcal{G}'$ es la teoría de grupos trivial. Si G es un modelo de $\mathcal{G}'$, entonces $\mathrm{or}(G) = 1$. Como todos los grupos de orden 1 son isomorfos, $\mathcal{G}'$ es categórica.

Observación. Si dos modelos M_1 y M_2 son modelos isomorfos de una teoría $\mathcal{T}$ y si $p \in \mathcal{L}(\mathcal{T})$ es tal que $v_{M_1}(p) = 1$, entonces $v_{M_2}(p) = 1$.

Teorema 6.3.11. *Si la teoría $\mathcal{T}$ es categórica, entonces $\mathcal{T}$ es completa.*

Demostración. Sea M_1 un modelo de $\mathcal{T}$ y sea $p \in \mathcal{L}(\mathcal{T})$ tal que $v_{M_1}(p) = 1$ entonces para todo modelo M de $\mathcal{T}$, M es isomorfo a M_1 entonces $v_M(p) = 1$ luego, por el Teorema 6.3.5, $\mathcal{T}$ es completa. □

Definición 6.3.12. El *cardinal* de un modelo $M = (M, \nu, \psi)$ es el cardinal $|M|$ del conjunto M.

Definición 6.3.13. Sea χ un número cardinal. Diremos que la teoría $\mathcal{T}$ es *χ-categórica* o que es *categórica en el cardinal* χ, si todos los modelos de $\mathcal{T}$ de cardinal χ son isomorfos.

Ejemplo 6.3.14. $\mathcal{G}$ es categórica en el cardinal 1, pero no en el cardinal 4, pues existen dos clases de isometría de orden 4.

Observación. Si χ es un cardinal finito, entonces en $\mathcal{L}(\mathcal{T})$ existe un elemento que se distingue si χ es el cardinal de un modelo de $\mathcal{T}$. Sea

$$\begin{aligned}\mathrm{al}(n) = (\exists a_1)\cdots(\exists a_n)\big(&\sim\mathcal{I}(a_1,a_2)\wedge\sim\mathcal{I}(a_1,a_3)\wedge\cdots\wedge\sim\mathcal{I}(a_1,a_n)\\ &\wedge\sim\mathcal{I}(a_2,a_3)\wedge\cdots\wedge\sim\mathcal{I}(a_2,a_n)\wedge\cdots\wedge\sim\mathcal{I}(a_{n-1},a_n)\big).\end{aligned}$$

Si M es un modelo de $\mathcal{T}$ y si $v_M(\mathrm{al}(n)) = 1$, entonces M posee al menos n elementos; si $v_M(\mathrm{al}(n)\wedge\sim\mathrm{al}(n+1)) = 1$, entonces M posee exactamente n elementos.

Teorema 6.3.15. *Supongamos que una teoría $\mathcal{T}$ posee modelos de cardinal finito arbitrariamente grandes. Entonces $\mathcal{T}$ posee un modelo infinito.*

Demostración. Sea $\mathcal{T} = (\mathcal{R}, A, C)$, y pongamos $\mathcal{T}' = (\mathcal{R}, A', C)$ donde $A' = A \cup \{\mathrm{al}(n) : n \in \mathbb{N}^+\}$. Si $A' \vdash_{\mathcal{I}} F$ entonces existe $N \subset \{\mathrm{al}(n) : n \in \mathbb{N}\}$ con $|N|$ finito tal que $A \cup N \vdash_{\mathcal{I}} F$. Pongamos $n_0 = \mathrm{máx}\{n : \mathrm{al}(n) \in N\}$, entonces por hipótesis

existe M modelo de $\mathcal{T}$ tal que $|M| \geq n_0$. Entonces M es modelo de $(\mathcal{R}, A \cup N, C)$ de donde $(\mathcal{R}, A \cup N, C)$ es consistente, una contradicción. Así que $\mathcal{T}'$ es consistente, luego existe un modelo M' de $\mathcal{T}'$. Si M_1 es un modelo de $\mathcal{T}'$, entonces $|M_1| \geq n$ para todo $n \in \mathbb{N}^+$, luego $|M_1|$ es infinito. □

Definición 6.3.16. Llamaremos *cardinal* de una teoría $\mathcal{T} = (\mathcal{R}, A, C)$, escrito $|\mathcal{T}|$, a $|\mathcal{R} \cup A|$. Diremos que $\mathcal{T}$ es *finita* si $\mathcal{R} \cup A$ es finito. Si A es finito diremos que $\mathcal{T}$ tiene *axiomatización finita*.

Observación. Si $x \in C$, entonces existe $a \in A$ tal que $x \in \text{var}(a)$ y $|\text{var}(a)|$ es finito, entonces o bien C y A son ambos finitos o bien $|C| \leq |A|$. Si $\mathcal{R} \cup A$ es infinito, entonces $|\mathcal{L}(\mathcal{T})| = |\mathcal{R} \cup A|$; si $\mathcal{R} \cup A$ es finito, entonces $|\mathcal{L}(\mathcal{T})|$ es numerable. Todo símbolo de relación debe aparecer en algún axioma, entonces o bien $\mathcal{R}$ y A son finitos o bien $|\mathcal{R}| \leq |A| = |\mathcal{R} \cup A|$. Si $A = \{a_1, \ldots, a_n\}$ es finito, entonces puede sustituirse por $A' = \{a_1 \wedge \cdots \wedge a_n\}$.

Teorema 6.3.17 (Teorema de Löwenheim-Skolem)**.** *Sea $\mathcal{T}$ una teoría de primer orden de cardinal χ, sea $\aleph$ un cardinal infinito tal que $\aleph > \chi$. Supongamos que $\mathcal{T}$ posee un modelo infinito, entonces $\mathcal{T}$ posee un modelo de cardinal $\aleph$.*

Demostración. Supongamos que $\mathcal{T} = (\mathcal{R}, A, C)$. Sea $V_0 \supset C$ tal que $|V_0 \setminus C| = \aleph$. Entonces $|P(V_0, \mathcal{R})| = \aleph$. Pongamos

$$A'_0 = I \cup A \cup \{\sim \mathcal{I}(x, y) : x, y \in V_0 \setminus C,\ x \neq y\}.$$

Obtenemos una teoría $\mathcal{T}' = (\mathcal{R}, A'_0, V_0)$. Supongamos que $\mathcal{T}'$ es inconsistente, entonces existe $B \subset \{\sim \mathcal{I}(x, y) : x, y \in V_0 \setminus C, x \neq y\}$ con $|N|$ finito tal que $A \cup B \vdash_{\mathcal{I}} F$, así $\mathcal{T}$ no posee un modelo infinito, lo que contradice la hipótesis, entonces $\mathcal{T}'$ es consistente.

Definimos inductivamente V_n, A'_n y A_n:

$$V_{n+1} = V_n \cup \{t_q^{(n)} : q(x) \in P(V_n, \mathcal{R}),\ (\exists x) q(x) \in A_n\},$$
$$A'_{n+1} = A_n \cup \{q(t_q^{(n)}) : q(x) \in P(V_n, \mathcal{R}),\ (\exists x) q(x) \in A_n\},$$

con $A_{n+1} \subset P(V_{n+1}, \mathcal{R})$ subconjunto consistente maximal tal que $A_{n+1} \supset A'_{n+1}$. Pongamos

$$V^* = \bigcup_n V_n, \qquad A^* = \bigcup_n A_n, \qquad P^* = P(V^*, \mathcal{R}) = \bigcup_n P(V_n, \mathcal{R}).$$

Como $A_0 \supset A'_0$ y A_0 es un subconjunto consistente maximal de $P(V_0, \mathcal{R})$ y $|P(V_0, \mathcal{R})| = \aleph$, entonces $|A_0| = \aleph$. Entonces, como $|P(V_n, \mathcal{R})| = |A_n| = \aleph$, resulta que $|V_{n+1}| = \aleph$ y por tanto $|P(V_{n+1}, \mathcal{R})| = |A_{n+1}| = \aleph$. Por inducción, $|P(V_n, \mathcal{R})| = \aleph$ para todo n, entonces $|V^*| = \aleph$ y $|P^*| = \aleph$.

Como $A^* = \bigcup_n A_n$ y A_n es un subconjunto consistente maximal de $P(V_n, \mathcal{R})$, entonces A^* es consistente (de lo contrario existiría A_k inconsistente). Entonces A^* es un subconjunto consistente de $P^* = P(V^*, \mathcal{R})$. Así por el Teorema de Satisfacibilidad, existe una interpretación propia (M, φ, ψ, v) de $P(V^*, \mathcal{R})$ tal que $v(A^*) \subset \{1\}$.

Entonces existe un modelo M de $\mathcal{T}' = (\mathcal{R}, A'_0, C)$ con $M = V^*/\psi\mathcal{I}$ y φ restringida a $\mathcal{L}(\mathcal{T})$. Como $|V^*| = \aleph$, entonces $|M| = |V^*/\psi\mathcal{I}| \leq \aleph$. Hemos construido A'_0 tal que todo modelo de $\mathcal{T}'$ tiene cardinal $\geq \aleph$, entonces $|M| = \aleph$. Por restricción a $\mathcal{L}(\mathcal{T})$ obtenemos un modelo M de $\mathcal{T}$. $\square$

Capítulo 7

Máquinas de Turing, Funciones Recursivas y Números de Gödel

7.1. Procesos de Decisión y Máquinas de Turing

Imaginamos una máquina de Turing como formada por dos partes: un conjunto finito $\mathfrak{D} = \{q_0, q_1, \ldots, q_m\}$ de (posibles) estados internos, un conjunto finito $\mathfrak{G} = \{s_0, s_1, \ldots, s_k\}$ que se llama el alfabeto de la máquina, donde $s_0 =$"vacío".

Tenemos los tipos de acciones:

- (q_i, s_j, s_ℓ, q_r): Estado interno inicial q_i, estado interno final q_r. Casilla escrutada con símbolo s_j, se sustituye s_j por s_ℓ.
- (q_i, s_j, R, q_r): Estado interno inicial q_i, estado interno final q_r. Casilla escrutada con símbolo s_j, la máquina desplaza la cinta para escrutar la casilla inmediata a la DERECHA de la que está siendo escrutada.
- (q_i, s_j, L, q_r): Estado interno inicial q_i, estado interno final q_r. Casilla escrutada con símbolo s_j, la máquina desplaza la cinta para escrutar la casilla inmediata a la IZQUIERDA de la que está siendo escrutada.

Si ninguna cuaterna empieza por q_i, s_j, se dice que la máquina *para*

Requerimiento determinista: la lista de respuestas de la máquina contiene a lo sumo una cuaterna que empiece con q_i, s_j.

Definición 7.1.1. Una *máquina de Turing* con alfabeto (finito) $\mathfrak{G}$ y conjunto finito de estados internos $\mathfrak{D}$ es un subconjunto M de $\mathfrak{D} \times \mathfrak{G} \times (\mathfrak{G} \cup \{L, R\}) \times \mathfrak{D}$ con $L, R \notin G$ tal que si (a, b, c, d) y $(a, b, c', d') \in M$ entonces $c = c'$ y $d = d'$.

Observación. Denotemos por s_{j_n} el símbolo impreso en la casilla con número n. En todo instante, solamente hay un número finito de casillas no vacías, entonces existen a, b enteros tales que para todo $n < a$ o $n > b$, $j_n = 0$. Entonces el contenido de la cinta queda completamente explicitado por $s_{j_a}\ s_{j_{a+1}} \cdots s_{j_n}\ \ldots, s_{j_b}$. Indicaremos que la máquina está en el estado interno q_i, escrutando la casilla n, se indica por la sucesión $s_{j_a}\ s_{j_{a+1}} \cdots s_{j_{n-1}}\ q_i\ s_{j_n} \cdots s_{j_b}$.

Definición 7.1.2. Una *descripción instantánea* de una máquina de Turing M, con alfabeto $\mathfrak{G}$ y conjunto de estados internos $\mathfrak{D}$, es una sucesión finita

$$d = s_{\alpha_1} s_{\alpha_2} \cdots s_{\alpha_r} q s_{\beta_1} s_{\beta_2} \cdots s_{\beta_t},$$

donde $s_{\alpha_i}, s_{\beta_j} \in \mathfrak{G}$ y $q \in \mathfrak{D}$.

Observación. Supongamos que $s_{\alpha_1} \cdots s_{\alpha_r} = \sigma$ y que $s_{\beta_1} \cdots s_{\beta_t} = \tau$, entonces $d = \sigma q \tau$. Tanto σ como τ pueden ser la sucesión vacía.

Observación. Dos descripciones $d = \sigma q \tau$ y $d' = \sigma' q' \tau'$ denotan el mismo estado si y sólo si $q = q'$, σ' se obtiene de σ añadiendo o eliminando s_0 a su izquierda, τ' se obtiene de τ añadiendo o eliminando s_0 a su derecha. Dos descripciones que están relacionadas de esta manera se llaman equivalentes; la clase de equivalencia que contiene la descripción d sería denotada por $[d]$ y le llamaremos el *estado* descrito por d. Para todo estado $[d]$ existe una única descripción $d = \sigma q \tau$ tal que si $\sigma \neq \emptyset$ y $\tau \neq \emptyset$, el primer símbolo de σ es distinto de s_0 y el último símbolo de τ es distinto de s_0. Esta descripción se llama *descripción óptima* de $[d]$.

Definición 7.1.3. La máquina de Turing *pasa* del estado $[d]$ al estado $[d']$, y escribiremos $[d] \overset{M}{\to} [d']$ si existen representantes $d = \sigma q \tau$ y $d' = \sigma' q' \tau'$ donde $\tau = s_\alpha \tau_1$, tales que

(i) $(q, s_\alpha, s_{\alpha'}, q') \in M$, $\sigma' = \sigma$, $\tau' = s_{\alpha'} \tau_1$,

(ii) $(q, s_\alpha, R, q') \in M$, $\sigma' = \sigma s_\alpha$, $\tau' = \tau_1$,

(iii) $(q, s_\alpha, L, q') \in M$, $\sigma = \sigma'$, $\tau' = s_\beta \tau$ para algn $s_\beta \in \mathfrak{G}$.

Observación. Existe a lo sumo un estado $[d']$ tal que $[d] \overset{M}{\to} [d']$, pues si $d \in [d]$ le corresponde un $d' \in [d']$ tal que (i), (ii) o (iii).

Definición 7.1.4. Un estado $[\sigma q \tau]$ se llama *inicial* si $q = q_0$. Un estado $[\sigma q s_\alpha \tau_1]$ se llama *terminal* si no existe ninguna cuaterna de la forma $(q, s_\alpha, c, d) \in M$.

Observación. $[d]$ es terminal si y sólo si no existe un estado $[d']$ tal que $[d] \overset{M}{\to} [d']$.

Definición 7.1.5. Una *computación* por una máquina M es una sucesión finita $[d_0], [d_1], \ldots, [d_p]$ de estados tales que $[d_0]$ es inicial, $[d_p]$ es terminal y $[d_i] \overset{M}{\to} [d_{i+1}]$ para $i = 0, 1, \ldots, p-1$.

Definición 7.1.6. Diremos que M (una máquina de Turing) *falla* con la entrada $[d_0]$ si no existe ninguna computación de M que empiece con el estado $[d_0]$.

Observación. Para todo estado $[d_i]$ existe un único estado $[d_{i+1}]$ tal que $[d_i] \overset{M}{\to} [d_{i+1}]$. Es por eso que el fallo de M con la entrada $[d_0]$ significa que la sucesión de estados tomados por M iniciada en $[d_0]$ es infinita.

7.2. Funciones Recursivas

Sea M una máquina de Turing con alfabeto $\mathfrak{G}$. Sea $(n_1, n_2, \ldots, n_k) \in \mathbb{N}^k$, pongamos

$$\operatorname{cod}(n_1, n_2, \ldots, n_k) = s_1^{n_1} s_0 s_1^{n_2} s_0 \cdots s_1^{n_{k-1}} s_0 s_1^{n_k},$$

donde $s^n = ss \ldots s$ (n veces).

Supongamos que existe una computación de M con estado inicial $d_0 = q_0 \operatorname{cod}(n_1, \ldots, n_k)$ y supongamos que $d_t = \sigma q \tau$ es su estado terminal (unívocamente determinado). Podemos tomar una descripción "d_t" del estado terminal d_t que tenga al menos ℓ ocurrencias de s_0 en τ. Sea $(a_1, \ldots, a_\ell) \in \mathbb{N}^\ell$ definiendo a_1 como el número de veces que aparece s_1 en τ antes de la primera ocurrencia de s_0, y a_i (para $2 \leq i \leq \ell$) como el número de veces que aparece s_1 en τ entre la ocurrencia $(i-1)$-ésima y la ocurrencia i-ésima de s_0.

Sea $U_M^{(k,\ell)} \subset \mathbb{N}^k$ tal que $(n_1, \ldots, n_k) \in U_M^{(k,\ell)}$ si y sólo si existe una computación C de M tal que $q_0 \operatorname{cod}(n_1, \ldots, n_k)$ es estado inicial de C. Si $(n_1, \ldots, n_k) \in U_M^{(k,\ell)}$, está definido $(a_1, \ldots, a_\ell) \in \mathbb{N}^\ell$.

Definición 7.2.1. La aplicación

$$\Psi_M^{(k,\ell)} \colon U_M^{(k,\ell)} \longrightarrow \mathbb{N}^\ell$$
$$(n_1, \ldots, n_k) \longmapsto (a_1, \ldots, a_\ell)$$

se llama *función recursiva parcial*. Si $U_M^{(k,\ell)} = \mathbb{N}^k$ entonces la aplicación $\Psi_M^{(k,\ell)}$ se llama *función recursiva total*.

Definición 7.2.2. Un subconjunto $U \subset \mathbb{N}$ se llama *recursivamente numerable* si $U = \emptyset$ o $U = f(\mathbb{N})$ donde f es una función recursiva $f \colon \mathbb{N} \to \mathbb{N}$.

Observación. Un conjunto U es recursivamente numerable si y sólo si es el dominio de una función recursiva parcial.

Definición 7.2.3. Un subconjunto $U \subset \mathbb{N}$ se llama *recursivo* si su función característica $\chi \colon U \to \mathbb{N}$, dada por $u \mapsto 1$ si $u \in U$ y $v \mapsto 0$ si $v \notin U$, es recursiva.

Observación. Un conjunto U es recursivo si y sólo si U y $\mathbb{N} \setminus U$ son recursivamente numerables.

7.3. Números de Gödel

Sea $\mathfrak{G}^* = \{s_i : i \in \mathbb{N}\}$ el alfabeto universal donde $s_0 =$"vacío", y $\mathfrak{D}^* = \{q_i : i \in \mathbb{N}\}$ la lista universal de estados internos donde $q_0 =$"estado interno inicial".

Una máquina de Turing M emplea un subconjunto finito de $\mathfrak{D}^*$ que contiene a q_0 y emplea un subconjunto finito de $\mathfrak{G}^*$ que contiene a s_0, es un subconjunto finito de $\mathfrak{D}^* \times \mathfrak{G}^* \times (\mathfrak{G}^* \cup \{L, R\}) \times \mathfrak{D}^*$.

Observación. Una máquina para cuando escruta un símbolo que no pertenece a su alfabeto.

Definición 7.3.1. Denotemos $(a, b, c, d) \in M$ mediante la fila *abcd*. Estas filas de M se pueden ordenar lexicográficamente. Definamos la aplicación $G \colon \{L, R\} \cup \mathfrak{G}^* \cup \mathfrak{D}^* \to \mathbb{N}$ dada por

$$G(L) = 1, \quad G(R) = 3, \quad G(s_i) = 4i + 5, \quad G(q_j) = 4j + 7, \qquad i, j \in \mathbb{N}.$$

Supongamos para todo $i = 1, \ldots, r$ $G(a_i) = m_i$ a_i símbolos, supongamos la fila $a_1 \cdots a_r$

$$G(a_1, \ldots, a_r) p_1^{n_1} \cdots p_r^{n_r}$$

$p_k = k$-ésimo número primo (de modo que $p_1 = 2$, $p_2 = 3$,...).

Si $\sigma_1, \ldots, \sigma_s$ son filas de símbolos, entonces definimos

$$G(\sigma_1, \ldots, \sigma_s) = p_1^{G(\sigma_1)} p_2^{G(\sigma_2)} \cdots p_s^{G(\sigma_s)}.$$

Finalmente, $G(M)$ es el número de Gödel de la única sucesión finita de filas asociadas a M.

Si se distingue cada símbolo a_i como el único elemento a_i y cada fila σ con el único término σ. G es inyectiva, por el Teorema Fundamental de la Aritmética (descomposición única de un natural en primos).

Supongamos que $\mathcal{T} = (R, A, C)$ una teoría numerable, entonces $|\mathcal{T}| = |R \cup A|$ es numerable, entonces $|R|$ es a lo sumo numerable y $|C| \leq |\mathcal{T}|$, entonces para todo $i \in \mathbb{N}$, $R_i = \{r_i \in R : \text{ar}(r) = i\}$ es a lo sumo numerable. Sea $R^* = \{r_{ij} : i, j \in \mathbb{N}\}$ tal que para todo $j \in \mathbb{N}$ $r_{ij} \in R_i^*$ es un conjunto universal de símbolos de relación.

Tenemos que $C^* = \{c_j : j \in \mathbb{N}\}$ es un conjunto universal de constantes, $X^* = \{x_j : j \in \mathbb{N}\}$ es un conjunto universal de variables, y $V^* = C^* \cup X^*$. Los símbolos de operación: $F, \Rightarrow .\{(\forall x_j) : j \in \mathbb{N}\}$ (se obvia paréntesis). Es un alfabeto universal donde se puede escribir cualquier teoría numerable, donde $\widetilde{P}(V^*, \mathcal{R}^*)$ es el álgebra de esta teoría numerable (sea usa variables estándar $C \cup \{x_i : i \in \mathbb{N}\}$). $w \in \widetilde{P}(V^*, \mathcal{R}^*)$, se puede escribir como una fila finita de símbolos del alfabeto universal donde escribiremos $\Rightarrow ab$ en lugar de $a \Rightarrow b$ y $r_{ij} x_1 x_2$ en lugar de $r_{ij}(x_1, x_2)$.

Así cada fila de símbolos tiene a lo sumo un sentido como elemento de $\widetilde{P}(V^*, \mathcal{R}^*)$. Asignamos números de Gödel al alfabeto universal de elementos de $\widetilde{P}(V^*, \mathcal{R}^*)$

$$\begin{array}{lll} G(F) = 2 & G(\Rightarrow) = 3 & G(r_{ij}) = 5^{i+1} 7^{j+1} \\ G(c_j) = 11^{j+1} & G(x_j) = 13^{j+1} & G((\forall x_j)) = 17^{j+1}. \end{array}$$

Para la fila de símbolos $a_1 a_2 \ldots a_n$

$$G(a_1 \ldots a_n) = p_1^{G(a_1)} \ldots p_n^{G(a_n)},$$

donde p_i es el i-ésimo número primo. Para $p \in P(V^*, \mathcal{R}^*) = \widetilde{P}(V^*, \mathcal{R}^*)$, ponemos

$$G(p) = \text{mín}\{G(w) : w \in P\}.$$

Observación. Se puede modificar G de manera que tenga definición única para máquina de Turing y álgebras de proposiciones.

Capítulo 8

Problemas Insolubles e Indecidibilidad en el Cálculo de Predicados

8.1. Problemas Insolubles en Matemáticas

Dada $\mathcal{T}$ una teoría matemática de primer orden, ¿podemos determinar si $p \in \mathcal{L}(\mathcal{T})$ es o no un teorema? Supongamos que $p \in \mathcal{L}(\mathcal{T})$ y supongamos que p es un teorema de $\mathcal{T}$, entonces existe demostración de p en $\mathcal{T}$, es decir, existe un conjunto finito de símbolos del alfabeto universal y podemos comprobar si se trata de un axioma o se obtiene de pasos anteriores (M.P. o Generalización), por M.P. es mecánico, mientras que por Generalización necesitamos identificar los axiomas matemáticos de $\mathcal{T}$.

Definición 8.1.1. Sea $\mathcal{T}$ una teoría numerable expresada en el alfabeto universal. Diremos que $\mathcal{T}$ está *efectivamente axiomatizada* si la función característica del conjunto de los números de Gödel de los axiomas matemáticos de $\mathcal{T}$ es recursiva.

Observación. Si $\mathcal{T}$ está efectivamente axiomatizada, entonces existe una máquina de Turing tal que dado $q \in P(V^*, \mathcal{R}^*)$, $G(q)$ nos dice si q es un axioma o no de $\mathcal{T}$.

Observación. Supongamos que $\mathcal{T} = (R, A, C)$ es una teoría efectivamente axiomatizada, entonces existe una máquina de Turing tal que dados los números de Gödel de

$p \in \mathcal{L}(\mathcal{T})$ y $p_1, \ldots, p_n$ es una sucesión de elementos de $P(V^*, \mathcal{R}^*)$, si $p_1, p_2 \ldots, p_n$ es o no una demostración de p en $\mathcal{T}$. Existe una máquina de Turing que computa, dado $G(p)$ con $\mathcal{T} \vdash p$, el menor número entre los números de Gödel de las demostraciones de p.

Observación. Si p no es teorema de $\mathcal{T}$, entonces $\mathcal{T}' = (\mathcal{R}, A \cup \{\sim p\}, C)$ es consistente, entonces posee un modelo. Luego si $\mathcal{T}'$ posee un modelo, entonces p no es teorema de $\mathcal{T}$.

Observación. En $\mathcal{T}$, una teoría efectivamente axiomatizada, el problema de decidir si p es o no un teorema es soluble pues: Si p es un teorema, se busca una demostración de p; si p no es un teorema, se busca un modelo de $\mathcal{T}'$.

Definición 8.1.2. La familia $\{p_n : n \in \mathbb{N}\}$ se llama *recursivamente numerable* si $\{G(p_n) : n \in \mathbb{N}\}$ es un subconjunto recursivamente numerable de $\mathbb{N}$, y se llama *recursivo* si $\{G(p_n) : n \in \mathbb{N}\}$ es un subconjunto recursivo de $\mathbb{N}$. Si $G(p_n)$ es una función recursiva de n, diremos que la familia está *recursivamente enumerada*.

Observación. Para determinar si p_n es o no un teorema de $\mathcal{T}$, se puede encontrar $f\colon \mathbb{N} \to \{0, 1\}$, dada por $n \mapsto f(p_n)$, que sea recursiva (i.e., calculable por algún procedimiento mecánico), tal que $f(p_n) = 1$ si y sólo si p_n es un teorema, es decir, que la familia $\{p_n\}$ está recursivamente enumerada.

Definición 8.1.3. Sea $\mathcal{F} = \{p_n : n \in \mathbb{N}\}$ una familia recursivamente enumerada de proposiciones de una teoría $\mathcal{T}$. Diremos que el problema de decisión para $\mathcal{F}$ es *recursivamente soluble* si la función característica de $\{n \in \mathbb{N} : \mathcal{T} \vdash p_n\}$ es recursiva.

Observación. Si $\mathcal{L}(\mathcal{T})$ tiene un problema de decisión recursivamente soluble, entonces $\mathcal{T}$ es *decidible*. Si $\mathcal{T}$ es una teoría numerable (en el alfabeto universal), entonces la asignación de la función $G\colon \mathcal{L}(\mathcal{T}) \to \mathbb{N}$ ordena $\mathcal{L}(\mathcal{T})$ proporcionando una enumeración recursiva de $\mathcal{L}(\mathcal{T})$.

Observación. Si $\mathcal{T}$ está efectivamente axiomatizada y es completa, entonces $\mathcal{T}$ es decidible, pues existe una máquina de Turing tal que si $p \in \mathcal{L}(\mathcal{T})$, dado $G(p)$, resuelve la cuestión de si p es o no un teorema.

Ejemplo 8.1.4. Sea M_n la n-ésima máquina de Turing. Determinar para todos los enteros n, r si existe o no una computación de M_n que empiece con el estado $q_0\,\mathrm{cod}(r)$, i.e., determinar si una máquina de Turing M_n (cualquiera) llegará parar después de introducir un entero r. Este problema es recursivamente insoluble. Supongamos que $f_n = \Psi_{M_n}^{(1,1)}$, el problema es determinar los pares (n, r) para los que $f_n(r)$ existe. Supongamos que $f\colon \mathbb{N} \to \mathbb{N}$ dada por

$$f(n) = \begin{cases} 1 & \text{si } f_n(n) \text{ existe} \\ 0 & \text{en otro caso} \end{cases}$$

es recursiva, entonces $g\colon \mathbb{N} \to \mathbb{N}$ dada por

$$g(n) = \begin{cases} f_n(n) + 1 & \text{si } f_n(n) \text{ existe} \\ 0 & \text{en otro caso} \end{cases}$$

es también recursiva pues $f_n(n)$ puede ser computado si existe. Además $\{f_n : n \in \mathbb{N}\}$ contiene a todas las funciones recursivas $\mathbb{N} \to \mathbb{N}$, entonces existe m tal que $g = f_m$, luego

$$f_m(m) = g(m) = f_m(m) + 1,$$

entonces f no es recursiva, por ello, no existe una máquina de Turing que determine para todo n si $f_n(n)$ existe o no. Como $h(n) = f_n(n)$ es recursiva parcial, existe M máquina de Turing que la computa, entonces el problema de parada de M es recursivamente insoluble.

Observación. Existen conjuntos recursivamente numerables que no son recursivos

$$A = \{n : f_n(n) \text{ existe}\} = h(U_{M_n}^{(1,1)})$$

y h es recursiva parcial. Además, si χ es la función característica de A, si ponemos $f = \chi$ no es recursiva, luego A es recursivamente numerable, pero A no es recursivo.

8.2. Problemas Insolubles en Aritmética

Definimos los axiomas de Peano en una teoría de primer orden $\mathcal{P}$. Sean $\theta \in \mathcal{R}_1$ donde $\theta(x)$ es "$x = 0$", $s \in \mathcal{R}_2$ donde $s(x, y)$ es "x es el siguiente de y", $a, m \in \mathcal{R}_3$ donde $a(x, y, z)$ es "$x + y = z$" y $m(x, y, z)$ es "$x \cdot y = z$".

1) Los axiomas de Peano son:

$p_1 : (\exists!x)\theta(x)$,
$p_2 : (\forall x)(\exists!x)s(y, x)$,
$p_3 : (\forall x)(\forall y)(\forall z)[(s(z, x) \wedge s(z, y)) \Rightarrow x = y]$,
$p_4 : (\forall x)(\forall y)(s(x, y) \Rightarrow\sim \theta(x))$,
p_5 : para todo $\pi(x) \in P(V, \mathcal{R})$ tal que $y, z \notin \mathrm{var}(\pi(x))$
$(\exists x)(\theta(x) \wedge \pi(x)) \wedge (\forall y)(\forall z)(\pi(z) \wedge s(y, z) \Rightarrow \pi(y)) \Rightarrow (\forall y)\pi(y)$.

Observación. $\mathcal{P}$ es una teoría numerable que admite a $\mathbb{N}$ como modelo.

2) Los axiomas de adición son:

$\mathrm{add}_1 : (\forall x)(\forall y)(\exists!z)a(x, y, z)$,
$\mathrm{add}_2 : (\forall x)(\forall y)(\theta(y) \Rightarrow a(x, y, x))$,
$\mathrm{add}_3 : (\forall x)(\forall y)(\forall z)(\forall t)(\forall u)[s(z, y) \wedge a(x, z, t) \wedge a(x, y, u) \Rightarrow s(t, u)]$.

3) Los axioma de multiplicación son:

$\mathrm{mult}_1 : (\forall x)(\forall y)(\exists!z)m(x, y, z)$,
$\mathrm{mult}_2 : (\forall x)(\forall y)(\theta(y) \Rightarrow m(x, y, y))$,
$\mathrm{mult}_3 : (\forall x)(\forall y)(\forall z)(\forall t)(\forall u)[s(z, y) \wedge m(x, z, t) \wedge m(x, y, u) \Rightarrow a(u, x, t)]$.

4) Los axiomas de identificación son:

$e_n = (\exists x_0)(\exists x_1)\cdots(\exists x_{n-1})[\theta(x_0) \wedge s(x_1, x_0) \wedge \cdots \wedge s(x_{n-1}, x_{n-2}) \wedge s(n, x_{n-1})]$.

Definición 8.2.1. La teoría $\mathcal{N}$ tal que $\mathcal{R}(\mathcal{N}) = \{=, \theta, s, a, m\}$, $C(\mathcal{N}) = \mathbb{N}$ y $A(\mathcal{N}) = \{p_1, \ldots, p_5, \mathrm{add}_1, \ldots, \mathrm{add}_3, \mathrm{mult}_1, \ldots, \mathrm{mult}_3, e_n, n \in \mathbb{N}\}$ se llama *aritmética recursiva.*

Observación. Sea $\mathcal{N}_0$ tal que $A(\mathcal{N}_0) = A(\mathcal{N}) \setminus \{p_5\}$. $\mathcal{N}$, $\mathcal{N}_0$ son teorías efectivamente axiomatizadas, pues la función característica del conjunto de los números de Gödel de A es recursiva.

Definición 8.2.2. Sean $\mathcal{T} = (\mathcal{R}, A, C)$ y $\mathcal{T}' = (\mathcal{R}', A', C')$ teorías de primer orden. Diremos que $\mathcal{T}'$ *extiende a* $\mathcal{T}$, y escribiremos $\mathcal{T}' \supseteq \mathcal{T}$ si $\mathcal{R}' \supseteq \mathcal{R}$, $A' \supseteq A$ y $C' \supseteq C$.

Definición 8.2.3. Sea $\mathcal{T}' \supseteq \mathcal{T}$ y $M = (M, \nu, \psi)$ un modelo de $\mathcal{T}$. Diremos que M *extiende a un modelo de* $\mathcal{T}'$ si existen aplicaciones $\nu' \colon C' \to M$ y $\psi' \colon \mathcal{R}' \to \mathrm{rel}(M)$ que extienden a ν y ψ respectivamente, tales que (M, ν', ψ') es un modelo de $\mathcal{T}'$.

Definición 8.2.4. Supongamos que $\mathcal{T} = (\mathcal{R}, A, C) \supseteq \mathcal{N}_0$ y que admite a $\mathbb{N}$ como modelo. Sea $f \colon U \to \mathbb{N}$ una función definida en algún subconjunto U de $\mathbb{N}$. Diremos que f es *fuertemente definible* en $\mathcal{T}$ si existe $p(x, y) \in P(V, \mathcal{R})$ tal que, para todo $m, n \in \mathbb{N}$, $\mathcal{T} \vdash p(m, n)$ si y sólo si $m \in U$ y $f(m) = n$.

Extendemos esta definición a funciones de varias variables. Sea $f \colon U \to \mathbb{N}^\ell$ donde $U \subset \mathbb{N}^k$. Diremos que f es *fuertemente definible* si existe $p(x_1, \ldots, x_{k+\ell}) \in P(V, \mathcal{R})$ tal que, para todo $(m_1, \ldots, m_k) \in \mathbb{N}^k$ y $(n_1, \ldots, n_\ell) \in \mathbb{N}^\ell$,

$$\mathcal{T} \vdash p(m_1, m_2, \ldots, m_k, n_1, n_2, \ldots, n_\ell)$$

si y sólo si $(m_1, \ldots, m_k) \in U$ y $f(m_1, \ldots, m_k) = (n_1, \ldots, n_\ell)$.

Observación. El resultado buscado es: "Si $\mathcal{T} \supseteq \mathcal{N}_0$ y admite a $\mathbb{N}$ como modelo, entonces toda función recursiva parcial es fuertemente definible en $\mathcal{T}$".

Definición 8.2.5. Supongamos que M es una máquina de Turing tal que $[d] = [s_{\beta_t} \ldots s_{\beta_1} q_i s_{\alpha_1} \ldots s_{\alpha_k}]$ es un estado de M. La *función de estado* correspondiente a $[d]$ es $f \colon \mathbb{N} \to \mathbb{N}$ dada por

$$\begin{aligned}
f(0) &= G(q_i), \\
f(2i+1) &= G(s_{\alpha_{i+1}}), \qquad 0 \leq i \leq k-1, \\
f(2i+1) &= G(s_0), \qquad i \geq k, \\
f(2i+2) &= G(s_{\beta_{i+1}}), \qquad 0 \leq i \leq \ell - 1, \\
f(2i+2) &= G(s_0), \qquad i \geq \ell.
\end{aligned}$$

Observación. Las funciones de estado son siempre fuertemente definibles ya que siempre toman el valor $G(s_0)$ salvo en un conjunto finito.

Observación. Supongamos que M es una máquina de Turing y sea f una función de estado inicial, a partir de f se puede construir la descripción de f_1 función de

estado que resulta después de un paso de la computación. Así se puede exhibir una descripción de la función de estado f_n resultante de n pasos de la computación, la complejidad de la descripción crece con n.

Lema 8.2.6 (Lema del número secuencial)**.** *Existe una función fuertemente definible* $\text{seq}\colon \mathbb{N}^+ \times \mathbb{N} \to \mathbb{N}$ *tal que para todo* n *y* $a_0, a_1, \ldots, a_n \in \mathbb{N}$*, existe un* $b \in \mathbb{N}^+$ *con la propiedad de que*

$$\text{seq}(b, r) = a_r, \qquad \textit{con} \quad r = 0, 1, \ldots, n.$$

Demostración. Sea $T(n)$ el n-ésimo número triangular

$$T(n) = 1 + 2 + \cdots + n = \frac{1}{2}n(n+1).$$

Para todo $z > 0$, existe un único n tal que

$$T(n) < z \leq T(n+1) = T(n) + n + 1.$$

Así que z se puede expresar de manera única como $z = T(n) + y$ con $0 < y \leq n + 1$. Sea $x = x + 2 - y$, entonces $x = L(z)$, $y = R(z)$ están bien definidas. Sea $P(x, y) = T(x + y - 2) - y$, P, L, R son funciones fuertemente definibles ya que $z = P(x, y)$ es

$$(x > 0) \wedge (y > 0) \wedge (2z = (x + y - 2)(x + y - 1) + 2y),$$

$x = L(z)$ es

$$(x > 0) \wedge (z > 0) \wedge (\exists y)[(y > 0) \wedge (2z = (x + y - 2)(x + y - 1) + 2y)],$$

e $y = R(z)$ es

$$(y > 0) \wedge (z > 0) \wedge (\exists x)[(x > 0) \wedge (2z = (x + y - 2)(x + y - 1) + 2y)].$$

La función $\text{seq}(b, r)$ se define por

$$L(b) = [1 + (r + 1)R(b)]t + \text{seq}(b, r), \qquad \text{con} \quad t \in \mathbb{N};$$

la relación $z = \text{seq}(x, y)$ es

$$(x > 0) \wedge [z < 1 + (y + 1)R(x)] \wedge (\exists t)[L(x) = t(1 + (y + 1)R(x)) + z].$$

Finalmente, sea $a_1, \ldots, a_n \in \mathbb{N}$. Sea $c \in \mathbb{N}$ tal que $c > a_r$ para todo $0 \leq r \leq n$ y $k \mid c$ para todo $k = 1, 2, \ldots, n$. Sea $m_r = 1 + (r + 1)c$ con $0 \leq r \leq n$. Supongamos que $0 \leq r < s \leq n$, entonces $m_r = 1 + (r + 1)c$ y $m_s = 1 + (s + 1)c$. Supongamos que $d \mid m_r$ y $d \mid m_s$, entonces $d \mid (s + 1)m_r - (r + 1)m_s$ y

$$(s + 1)m_r - (r + 1)m_s = (s + 1) - (r + 1) + (s + 1)(r + 1)c - (r + 1)(s + 1)c = s - r,$$

entonces $d \mid s - r$ y como $1 \leq s - r \leq n$ entonces $s - r \mid c$. Luego $d \mid c$ y $d \mid (1 + (r + 1)c)$ entonces $d \mid 1$ de donde $d = 1$, así para todo $0 \leq r, s \leq n$, $(m_r, m_s) = 1$.

Por tanto, el sistema de congruencias

$$x \equiv a_r \text{ mód } m_r \qquad (r = 0, \ldots, n)$$

tiene solución por el Teorema chino del residuo. Sea e una solución positiva del sistema y pongamos $b = P(e, c)$. Entonces $e = L(b)$, $c = R(b)$ y

$$L(b) \equiv a_r \text{ mód } (1 + (r + 1)R(b)), \qquad (r = 0, \ldots, n)$$

y $a_r < c < 1 + (r + 1)R(b)$, lo cual muestra que $a_r = \text{seq}(b, r)$ con $r = 0, \ldots, n$. □

Observación. Sea M una máquina de Turing y sea $(q_\alpha, s_\beta, a, b) \in M$, definimos $M_{\alpha\beta}(x, y, z) \in P(V, \mathcal{R})$ de tal modo que: existe γ tal que $b = q_\gamma$, existe β' tal que $a = s_{\beta'}$, o bien $a = L$ ó $a = R$. Pongamos

$$M_{\alpha\beta}(x, y, z) = [\text{seq}(x, 0) = G(q_\alpha)] \wedge [\text{seq}(x, 1) = G(s_\beta)] \wedge [y = 0 \Rightarrow z = G(q_\gamma)] \wedge k(x, y, z)$$

donde

$$K(x, y, z) = [y = 1 \Rightarrow z = G(s_{\beta'})] \wedge [y > 0 \Rightarrow z = \text{seq}(x, y)],$$

si $a = s_{\beta'}$

$$K(x,y,z) = [((\exists k)(y = 2k+1)) \Rightarrow z = \text{seq}(x, y+z)] \wedge [y = z \Rightarrow z = \text{seq}(x,1)]$$
$$\wedge [((\exists k)(y = 2k+4)) \Rightarrow z = \text{seq}(x, y-2)],$$

si $a = R$

$$K(x,y,z) = [y = 1 \Rightarrow z = \text{seq}(x,2)] \wedge [((\exists k)(y = 2k+3)) \Rightarrow z = \text{seq}(x, y-2)]$$
$$\wedge [((\exists k)(y = 2k+2)) \Rightarrow z = \text{seq}(x, y+2)],$$

si $a = L$.

Sea

$$M(x,y,z) = \bigvee_{\alpha,\beta} M_{\alpha,\beta}(x,y,z)$$

disyunción sobre el número finito de pares (α, β) tal que $(q_\alpha, s_\beta, a, b) \in M$; si no existe alguna cuaterna, entonces $M(x,y,z) = F$.

Supongamos que f y g son funciones de estado tales que $[f] \overset{M}{\to} [g]$. Dado $r \in \mathbb{N}$, sea $u \in \mathbb{N}$ tal que $\text{seq}(u,i) = f(i)$ para $i = 0, 1, \ldots, r+2$. Si $k \in \mathbb{N}$, entonces $k = g(r)$ si y sólo si $\mathcal{T} \vdash M(u,r,k)$.

Lema 8.2.7. *Sea f una función de estado inicial (i.e., $f(0) = G(q_0)$) y sea $g(n,r)$ el valor en r de la función de estado después de n pasos en la computación de M iniciando en $[f]$. Entonces g es fuertemente definible en $\mathcal{T}$.*

Demostración. Sea

$$\varphi(x,y,z) = (\exists u)[(\forall v)(v \leq y + 2x \Rightarrow \text{seq}(\text{seq}(u,0), v) = f(v))$$
$$\wedge (\text{seq}(\text{seq}(u,x), y) = z) \wedge (\forall w)(\forall t)(((1 \leq w \leq x)$$
$$\wedge (t \leq y + 2(x-w))) \Rightarrow M(\text{seq}(u, w-1), t, \text{seq}(\text{seq}(u,w), t)))],$$

entonces $g(u,r) = k$ si y sólo si $\mathcal{T} \vdash \varphi(u,r,k)$. □

Observación. Sea f una función de estado inicial. Se puede expresar en términos de dos enteros, pues siempre podemos hallar $u, v \in \mathbb{N}$ tales que

$$f(x) = \begin{cases} \text{seq}(u,x) & \text{si } x \leq v, \\ G(s_0) & \text{si } x < v. \end{cases}$$

También se pueden sustituir u y v por un solo entero

$$w = P(u, v) \qquad \text{cuando} \quad u = L(w), \quad v = R(w)$$

Substituyendo f por u y v en φ, existe $\psi(u, v; x, y, z)$ que describe el comportamiento de M para cualquier entrada.

Observación. Sea M una máquina de Turing puesta a operar en el estado dado por (u, v), para en el estado de la función con valor z en y es

$$(\exists x)[\psi(u, v; x, y, z) \wedge (\forall x')(x' > x \Rightarrow (\forall t)(\sim \psi(u, v; x', y, t)))].$$

Teorema 8.2.8. *Sea $\mathcal{T} \supseteq \mathcal{N}_0$ una teoría que admite a $\mathbb{N}$ como modelo. Entonces toda función recursiva parcial es fuertemente definible en $\mathcal{T}$.*

Demostración. Adaptamos la función de estado a $\Psi_M^{(k,\ell)}$ y luego aplicamos los resultados anteriores. □

Observación. Si ρ es una relación en $\mathbb{N}$ tal que χ_ρ es recursiva, entonces es fuertemente definible en cualquier teoría $\mathcal{T} \supseteq \mathcal{N}_0$ que admite a $\mathbb{N}$ como modelo (Teorema 8.2.8). Entonces sea $\text{comp}(x_1, x_2, x_3)$ tal que "la máquina de Turing con número de Gödel x_1 aplicada al número x_2 computa x_3". Por el ejemplo dado para mostrar la insolubilidad del problema de parada, tenemos que

$$\{(\exists x)\,\text{comp}(n, n, x) : n \in \mathbb{N}\}$$

tiene un problema de decisión insoluble.

Teorema 8.2.9. *Sea $\mathcal{T} \supseteq \mathcal{N}_0$ una teoría que admite a $\mathbb{N}$ como modelo. Entonces $\mathcal{T}$ es indecidible. En particular $\mathcal{N}$ es indecidible.*

Demostración. Si $\mathcal{T}$ tuviera un proceso de decisión, entonces la familia $\{(\exists x)\,\text{comp}(n, n, x) : n \in \mathbb{N}\}$ tendrá un proceso de decisión. □

Teorema 8.2.10. *Sea $\mathcal{T} \supseteq \mathcal{N}_0$ una teoría efectivamente axiomatizada que admite a $\mathbb{N}$ como modelo. Entonces $\mathcal{T}$ es incompleta.*

Demostración. Si T es efectivamente axiomatizada y es completa, entonces $\mathcal{T}$ es decidible. Como $\mathcal{T} \supseteq \mathcal{N}_0$ y admite a $\mathbb{N}$ como modelo, entonces $\mathcal{T}$ es indecidible luego $\mathcal{T}$ es incompleta.

Sean $\mathcal{T} = (\mathcal{R}, A, C)$, $P = P(V, \mathcal{R})$, $G\colon P \to \mathbb{N}$ la función de Gödel y $F\colon G(P) \to P$ con $F = G^{-1}$ (G inyectiva). Definimos $\mathrm{dem}_{\mathcal{T}}(x_1, x_2)$ como la relación "x_2 es el número de Gödel de una demostración en $\mathcal{T}$ de $F(x_1)$", la cual es recursiva pues las demostraciones en $\mathcal{T}$ se pueden comprobar con una máquina de Turing.

Sea

$$\mathrm{teorema}_{\mathcal{T}}(x_1) = (\exists x_2)\,\mathrm{dem}_{\mathcal{T}}(x_1, x_2)$$

definido como "x_1 es el número de Gödel de un teorema de $\mathcal{T}$". Sea $w \in P$ y escribimos $w(x_0)$ si depende de x_0. Si $n \in \mathbb{N}$, entonces $n \in C$ luego $w(n) \in P$. Sea $\mathrm{sub}(n, w) = w(n)$ función de w y de n. La función $\varphi(m, n) = G(\mathrm{sub}(m, F(n)))$ para $m \in \mathbb{N}$, $n \in G(P)$ es una función recursiva parcial, luego existe $p(x_1, x_2, x_3) \in P$ tal que $\varphi(x_1, x_2) = x_3$.

Ahora pondremos

$$\pi(x_1, x_2) = (\exists x_3)(p(x_1, x_2, x_3) \wedge \mathrm{teorema}_{\mathcal{T}}(x_3)).$$

Escogemos w tal que $\mathrm{var}(w) \subseteq \{x_0\} \cup C$, entonces $w(m) \in \mathcal{L}(\mathcal{T})$ para todo $m \in \mathbb{N}$. Sea $n = G(w)$, entonces $\pi(m, n)$ es verdadera en $\mathbb{N}$ si y sólo si existe $a \in \mathbb{N}$ tal que $\varphi(m, n) = a$ y a es el número de Gödel de un teorema de $\mathcal{T}$. Como $\varphi(m, n) = G(w(m))$, entonces a es el número de Gödel de $w(m)$ y de un teorema. Por tanto, $\pi(m, n)$ es verdadero en $\mathbb{N}$ si y sólo si $\mathcal{T} \vdash w(m)$. Escogemos ahora $w(x_0) = \sim \pi(x_0, x_0)$ con $n = G(\sim \pi(x_0, x_0))$ y $q = w(n)$, entonces $\pi(n, n)$ es verdadero en $\mathbb{N}$ si y sólo si $\mathcal{T} \vdash q$. Pero $q = \sim \pi(n, n)$, luego $\mathcal{T} \vdash q$ si y sólo si q es falso en $\mathbb{N}$. Como $\mathbb{N}$ es modelo de $\mathcal{T}$, $\mathcal{T} \vdash q$ implica que q verdadera en $\mathbb{N}$. Luego, q no puede ser teorema un $\mathcal{T}$ así que q es verdadero en $\mathbb{N}$, entonces $\sim q$ no puede ser teorema de $\mathcal{T}$. Así que $q = \sim \pi(n, n)$ muestra la incompletitud de $\mathcal{T}$. □

Observación. Supongamos que $\mathcal{T}' \supseteq \mathcal{T}$ tal que $A' = A \cup \{q\}$, entonces substituimos

teorema$_{\mathcal{T}}(x_3)$ por teorema$_{\mathcal{T}'}(x_3)$ en la construcción anterior y tenemos el mismo resultado con un nuevo elemento q'. "Ninguna axiomatización efectiva de $\mathbb{N}$ puede dar lugar a una teoría completa."

8.3. Indecidibilidad del Cálculo de Predicados

Lema 8.3.1. *Sean $\mathcal{T}$, $\mathcal{T}'$ teorías y $\varphi\colon \mathcal{L}(\mathcal{T}) \to \mathcal{L}(\mathcal{T}')$ una función recursiva tal que para todo $p \in \mathcal{L}(\mathcal{T})$, se tenga que $\mathcal{T} \vdash p$ si y sólo si $\mathcal{T}' \vdash \varphi(p)$. Supongamos que $\mathcal{T}'$ es decidible. Entonces $\mathcal{T}$ es decidible.*

Demostración. Para mostrar que $\mathcal{T} \vdash p$ es suficiente hallar $\varphi(p)$ y un proceso de decisión para $\mathcal{T}'$. □

Lema 8.3.2. *Sea $\mathcal{N}_1$ la teoría formada a partir de la teoría $\mathcal{N}_0$ omitiendo las constantes y los axiomas e_n de identificación de constantes. Entonces $\mathcal{N}_1$ es indecidible.*

Demostración. Sea $n \in \mathbb{N}$ y definamos

$$e_n(x) = (\exists x_0)(\exists x_1)\cdots(\exists x_{n-1})(\theta(x_0) \wedge s(x_0, x_1) \wedge \cdots \wedge s(x, x_{n-1})).$$

Si $p \in \mathcal{L}(\mathcal{N}_0)$ entonces $\mathrm{var}(p) \subseteq \mathbb{N}$. Luego podemos hallar un elemento $p(x_1, \ldots, x_r) \in P(V \setminus \mathbb{N}, \mathcal{R})$ tal que existen $x_1, \ldots, x_r \in \mathbb{N}$ tal que $p = p(n_1, \ldots, n_r)$. Definamos $\varphi\colon \mathcal{L}(\mathcal{N}_0) \to \mathcal{L}(\mathcal{N}_1)$ por

$$p \longmapsto (\forall x_1)\cdots(\forall x_r)(e_{n_1}(x_1) \wedge \cdots \wedge e_{n_r}(x_r) \Rightarrow p(x_1, \ldots, x_r)).$$

Supongamos que $\mathcal{N}_1 \vdash \varphi(p)$, como $\mathcal{N}_0 \supseteq \mathcal{N}_1$, entonces $\mathcal{N}_0 \vdash \varphi(p)$. Como $e_{n_i}(n_i)$ es un axioma de $\mathcal{N}_0$ para todo i, entonces $\mathcal{N}_0 \vdash p(n_1, \ldots, n_r)$, i.e., $\mathcal{N}_0 \vdash p$.

Supongamos que $\mathcal{N}_0 \vdash p$, como para todo $n \in \mathbb{N}$ $\mathcal{N}_1 \vdash (\exists!x)e_n(x)$, entonces para todo $n \in \mathbb{N}$. Sea M un modelo de $\mathcal{N}_1$, entonces existe un único $m_n \in M$ tal que $M \vDash e(m_n)$; la aplicación $n \mapsto m_n$ hace que M sea un modelo de $\mathcal{N}_0$ donde $p(m_1, \ldots, m_r)$ es verdadero en M. Así $\varphi(p)$ es verdadero en todo modelo de $\mathcal{N}_1$, entonces $\mathcal{N}_1 \vdash \varphi(p)$. □

Lema 8.3.3. *Sea* $V = \{x_0, x_1, \dots\}$ *y* $\mathcal{R} = \{\rho\}$*, donde* ρ *es un símbolo de relación cuaternaria. Entonces* $\mathrm{Pred}(V, \mathcal{R})$ *es indecidible.*

Demostración. Consideremos primero una relación de identidad y axiomas en $\mathrm{Pred}(V, \mathcal{R})$. La teoría $\mathcal{N}_1$ sólo contiene un número finito de símbolos de relación, entonces el conjunto de los axiomas de sustitución de elementos es finito

$$(\forall x_1)\cdots(\forall x_n)[\mathcal{I}(x_j, y) \Rightarrow (r(x_1, \dots, x_n) \Rightarrow r(x_1, \dots, x_{j-1}, y, x_j, \dots, x_n))].$$

Entonces $\mathcal{N}_1$ tiene un número finito de axiomas de identidad, sea α la conjunción de estos axiomas.

Intuitivamente consideramos $\rho(x, y, z, t)$ como "$xy+z = t$" ($\mathrm{ar}(\rho) = 4$). Definamos un homomorfismo (de álgebras) $f\colon P(V, \mathcal{R})^{(1)} \to P(V, \mathcal{R})$ donde $\mathcal{R}^{(1)} = \{=, \theta, s, a, m\}$ tal que

$$\begin{aligned}
f(\theta(x)) &= p(x, x, x, x),\\
f(x = y) &= (\forall z)(\forall t)(\rho(z, z, z, z) \Rightarrow \rho(z, t, x, y)),\\
f(s(x, y)) &= (\forall z)(\forall t)[(\rho(z, z, z, z) \wedge (\forall n)\rho(t, u, z, u)) \Rightarrow \rho(t, y, t, x)],\\
f(a(x, y, z)) &= (\forall t)[(\forall u)(\forall v)(\rho(u, u, u, u) \Rightarrow \rho(t, v, u, v)) \Rightarrow \rho(t, x, y, z)],\\
f(m(x, y, z)) &= (\forall t)(\rho(t, t, t, t) \Rightarrow \rho(x, y, t, z)),
\end{aligned}$$

para todo $x, y, z \in V$. Definamos $g\colon P(V, \mathcal{R}^{(1)}) \to P(V, \mathcal{R})$ dada por $g(p) = f(a) \Rightarrow f(p)$.

Supongamos que $\mathcal{N}_1 \vdash p$. Aplicamos f a cada elemento de la demostración de p en $\mathcal{N}_1$ a partir de α, entonces tenemos una demostración de $f(p)$ a partir de $f(\alpha)$, luego $f(\alpha) \Rightarrow f(p)$ es un teorema. Recíprocamente, supongamos que $f(a) \Rightarrow f(p)$ es un teorema. Si M es un modelo de $\mathcal{N}_1$, entonces la interpretación $\rho(x, y, z, t)$ como "$xy + z = t$" proporciona una interpretación de $P(V, \mathcal{R})$ donde $f(\alpha)$ es verdadero. Luego $f(p)$ es verdadero pues $f(a) \Rightarrow f(p)$ es un teorema, luego p es verdadero en M por la interpretación de ρ por lo que $\mathcal{N}_1 \vdash p$. Así g hace que $\mathrm{Pred}(V, \mathcal{R})$ sea indecidible. □

Corolario 8.3.4 (Teorema de Church)**.** *Sea $\mathcal{R}^* = \{r_{ij} : i, j \in \mathbb{N}\}$ con r_{ij} un símbolo de relación i-aria, el alfabeto universal para las relaciones. Entonces* $\mathrm{Pred}(V, \mathcal{R}^*)$ *es indecidible.*

Demostración. La inclusión $P(V, \mathcal{R}) \to P(V, \mathcal{R}^*)$ hace que $\mathrm{Pred}(V, \mathcal{R}^*)$ sea indecidible. □

Lema 8.3.5. *Sea ρ una relación cuaternaria en el conjunto no vacío S. Pongamos $S' = \{K\} \cup S^2 \cup S^4$. Dado $x \in S$, definamos $\Delta(x) = (x, x) \in S'$. Sea r la relación binaria de S' consistente en aquellos pares (a, b) para los cuales es válida el menos una de las siguientes proposiciones:*

(a) *$a = (x, y)$, $b = (z, t)$, donde $x, y, z, t \in S$ y $x = y = z$ ó $y = z = t$,*

(b) *$a = (x, y)$, $b = (x, y, z, t)$ donde $x, y, z, t \in S$,*

(c) *$a = (x, y, z, t)$, $b = (z, t)$ donde $x, y, z, t \in S$,*

(d) *$a = K$, $b = (x, y, z, t)$ donde $(x, y, z, t) \in \rho$.*

Entonces los elementos de $\Delta(S)$, y de ρ, se pueden caracterizar en términos de r.

Demostración. Si $a \in S'$, entonces $a \in \Delta(S)$ si y sólo si $(a, a) \in r$.

`Afirmación`: $(x, y, z, t) \in S^4$ con $X = \Delta(x)$, $Y = \Delta(y)$, $Z = \Delta(z)$, y $T = \Delta(t)$; $(x, y, z, t) \in \rho$ si y sólo si existen $A, B, C, D \in S^1$ tales que (X, A), (D, Y), (Z, B), (B, T), (A, C), (C, B), $(D, C) \in r$, pero $(E, D) \notin r$ para todo E.

Observamos que para todo E $(E, D) \notin r$ entonces $D = K$. Entonces $(D, C) \in r$ si y sólo si $C \in \rho$; si $(C, B) \in r$ entonces B es el par final de C, si $(A, C) \in r$ entonces $A = K$ ó A es el par final de C. Como $(X, A) \in r$ entonces $A \neq K$, luego A es el par inicial de C. Luego $C = (x, y, z, t) \in \rho$. □

Teorema 8.3.6 (Teorema de Kalmar)**.** *Sea r un símbolo de predicado binario. Entonces* $\mathrm{Pred}(V, \{r\})$ *es indecidible.*

Observación. Si existe $r \in \mathcal{R}$ tal que $\mathrm{ar}(r) = 2$, entonces $\mathrm{Pred}(V, \mathcal{R})$ es indecidible.

Demostración. Sea

$$R(x,y,z,t) = (\exists a)(\exists b)(\exists c)(\exists d)[r(x,a) \wedge r(a,y) \wedge r(z,b) \wedge r(b,t) \\ \wedge r(a,c) \wedge r(c,b) \wedge r(d,c) \wedge (\forall c) \sim r(c,d)].$$

Sea $p \in P(V, \{\rho\})$ donde $\mathrm{ar}(\rho) = 4$. Si $\mathrm{var}(p) \neq \emptyset$, $\pi_p = \bigwedge\{r(x,x) : x \in \mathrm{var}(p)\}$. Si $\mathrm{var}(p) = \emptyset$, π_p no está definido. Definimos inductivamente $k(p)$

$$\begin{aligned} k(F) &= F, \\ k(\rho(x,y,z,t)) &= R(x,y,z,t) \qquad \text{para todo } x,y,z,t \in V, \\ k(q_1 \Rightarrow q_2) &= k(q_1) \Rightarrow k(q_2), \\ k((\forall x)q) &= (\forall x)(r(x,x) \Rightarrow k(q)). \end{aligned}$$

Ahora definimos $f\colon P(V, \{\rho\}) \to P(V, \{r\})$ por

$$f(p) = \begin{cases} \pi_p \Rightarrow k(p) & \text{si } \mathrm{var}(p) \neq \emptyset, \\ k(p) & \text{si } \mathrm{var}(p) = \emptyset. \end{cases}$$

Supongamos que $f(p)$ es un teorema.

Observación. La verdad o falsedad de p respecto de una interpretación depende sólo de la elección del conjunto S y de la relación ρ de S.

Construyamos S' y la relación r de S' como en el Lema. Sólo consideramos los elementos de $\Delta(S)$ por la definición de f. Luego p es verdadero en S si y sólo si $f(p)$ es verdadero en S'. Como $f(p)$ es un teorema en $P(V, \{r\})$, entonces p es verdadero en cualquier interpretación por lo que p es un teorema.

Recíprocamente, supongamos que p es un teorema, y sea $\{p_i\}_{i=1,\ldots,n}$ una demostración de p. (Inducción sobre n.) Supongamos que $f(p_1), \ldots, f(p_{n-1})$ son teoremas. Sea p un axioma, entonces $f(p)$ es un teorema. Si p resulta de p_i, p_j por MP, entonces $f(p)$ es deducible de $f(p_i)$ y $f(p_j)$ (Teorema de la Deducción). Supongamos que $p = (\forall x)q$ se haya obtenido por Generalización. Entonces $p_{n-1} = q$ y $f(q) = \pi_q \Rightarrow k(q)$ es un

teorema (si $\text{var}(q) = \emptyset$, $f(p)$ es un teorema), $\pi_q = \pi_p$ ó $\pi_q = \pi_p \wedge r(x,x)$ entonces $\pi_p \Rightarrow (r(x,x) \Rightarrow k(q))$ es un teorema, luego por Generalización $(\forall x)(\pi_p \Rightarrow (r(x,x) \Rightarrow k(q)))$, como $x \notin \text{var}(p)$ entonces $\pi_p \Rightarrow (\forall x)(r(x,x) \Rightarrow k(q))$ es un teorema, entonces $f(p)$ es teorema. □

Observación. Si R sólo contiene relaciones monarias, $\text{Pred}(V, \mathcal{R})$ es decidible.

Capítulo 9

Epílogo

Kurt Gödel, un nombre que será recordado por mucho tiempo, posiblemente hasta que alguien pueda lograr algún resultado que lo supere o invalide de cierta manera, ya sean decenas, cientos o miles de años (suposición no exagerada, tomando en cuenta que es considerado el más importante lógico desde Aristóteles).

Ya vimos algo de su historia y pudimos mostrar sus teoremas más reconocidos: el Teorema de Completitud de la lógica de Primer Orden (en el capítulo 4) y los Teoremas de Indecidibilidad e Incompletitud de la Aritmética (en el capítulo 8). Asimismo, vimos una extensión de su Teorema de Indecidibilidad debida a Alonzo Church y la generalización de László Kalmar (también en el capítulo 8), donde se muestra que el Cálculo de Predicados $Pred(V, \{r\})$ es indecidible con r siendo una relación de aridad mayor o igual a 2.

La importancia de estos teoremas demostrados es muy grande, teniendo repercusiones en todos los ámbitos de la Lógica Matemática, tanto así que en ningún libro de esta disciplina puede faltar alguna mención a los Teoremas de Gödel (de lo contrario sería considerado *Incompleto*). Asimismo, estos Teoremas fueron la inspiración de muchos otros resultados importantes transversales a varias disciplinas.

9.1. Entscheidungsproblem

Entscheidungsproblem es "El Problema de Decisión"que indica: ¿Existe un algoritmo (procedimiento finito) que decida si una proposición cualquiera en la lógica de primer orden es universalmente válida o no? (en toda estructura donde los axiomas supuestos son válidos)

Aclarando algunos términos de manera informal, ya que sus definiciones formales se encuentran en los capítulos precedentes:

- La definición de "procedimiento finito"es lo mismo que un "algoritmo", en matemática son las demostraciones en teorías axiomáticas, en informática son los programas. Históricamente os procedimientos finitos fueron estudiados por Aristóteles, Leibnitz, Descartes y Russell.
- Lógica de primer orden, que es básicamente la lógica matemática estudiada en cursos básicos universitarios, con cuantificadores (existe y para todo) que se refieren a variables simples.
- Proposiciones, que son secuencias correctamente ensambladas o "bien formadas"de variables, símbolos cuantificadores y conectivos lógicos.
- "Universalmente válida", significa que es verdadera para cualquier interpretación que se tenga (es decir independiente de quién la evalúe).
- Estructura axiomática es una colección de supuestos que estructuran las reglas de un sistema, es decir las "reglas de juego "de una teoría.

Históricamente, desde el griego Epiménides y el Rey David postulaban proposiciones cuyo análisis de veracidad ponía en duda el mismo procedimiento de realizar el análisis, ya que no podía determinarse si eran verdaderas o falsas (por ejemplo "Estoy mintiendo "o "Todo hombre es un mentiroso ", que son verdaderas si y solamente si son falsas). Posteriormente, para resolver de fondo estas proposiciones incómodas, Leibnitz propuso "construir una máquina que manipule símbolos para determinar los valores de verdad de las proposiciones matemáticas ", de esta manera sería objetivo el análisis de las proposiciones conflictivas.

Hilbert asumió como una tarea común a la comunidad matemática el reto de resolver el Problema de Decisión, como un pilar dentro de su sistema formalista y lo planteó claramente como el tercero de sus (muy famosos) 23 problemas más importantes del siglo XX. Junto con Ackerman señalaron el camino a seguir: "El problema de Decisión se resuelve si uno conoce un procedimiento que le permita decidir la validez (o satasfacibilidad) de una expresión lógica dada, mediante un número finito de operaciones."Estaban (casi) seguros que no deberían existir las proposiciones como la del mentiroso en Matemática.

Treinta años después del reto de Hilbert, Gödel prueba[1] la existencia de sentencias verdaderas en sistemas axiomáticos, que incluyen a la aritmética. que no se pueden probar ni refutar (indecidibles). Para ello definió formalmente las funciones recursivas e inventó los "números de Gödel (convirtiéndose en el desconocido y verdadero

[1]Hemos ejecutado la demostración formal en los capítulos previos

precursor de la era actual de la informática como veremos más adelante). Pero ¿cómo lo hizo?, veamos una sencilla receta:

- Tómense las sentencias, axiomas, proposiciones, demostraciones y teoremas
- Asígnese por isomorfismo un número natural a cada una (Números de Gödel)
- Constrúyase una proposición sobre la "demostrabilidad"de un teorema
- Tómese la negación de esta proposición - Diagonalícese con el número de Gödel de esta misma proposición (Diagonalización de Georg Cantor)
- La proposición resultante es: "Soy la prueba de que esta proposición no es demostrable"
- De manera equivalente: "Esta proposición es falsa"

Sin embargo queda realmente la pregunta sobre, si las proposiciones indecidibles (construidas conforme la receta anterior) dan una respuesta al problema de Decisión. La respuesta es NO, porque no muestran si existe o no un "procedimiento"para mostrar o no la validez de una proposición cualquiera. Es decir, el pedazo que falta en la torta completa de la prueba sería: ¿qué es un procedimiento o algoritmo? Tanto Alonzo Church como Alan Turing trabajaron en este tema con soluciones paralelas.

Church llegó a una solución en 1936 usando su famoso cálculo-lambda, sin embargo, fue Turing el primero en llegar a la respuesta correcta indicando que "EL PROBLEMA DE DECISIÓN NO TIENE SOLUCIÓN "ALAN TURING (1935)

Pero ¿cómo lo hizo?: usando la Máquina Universal de Turing para definir procedimientos (algoritmos) desde el punto de vista matemático. Una de estas máquinas (imposibles de construir físicamente) cuenta con una cinta infinita, un "sensor"de lectura, grabación y borrado y que cuenta con un número finito de estados internos.[2]

Análogamente al problema de Decisión se plantea el Problema de Parada (Halting Problem): "Dado un programa de computadora cualquiera, decidir si este programa termina de correr o si corre indefinidamente."

Puesto que: Si se resuelve negativamente el problema de parada, no existirá un procedimiento para determinar si una proposición es válida o no lo es, porque si tuviéramos este procedimiento, podemos aplicarlo al mismo problema de parada.

¿Pero como resolver el problema de parada?. Damos la siguiente receta:

[2]En el capítulo 7 se presenta un formalismo de estas Máquinas.

- Tómense todos los procedimientos (o algoritmos)
- Asígnese un número natural a cada uno (Números de Gödel)
- Constrúyase un algoritmo sobre la "No parada"de un algoritmo cualquiera
- Tómese la negación de este algoritmo
- Diagonalícese con el desglose binario de este mismo algoritmo (G.Cantor)
- El algoritmo resultante indica: "Este algorimo está fuera de la ennumeración inicial de algoritmos"
- De manera equivalente "Este algoritmo para determinar la continuidad (o parada) no existe"

Pues si,se trata de la misma receta de Gödel cambiando los ingredientes.

Posteriormente se demostraron una serie de equivalencias entre el cálculo-lambda de Church, las máquinas de Turing y las funciones recursivas de Gödel que despertaron la curiosidad de Church, quien postuló su famosa Tesis (también conocida como la Hipótesis de Church-Turing que permanece abierta) que indica: "Cualquier computación que puede ser llevada a cabo por medios mecánicos, puede ser realizada por una Máquina de Turing"o de manera equivalente:

"TODA FUNCIÓN EFECTIVAMENTE CALCULABLE ES COMPUTABLE"

Las preguntas que subyacen para que este problema esté abierto son: ¿Qué es una computación llevada a cabo por medios mecánicos? ¿Qué es una función efectivamente calculable?. La respuesta (casi) final es: Aceptemos la tesis, ya que estas nociones son intuitivas. La tesis es una proposición que caracteriza la naturaleza de la computación y no puede ser formalmente probada.

Gödel indicó que: "El concepto 'computable'es en cierto sentido absoluto (ya que no depende esencialmente en el sistema en que esté definido), mientras prácticamente todos los otros conceptos familiares Metamatemáticos dependen del sistema [donde fueron definidos]"

Durante varias décadas se han planteado muchos formalismos que describen la computabilidad efectiva, entre los que mencionamos:

- Máquinas o Algoritmos de Turing
- Cálculo Lambda (Church)
- Cadenas de Markov

- Funciones reconocibles (‘reckonable ’) de Kleene
- Funciones recursivas (Gödel)
- Funciones de Herbrand
- Sistemas canónicos (Post)
- Máquinas Post-Turing (Wang-Davis)
- Contadores Arriba-Abajo (Minsky)
- Modelo de máquina de conteo (Malzak-Lambek)
- Máquina apuntadora (Kolmogorov-Uspensky)

Asombrosamente se ha demostrado que TODOS estos son EQUIVALENTES.

Cabe mencionar el esfuerzo de dos matemáticos rusos que en los años 2000 trabajaron en base a la siguiente motivación de Gödel: “... puede ser posible ? postular un conjunto de axiomas que incorporen las propiedades generalmente aceptadas [de computabilidad] y hacer algo con esas bases.”

Gurevich y Deshowitz postularon una “prueba ”de la tesis de Church usando una axiomatización natural de la computabilidad, es decir construyendo una colección de axiomas que consideran ?naturales? que permiten definir formalmente lo que usualmente se conoce como algorimo.

Entre sus resultados tenemos los siguientes:

Definición: Un algoritmo es un sistema transicional de estados abstractos y complejidad acotada.
Teorema de representación: Para todo algoritmo existe una máquina de estados abstractos con los mismos estados y la misma función de transiciones.

9.2. Gödel y compiladores

Como fue señalado previamente, Alan Turing se basó en la forma del primer teorema de Indecidibildad de Gödel para probar la imposibilidad de solución del famoso “Problema de Parada ”, siendo posiblemente el resultado práctico más importante del siglo pasado, ya que las Máquinas de Turing fueron la base para la revolución de la Era del Computador, que seguimos viviendo en nuestros días.

Es aceptado generalmente, que Alan Turing es el precursor de la Era del Computador, sin embargo, Martin Davis en [Davis, 2000] afirma que realmente es Kurt GÓdel, pero no solamente por haber tenido la idea original del tipo de prueba antes mencionada, sino, porque la base real de la implementación efectiva en computadores de un algoritmo cualquiera recae en el "Compilador", que es básicamente el traductor entre el lenguaje usual de las personas, con las operaciones que realizan los computadores.

Como se vio en la sección anterior y en capítulo 7, Kurt Gödel inventó los Números de Gödel, formados de tal manera que los procesos de demostración pueden ser reflejados entre Sistemas Lógicos y Sistemas Numéricos, de ida y vuelta. Este proceso es exactamente lo que se requiere de un Compilador. A continuación una traducción libre de parte de la sección "Kurt Gödel, Programador de computadoras"en [Davis, 2000]:

> En 1930 la realización de un dispositivo físico actual que pueda funcionar como una computadora programable, de propósito general y procesadora de información estaba aun décadas en el futuro. Aun así, cualquiera que actualmente tenga conocimiento sobre los lenguajes modernos de programación, leyendo el documento de Gödel sobre indecidibilidad escrito en ese año, verá una secuencia de 45 fórmulas que se ven muy similares a un programa de computadora. Esta similitud no es accidental. Al demostrar que la propiedad de ser el código de una prueba en PM [3] es expresable dentro de PM, Gödel tuvo que lidiar con muchos de los mismos problemas que encaran las personas que diseñan lenguajes de programación y aquellas que escriben programas en esos lenguajes. Al nivel fundamental, las computadoras contemporáneas pueden realizar solamente operaciones básicas en cadenas cortas de 0s y 1s. Diseñadores de los llamados "lenguajes de alto nivel"encaran la tarea de proveer a los programadores con locuciones que encapsulen las altamente complejas operaciones con las que quisieran ellos trabajar. Para que los programas escritos usando estas locuciones sean aceptados por una computadora, ellos deben ser traducidos en lenguaje de máquina - en un listado detallado de las operaciones básicas que se necesitan para ejecutarlos. Esto es realizado por programas especializados de traducción, denominados *intérpretes* o *compiladores* [4].

[3] Cualquier sistema relacionado similar a Principia Mathematica de Russell y Whitehead.

[4] Un *intérprete* funciona traduciendo los pasos de un programa uno por uno en lenguaje de máquina y ejecutando actualmente cada paso, antes de proceder al siguiente. Un *compilador* traduce un programa entero en lenguaje de máquina. El programa en lenguaje de máquina así producido puede correr como un objeto independiente, sin necesidad posterior del compilador. Casi todo el software comercial es generado por compiladores.

Martin Davis, gran lógico y pionero en sistemas informáticos, basa mucha de su obra en Gödel, como él mismo lo menciona en [Davis, 2000] y en [Davis, 1982], ya que una de las conferencias que le "influyó profundamente en sus propias visiones sobre los fundamentos de las matemáticas ", fue la que asistió en 1951, en Providence, Rhode Island de la American Mathematical Society, donde Kurt Gödel disertó sobre *Algunos teoremas básicos en los Fundamentos de Matemáticas y sus Implicaciones.*

Históricamente, Gödel fue el primero en crear un mecanismo de Compilación, aunque muy formal y poco práctico para implementarlo en sistemas electrónicos, efectivamente fue el primer esquema de mapeo que permitió transformar el lenguaje y los modelos básicos de razonamiento en cálculos numéricos, haciendo que a su vez los resultados de los cálculos coincidan perfectamente con las deducciones lógicas a partir de las premisas inicialmente introducidas.[5]

9.3. Smullyan y Tarski

Existen formas más abstractas de probar los resultados de Gödel, entre los más importantes desarrollaremos de manera rápida y sencilla las formas desarrolladas por Raymond Smullyan y la interpretación realizada por el mismo Smullyan de los importantes Teoremas de Tarski sobre la Artimética, que forman parte de sus estudios sobre la "Verdad Matemática".[6]

Para la presente sección seguiremos el primer capítulo de [Smullyan, 1992], en una traducción libre.

El Teorema de Tarski para la Aritmética indica que el conjunto de números de Gödel de las sentencias Aritméticas verdaderas, no puede ser definido con lógica de primer orden usando operaciones de suma, producto y potenciación.

la forma abstracta del Segundo Teorema de Gödel conforme Smullyan indica que: Si suponemos que un Sistema Axiomático $\mathcal{S}$ es diagonalizable (se puede aplicar el proceso general de Diagonalización de Cantor), en este caso, si suponemos que $\mathcal{S}$ es

[5]Asimismo, se debe mencionar el gigante aporte de John Von Neumann, quien no solamente fue (posiblemente) el primero en entender a cabalidad las implicaciones del Primer Teorema de Indecidibilidad de Gödel (llegando inmediatamente al Segundo Teorema de Gödel), sino también elaborando la primera arquitectura de sistemas informáticos basadas en Máquinas de Turing, que efectivamente funcionaron desde los computadores ENIAC

[6]Estudios que hasta la fecha son considerados los más importantes referentes para Lógicos, Matemáticos y Filósofos.

Consistente, entonces la sentencia $consis(\mathcal{S})$ (que prueba la Consistencia de $\mathcal{S}$) no puede ser demostrable en $\mathcal{S}$.

A continuación se expondrá brevemente la construcción de las formas abstractas de el Primer Teorema de Gödel y el Teorema de Tarski para la Aritmética:

9.3.1. Preliminares

Estudiaremos los lenguajes $\mathcal{L}$ en los que se aplican Los siguientes items:

- Un conjunto numerable $\mathcal{E}$, cuyos elementos se llaman *expresiones* de $\mathcal{L}$.
- Un subconjunto $\mathcal{S}$ de $\mathcal{E}$ cuyos elementos se llaman las *sentencias* de $\mathcal{L}$.
- Un subconjunto $\mathcal{P}$ de $\mathcal{S}$ cuyos elementos se llaman las sentencias *demostrables* de $\mathcal{L}$.
- Un subconjunto $\mathcal{R}$ de $\mathcal{S}$ cuyos elementos se llaman las sentencias *refutables* (también denominadas sentencias *no demostrables*) de $\mathcal{L}$.
- Un conjunto $\mathcal{H}$ de expresiones cuyos elementos se llaman *predicados* (que pueden ser entendidos informalmente como nombres de conjuntos de números naturales).
- Una función Φ que asigna a cada expresión E y a cada número natural n una expresión $E(n)$. Esta función es requerida para obedecer la condición que para cada predicado H y cada número natural n, la expresión $H(n)$ es una sentencia (informalmente la sentencia $H(n)$ expresa la proposición que el número n pertenece al conjunto nombrado por H).
- Un conjunto $\mathcal{T}$ de sentencias cuyos elementos se llaman las sentencias *verdaderas* de $\mathcal{L}$.

Definición 9.3.1. Decimos que un predicado H es *verdadero* para un número n o que n *satisface* H si $H(n)$ es una sentencia verdadera (es un elemento de $\mathcal{T}$). Un conjunto está *expresado* por H si está formado por todos los n que satisfagan H. De esta manera, para cualquier conjunto A de números naturales, H expresa A si y solo si para todo número natural n:

$$H(n) \in \mathcal{T} \Leftrightarrow n \in A$$

Definición 9.3.2. Un conjunto A se llama *expresable* o *nombrable* en $\mathcal{L}$ si A es expresado para algún predicado de $\mathcal{L}$.

Como hay solamente una cantidad numerable de expresiones de $\mathcal{L}$, entonces solamente pueden existir una cantidad finita o numerable de predicados de $\mathcal{L}$. Sin embargo, por el Teorema de la cardinalidad del conjunto potencia de Cantor, existe una cantidad infinita no numerable de conjuntos de números naturales. Por tanto, no todo conjunto de números naturales es expresable en $\mathcal{L}$.

Definición 9.3.3. El sistema[7] $\mathcal{L}$ se llama *correcto* si toda sentencia demostrable es verdadera y si toda sentencia refutable es falsa (no verdadera). Esto significa que $\mathcal{P} \subset \mathcal{T}$ y que $\mathcal{R} \cap \mathcal{T} = \emptyset$

9.3.2. Forma Abstracta del Teorema de Gödel

Nos interesan conocer las condiciones suficientes para que $\mathcal{L}$, siendo correcto, contenga una sentencia verdadera y no demostrable en $\mathcal{L}$.

Definición 9.3.4. Sea g una función inyectiva que asigne a cada expresión E un número natural $g(E)$ llamado *el número de Gödel* de E [8]. Técnicamente, suponemos que todo número natural es un número de Gödel de alguna expresión. Con estas premisas, cada número natural n es el número de Gödel de una única expresión, denotemos E_n a esa expresión, de manera que $g(E_n) = n$.

Definición 9.3.5. Entendemos por *diagonalización* de E_n la expresión $E_n(n)$.

Si E_n es un predicado, entonces su diagonalización es una sentencia. Esta sentencia es verdadera si y solo si su propio número de satisface el predicado E_n.

Definición 9.3.6. Para cualquier número natural n sea $d(n)$ el número de Gödel de $E_n(n)$, así $d(n) = g(E_n(n))$. Llamamos a la función d la *diagonal* del sistema.
Sea A un conjunto de números naturales, el conjunto A^* formado por todos los números naturales n tales que $d(n) \in A$. De donde, para todo n tenemos la equivalencia

[7] Denominamos sistema al Lenguaje junto con los items previamente mencionados.

[8] Se aclara que la función g permanece abstracta, no es construida y es parte del sistema $\mathcal{L}$.

inmediata de la definición de A^*:

$$n \in A^* \Leftrightarrow d(n) \in A$$

Sea P el conjunto de números de Gödel de todas las sentencias demostrables. Para cualquier conjunto de números naturales A, sea $\tilde{\text{A}}$ el complemento de A respecto de los números naturales.

Teorema 9.3.7. [9] *[Forma abstracta del teorema de Gödel] Si el conjunto $\tilde{P}^*$ es expresable en $\mathcal{L}$ y $\mathcal{L}$ es correcto, entonces existe una sentencia verdadera de $\mathcal{L}$, pero no demostrable en $\mathcal{L}$.*

9.3.3. Forma Abstracta del Teorema de Tarski

Se observa que la verificación que $\tilde{\text{P}}^*$ es expresable en $\mathcal{L}$ se obtiene a continuación de las siguientes tres condiciones independientemente:

G1: Para cualquier conjunto A expresable en $\mathcal{L}$, el conjunto A^* es expresable en $\mathcal{L}$.

G2: Para cualquier conjunto A expresable en $\mathcal{L}$, el conjunto $\tilde{\text{A}}$ es expresable en $\mathcal{L}$.

G3: El conjunto P es expresable en $\mathcal{L}$.

Definición 9.3.8. Llamamos a una sentencia E_n una *sentencia Gödel* para un conjunto A de números naturales si se cumple alguna de las siguientes:

a) E_n es verdadera y su número de Gödel está en A.

b) E_n es falsa (no es verdadera) y su número de Gödel no está en A.

Así, E_n es una sentencia de Gödel para A si y solo si se cumple la siguiente condición:

$$E_n \in \mathcal{T} \Leftrightarrow n \in A$$

Se puede pensar, informalmente, que una sentencia de Gödel para A es una sentencia que afirma que su propio número de Gödel reside en A. La sentencia es verdadera si y solo si su número de Gödel está en A.

[9] En esta sección no incluiremos las demostraciones de los teoremas, que se pueden obtener de [Smullyan, 1992].

Lema 9.3.9 (Lema Diagonal)**.** *a) Para cualquier conjunto de números naturales A, si A^* es expresable en $\mathcal{L}$, entonces existe una sentencia de Gödel para A.*

b) Si $\mathcal{L}$ satisface la condición G1, entonces, para cualquier conjunto de números naturales A expresable en $\mathcal{L}$, existe una sentencia de Gödel para A.

Teorema 9.3.10 (Forma abstracta del Teorema de Tarski)**.** *Sea T el conjunto de los números de Gödel de las sentencias verdaderas en $\mathcal{L}$, entonces:*

a) El conjunto $\tilde{T}^*$ no es expresable en $\mathcal{L}$.

b) Si se cumple la condición G1, entonces $\tilde{T}$ no es expresable en $\mathcal{L}$.

c) Si ambas condiciones G1 y G2 se cumplen, entonces el conjunto T no es expresable en $\mathcal{L}$.

Parafraseando el punto c) del teorema de Tarski, podemos indicar: Para sistemas suficientemente potentes (que cumplen G1 y G2), la "verdad en el sistema"no es definible dentro del sistema.

9.3.4. La forma dual del argumento de Gödel

Definición 9.3.11. El sistema $\mathcal{L}$ se llama *consistente* si ninguna sentencia es demostrable y refutable simultáneamente en $\mathcal{L}$ (es decir que $\mathcal{P} \cap \mathcal{R} = \emptyset$) y se llama *inconsistente* en caso contrario.

Se observa que si $\mathcal{L}$ es correcto, entonces es automáticamente consistente, ya que $\mathcal{P} \subset \mathcal{T}$ y $\mathcal{T} \cap \mathcal{R} = \emptyset$. El recíproco no es necesariamente cierto.

Definición 9.3.12. Una sentencia X es llamada *decidible* en $\mathcal{L}$ si es o demostrable o refutable en $\mathcal{L}$, se llama *indecidible* en otro caso.
El sistema $\mathcal{L}$ se llama *completo* si toda sentencia es decidible en $\mathcal{L}$ y se llama *incompleto* si alguna sentencia es indecidible en $\mathcal{L}$.

Teorema 9.3.13 (Forma abstracta del Teorema de Incompletitud de Gödel)**.** *Si $\mathcal{L}$ es correcto y el conjunto $\tilde{P}^*$ es expresable en $\mathcal{L}$, entonces $\mathcal{L}$ es incompleto.*

Sea R el conjunto de números de Gödel de las sentencias refutables.

Teorema 9.3.14 (Forma dual del argumento de Gödel)**.** *Si $\mathcal{L}$ es correcto y el conjunto R^* es expresable en $\mathcal{L}$, entonces $\mathcal{L}$ es incompleto. Específicamente, si $\mathcal{L}$ es correcto y K es un predicado que expresa al conjunto R^*, entonces su diagonalización $K(k)$ es indecidible en $\mathcal{L}$ (con k el número de Gödel de K).*

9.4. Algunos resultados basados en ideas de Gödel

Entre una pleyade de autores que siguen de manera muy cercana a Gödel y basan sus resultados en sus ideas, trataremos sobre tres que se destacan por diferentes motivos, en áreas bastante separadas, son Gregory Chaitin, Roger Penrose y Kenneth Arrow, quienes expresan resultados disímiles pero muy interesantes, que se siguen de los argumentos de Gödel.

Los resultados que se presentan en esta sección, se extraen de los libros [Chaitin, 1998], [Penrose, 1994] y [Barrow, 1998], con traducción libre, tomando en cuenta que el contexto de los resultados de GÓdel fueron explicados previamente en diferentes secciones.

9.4.1. Chaitin y la probabilidad de parada

Como preámbulo a los resultados de Chaitin, se presenta los comentarios del mismo Chaitin sobre otro de los resultados importantes en Matemática: el problema X (décimo) de Hilbert de los 23 problemas para ser resueltos en el siglo XX, propuestos en el Congreso Internacional de Matemáticos del año 1900, este problema fue resuelto por Matijasevič en los años 1970, indicando que es imposible.

El problema indica: Encontrar un algoritmo que determine si una ecuación diofántica polinómica dada con coeficientes enteros tiene solución entera.

Al respecto los comentarios de Chaitin, que también son un buen preámbulo para sus resultados:

> Matijasevič mostró que existe una ecuación diofántica polinómica con un parámetro, con la siguiente propiedad: Se varía el parámetro y se pregunta si la ecuación tiene solución. Resulta que este resultado es equivalente al problema de parada resuelto por Turing [10] y en consecuencia escapa

[10] Considerado en detalle en la sección Entscheidungsproblem del Capítulo 9 y en el Capítulo 7

del poder del razonamiento matemático y del razonamiento axiomático formal.

¿Cómo difiere esto de lo que hace Chaitin?. Este último usa una ecuación diofántica exponencial, que permite el uso de variables en los exponentes, Matijasevič solo permite exponentes constantes. La gran diferencia reside en que Hilbert buscaba la existencia de un algoritmo que determine si una ecuación diofántica tiene una solución. La pregunta que se hace Chaitin para obtener aleatoriedad en teoría de números elemental, en la aritmética de los números naturales, es algo más sofisticada. En lugar de preguntar si existe una solución, Chaitin plantea si existe un número finito o infinito de soluciones - una pregunta más abstracta.

La ecuación de Chaitin de más de 200 páginas es construida de manera que tiene un número finito o infinito de soluciones, dependiendo si un bit particular de la probabilidad de parada[11] es 0 o 1. Si se varía el parámetro, se obtiene un bit individual de Ω. La ecuación de Matijasevič es construida de manera que tiene solución si y solo si un programa particular para, con cada variación del parámetro se obtiene un particular programa computacional.

De esta manera, inclusive en aritmética se puede encontrar la absoluta falta de estructura de Ω, su aleatoriedad e información matemática irreducible. Hasta el mismo razonamiento es impotente en esas áreas de la aritmética, la ecuación de Chaitin muestra este punto. Chaitin usó las ideas que comenzaron con el documento original de 1931 de Gödel, sin embargo el documento de Matijasevič y Jones de 1984 le proporcionaron las herramientas que necesitaba.

Por estos motivos, Chaitin afirma que existe aleatoriedad en ña teoría de números elemental, en la misma aritmética de los números naturales. Esta es una pared impenetrable, es el peor escenario. De Gödel se sabe que no podemos hacer que un sistema axiomático demuestre su propia completitud. Se sabía que existían dificultades y Turing se encargó de mostrar cuan básicos eran, sin embargo Ω es un caso extremo donde el razonamiento falla completamente.

La ecuación de Matijasevič brinda N preguntas aritméticas con respuestas si/no que resultan ser solamente $logN$ bits de información algorítmica. La

[11] Un poco más adelante definiremos los conceptos de probabilidad de parada y de Ω

ecuación de Chaitin brinda N preguntas aritméticas con respuestas si/no, que son información matemática irreducible y no comprimible.

A continuación las definiciones que quedaban pendientes, explicadas de manera bastante informal por el propio Chaitin:

¿Qué exactamente es la probabilidad de parada?. Chaitin escribe una expresión para definirla[12]:

$$\Omega = \sum_{p\ para} 2^{-|p|}$$

En lugar de buscar programas individuales y preguntar si paran, se colocan todos los programas computacionales en una bolsa. Si se genera un programa computacioal aleatoriamente lanzando una moneda para cada bit del programa, ¿cuál es la posibilidad de que este programa pare?. Se consideran los programas como secuencias de bits y se genera cada bit por un lanzamiento independiente de una moneda legítima, así, si un programa tiene N bits de largo, entonces la probabilidad de que se obtenga ese programa particular es 2^{-N}. Cualquier programa p que pare contribuye en $2^{-|p|}$, dos a la menos su tamaño en bits (el número de bits en el programa), a la probabilidad de parada.

Existe un detalle técnico que es muy importante. La siguiente expresión no depurada resulta infinito:

$$\Omega = \sum_{p\ para} 2^{-|p|}$$

Por este motivo, Chaitin tuvo que restringir a los programas válidos p tales que sus extensiones no son programas válidos. de esta manera se tiene que:

$$0 < \Omega = \sum_{p\ para} 2^{-|p|} < 1$$

De lo contrario, resulta que Ω es infinito, tomó 10 años a Chaitin en lograr este resultado, desde los años 1960 cuando montó la teoría de información algorítmica, hasta 1974 año en que consideró programas "auto delimitantes", para luego descubrir la probabilidad de parada Ω.

La idea es que se genera cada bit de un programa lanzando una moneda y preguntar cuál es la probabilidad de que este programa pare. Este número Ω, la probabilidad de parada, no es solamente un real no computable (Turing ya sabía cómo generar estos números reales). Es no computable en la peor forma posible.

[12]Aclarando que p son programas computacionales (Máquinas de Turing)

9.4.2. Penrose y el pensamiento Platónico

El gran científico Roger Penrose fue ampliamente influenciado por Gödel, como menciona en varios párrafos de sus libros, en particular en su importante obra (de más de 450 páginas) [Penrose, 1994], inclusive los puntos de vista y filosofía personal Platónica quedan enmarcados en las visiones comunes que ambos sostienen, podemos ver esto en los siguientes fragmentos de la obra citada, con una traducción libre. Es importante mencionar que Penrose sentó las bases de los espacios Twistor y otros resultados matemáticos importantes, con los cuales Stephen Hawking pudo desarrollar sus conocidas teorías.

Se debe aclarar que uno de los aspectos más importantes del pensamiento platónico se basa generalmente en la famosa "cueva de Platón"[13], que describe pictóricamente los mundos físico y de las percepciones. Penrose amplía esta alegoría con un mundo adicional, el de las *formas matemáticas*:

> El mundo que conocemos más directamente es el *mundo de nuestras percepciones conscientes*, sin embargo es el mundo que menos conocemos en términos científicos. Este mundo contiene felicidad y dolor, y la percepción de los colores. Contiene nuestras memoras de nuestra niñez temprana y nuestro miedo a la muerte. Contiene amor, entendimiento, y el conocimiento de numerosos hechos, así como ignorancia y venganza. Es un mundo que contiene imágenes mentales de sillas y mesas, y donde los olores, sonidos, sensaciones de todo tipo se mezclan con nuestros pensamientos y nuestras decisiones para actuar.
>
> Existen dos otros mundos de los que estamos conscientes - menos directamente que el mundo de las percepciones - pero de los cuales conocemos bastante. Uno de estos mundos es el llamado *mundo físico*. Este mundo contiene sillas y mesas actuales, televisores y automóviles, seres humanos, cerebros humanos, y las acciones de las neuronas. En este mundo está el sol, la luna y las estrellas. También están nubes, huracanes, flores, mariposas y rocas; y en un nivel más profundo están las moléculas y átomos, electrones y protones, y el espacio-tiempo. También contiene citoesqueletos, diámeros de tubulina y superconductores. No está del todo claro

[13]Se trata de una explicación metafórica, realizada por el filósofo griego Platón al principio del VII libro de la República, sobre la situación en que se encuentra el ser humano respecto del conocimiento.? En ella, Platón explica su teoría de cómo podemos captar la existencia de los dos mundos: el mundo sensible (conocido a través de los sentidos) y el mundo inteligible (sólo alcanzable mediante el uso exclusivo de la razón).

> porqué el mundo de nuestras percepciones tenga algo que ver con el mundo físico, pero aparentemente lo hace.
>
> Hay también un otro mundo, cuya existencia actual muchos encuentran difícil de aceptar: *el mundo de las formas matemáticas*. Allí, encontramos los números naturales: 0,1,2,3,..., y el álgebra de números complejos. Encontramos el Teorema de Lagrange: que todo número natural es la suma de cuatro cuadrados. Encontramos el teorema Pitagórico de Geometría Euclidiana (sobre los cuadrados de los lados en un triángulo rectángulo). Allí se encuentra la proposición que indica que para cada par de números naturales, axb=bxa. En este mismo mundo Platónico está el hecho de que este último resultado no se mantiene para algunos otros tipos de números (por ejemplo con el producto Grasmaniano). Este mismo mundo Platónico contiene geometrías diferentes a la Euclidiana, en las cuales el Teorema Pitagórico falla. Contiene números infinitos y números no computables, además de ordinales recursivos y no recursivos. Allí existen acciones de Máquinas de Turing que nunca se detienen así como máquinas Oráculo. Están allí muchos tipos de problemas matemáticos que son insolubles computacionalmente, como el problema de embaldosado de poliominós. También en este mundo están las ecuaciones electromagnéticas de Maxwell así como las ecuaciones gravitacionales de Einstein e innumerables espacios-tiempos teóricos que las satisfacen - Sean físicamente realistas o no. Allí están las simulaciones matemáticas de sillas, mesas, como podrían ser usadas en "realidad virtual", y también simulaciones de agujeros negros y huracanes.

Es interesante la visión filosófica que Penrose tiene, construida a partir de los resultados de Gödel, sobre la cual realizó bastantes estudios físicos y biológicos, llegando a postular una teoría de la mente, basada en Gödel, como se puede apreciar en otra sección de [Penrose, 1994]:

> En la parte I [14], estuve muy inmerso en algunas de las implicaciones del famoso teorema de incompletitud de Gödel. Algunos lectores podrían opinar que el teorema de Gödel nos indica que existen partes del mundo de las verdades matemáticas Platónicas que en principio yacen más allá del entendimiento humano y su percepción. Espero que mis argumentos hayan dejado claro que este *no* es el caso [15]. Las proposiciones matemáticas específicas que el ingenioso argumento de Gödel proveen son aquellas

[14] La parte I del libro [Penrose, 1994] titula "Porqué necesitamos nueva Física para entender La Mente"

[15] Mostowski (1975), en la introducción de su libro, coloca claramente que los argumentos como los de Gödel no tratan las cuestiones de si existen a su vez preguntas matemáticas *absolutamente*

> accesibles a los humanos - siempre que sean construidas desde sistemas (formales) Matemáticos que previamente fueron aceptados como maneras válidas de acceder a verdades matemáticas. Los argumentos de Gödel no sostienen la existencia de verdades matemáticas inaccesibles. Sin embargo, si sostienen que la percepción humana yace más allá de los argumentos formales y más allá de los procedimientos computacionales. Más aun, sostiene fuertemente la existencia misma del mundo matemático Platónico. La verdad matemática no está determinada arbitrariamente por las reglas de cierto sistema formal "hecho-por-el-hombre", ella tiene una naturaleza absoluta, estando más allá de cualquier sistema con reglas específicas. El soporte hacia el punto de vista Platónico (en contraposición del formalista) fue una parte importante de las motivaciones iniciales de Gödel. Por otra parte, los argumentos del teorema de Gödel sirven para ilustrar la profunda y misteriosa naturaleza de nuestras percepciones matemáticas. Nosotros no solo "calculamos"para formar estas percepciones, algo más está profundamente inmerso - que sería imposible sin nuestra realización consciente, que realmente es el mundo de las percepciones.

9.4.3. El teorema de imposibilidad de Arrow

La presente sección presenta un resultado de imposibilidad original en el área de ciencia política debida a Kenneth Arrow, quien en 1972 ganó el premio Nobel de Economía, gracias en parte a este Teorema. A continuación una traducción libre de una parte de la sección correspondiente a Arrow en [Barrow, 1998]:

> Arrow quería acortar camino a través del vasto contenido de diferentes sistemas de votación, aislando las características esenciales de cualquier sistema democrático, para descubrir si existiesen condiciones bajo las cuales la intransitividad pueda ser evitada [16]. Él asumió que las preferencias individuales satisfacen dos reglas simples:
>
> (a) *Comparabilidad de alternativas.* Si existen dos alternativas, x e y, entonces se cumple que x es preferido antes que y o que y es preferido antes que x. Esto requiere que las alternativas tengan alguna propiedad en común que pueda usarse para comparar su valor. Los empates no son permitidos en preferencias individuales.

indecidibles. El problema debe quedar completamente abierto, por ahora, en cuanto a lo que se pueda probar o refutar (...).

[16]Se entiende *intransitividad* a la paradoja de la elección racional basada en el hecho que: si A es preferido antes que B y B es preferido antes que C, no signifique que A es preferido antes que C.

(b) *Transitividad* Elecciones individuales por votantes son consistentes en su orden de preferencia; esto es, si x es preferido antes que y e y es preferido antes que z, entonces necesariamente, x es preferido antes que z. Se debe notar que se está tratando de determinar si esta propiedad será o no compartida por la decisión colectiva de los votantes.

El último paso fue elegir características definitorias de la elección democrática, que serían deseables por cualquier elección social derivada de muchas elecciones individuales que se deben respetar. Se eligen las siguientes cinco:

Condición 1 *Libertad irrestricta de la elección individual.* A cada votante individual se le permite elegir cualquier orden posible de los candidatos. No existen organizaciones que puedan prevenir cualquier preferencia expresada por los votantes.

Condición 2 *La elección social debe positivamente reflejar las elecciones individuales.* Si la elección social es de tal forma que x es preferida a y, además no hay individuos que cambian su preferencia, entonces x debe mantenerse socialmente preferida ante y. Esto asegura que el método de totalización de los votos individuales para obtener la elección colectiva no sea perversa.

Condición 3 *Alternativas irrelevantes no deben tener efectos.* El orden social de algún subconjunto de elecciones no es alterada por los cambios en el orden de otras posibilidades que no estén en ese subconjunto.

Condición 4 *La voz de las personas cuenta.* El resultado de la elección no es impuesta. La preferencia social no puede ser des-relacionada de las preferencias de los votantes individuales. Esto previene que la elección social sea impuesta hacia la sociedad desde afuera, por ejemplo, por alguna creencia religiosa.

Condición 5 *No dictaduras.* No existe individuo de manera que la preferencia de este individuo siempre determine la preferencia social general. Esto previene que la elección social sea impuesta hacia la misma sociedad desde adentro, por un individuo.

El propósito de estas condiciones es permitir un examen riguroso de las consecuencias de muchos posibles enlaces entre las preferencias individuales y colectivas, enmarcado solamente por restricciones justas y razonables que la mayoría de los miembros de la sociedad las consideren deseables, si no esenciales, para la elección democrática. De manera significativa, Arrow probó que: *si las elecciones individuales son finitas en número, y obedecen las reglas (a) y (b) entonces no existe un método para combinar*

las preferencias individuales para producir una elección social que cumpla todas las condiciones 1 a la 5.
Todo método de construir una elección social que satisfaga las condiciones 1 a la 3, o viola las condiciones a la 5 o contraviene las reglas (a) o (b). Notese que la intransitividad social no surge de ninguna intransitividad de preferencias individuales, porque ellas están explicitamente prohibidas por la regla (b). Si las condiciones democráticas 1 a la 5 y a son satisfechas, entonces debe existir intransitividad en el resultado. No existe algo como consenso social.

9.4.4. Hofstadter, bucles extraños

La fantástica y extensa obra de Douglas Hofstadter ganadora del premio Pulitzer "Gödel Escer Bach - An eternal golden braid"[Hofstadter, 1979] [17], amalgama gran cantidad de ideas, conceptos y conocimiento sobre *Bucles extraños* o *Strange Loops*, que se podrían entender como autoreferencias asimétricas recursivas, aunque cada lector de las más de 770 páginas tendrá su propia interpretación.

Como una muestra de la importancia que tienen los resultados de Gödel en el contexto del libro mencionado, a continuación, se presenta una traducción libre de las partes importantes sobre la visión general que aparece en la vigésima edición:

Parte I: GEB:

Introducción: Una ofrenda lógico-musical. El libro abre con la historia de *La ofrenda musical* de Bach. Bach realizó una *impronta* visita al Rey Federico el Grande de Prusia, y se le requirió improvisar sobre un tema presentado por el Rey. Sus improvisaciones formaron la base de una gran obra. La *Ofrenda Musical* y su historia forman un tema sobre el cual Hofstadter "improvisa"a lo largo del libro, haciendo una surte de "Ofrenda Metamusical". Se discuten la autoreferencia y la interacción entre diferentes niveles en Bach; lo que lleva a una discusión de ideas en los dibujos de Escher y luego el Teorema de Gödel. Una breve presentación de la historia de la lógica y las paradojas se presenta como preámbulo para el Teorema de Gödel. Esto conduce al razonamiento mecánico y computadoras, y al debate sobre si la (verdadera) Inteligencia Artificial es posible. Se cierra la introducción con una explicación de los orígenes del libro - particularmente, el porqué y el motivo de los Diálogos.[18]

[17]Traducida como Gödel, Escher y Bach - Un eterno y grácil bucle.

[18]Se aclara que se dejan de lado la referencia a la mayoría de los diálogos que aparecen luego de los correspondientes resúmenes de los capítulos, ya que no tienen relevancia para el presente trabajo.

Capítulo I: El acertijo MU. Es presentado un sistema formal simple (el sistema MIU), donde se insta al lector a trabajar el acertijo para ganar familiaridad con los sistemas formales en general. Una cantidad de nociones fundamentales se introducen: cadena, axioma, teorema, regla de inferencia, derivación, sistema formal, procedimiento de decisión, trabajar dentro/fuera del sistema.

Chapter II: Significado y forma en Matemáticas. Se presenta un nuevo sistema formal (el sistema pq), incluso más simple que el sistema MIU del Capítulo I. En apariencia sin sentido al inicio, repentinamente se revela que sus símbolos tienen significado, en virtud de la forma de los teoremas en los que aparecen. Esta revelación es la primera noción importante del significado: su conexión profunda con el isomorfismo. Luego se discuten varios temas relacionados con el significado , como son verdad, prueba, manipulación de símbolos, y el concepto elusivo de "forma".

Capítulo III: Figura y Motivo. La distinción de figura y motivo en arte se compara con la distinción entre teoremas y no-teoremas en sistemas formales. La pregunta "¿Puede una figura necesariamente tener la misma información que su motivo?"lleva a la distinción entre conjuntos recursivamente enumerables y conjuntos recursivos.

Capítulo IV: Consistencia, Completitud y Geometría. El diálogo precedente[19] es explicado conforme es posible hasta este punto. Esto lleva de nuevo a la pregunta de cómo y cuándo los símbolos de los sistemas formales adquieren significado. Se presenta la historia de las Geometrías Euclidianas y No-Euclidianas, como una ilustración de la noción elusiva de "términos indefinidos". Esto conduce a ideas sobre la consistencia de geometrías diferentes y posiblemente "rivales". A través de esta discusión se clarifica la noción de términos indefinidos, y se considera la relación de los términos indefinidos con la percepción y los procesos mentales.

[19] *Contracrostipunto.* Este Diálogo es central para el libro, pues contiene un conjunto de paráfrasis de la construcción auto-referente de Gödel y de su Teorema de Incompletitud. Una de las paráfrasis del Teorema indica "Para cada tocadiscos existe un disco que no puede tocar."El título del diálogo es un cruce entre las palabras "acróstico"y "contrapunto", una palabra Latina que Bach usaba para denotar las muchas fugas y cánones que hacen su *Arte de la Fuga*. Aparecen algunas referencias explícitas al *Arte de la Fuga*. El Diálogo mismo oculta algunos trucos acrósticos.

Capítulo V: Estructuras Recursivas y Procesos. La idea de recursividad se presenta en muchos contextos diferentes: patrones musicales, patrones lingüísticos, estructuras geométricas, funciones matemáticas, teorías físicas, programas computables y otros.

Capítulo VI: La Ubicación del Significado. Una amplia discusión sobre cómo el significado se divide entre el mensaje codificado, el decodificador y el receptor. Los ejemplos presentados incluyen cadenas de ADN, inscripciones no descifradas en tablillas antiguas y grabaciones fonográficas que navegan por el espacio. Se postula una relación entre inteligencia y significado "absoluto".

Capítulo VII: El Cálculo Proposicional. Se sugiere cómo las palabras como "y"pueden ser gobernadas por reglas formales. Nuevamente surgen las ideas de isomorfismo y adquisición automática de significado por los símbolos del sistema. Todos los ejemplos de este capítulo, incidentalmente, son "Zentencias", - sentencias tomadas de los kõans Zen[20]. Esto es hecho a propósito, de alguna manera irónicamente, puesto que los kõans Zen son historias deliberadamente ilógicas.

Capítulo VIII: Teoría de Números Tipográfica. Se presenta una extensión del Cálculo de Proposiciones, denominado "TNT". En TNT, el razonamiento en teoría de números puede ser realizada con manipulaciones inflexibles de símbolos. Se consideran diferencias entre el razonamiento formal y el pensamiento humano.

Capítulo IX: Mumon y Gödel. Se realiza un intento de hablar sobre las extrañas ideas del Budismo Zen. El monje Zen Mumon, quien realizó reconocidos comentarios en varios kõans, es una figura central. De cierta manera, las ideas Zen sostienen una reminiscencia metafórica a algunas ideas contemporáneas en la filosofía de las Matemáticas. Luego de esta "es-Zena", la idea fundamental de Gödel sobre la numeración de Gödel es introducida, y se hace una primera pasada por el Teorema de Gödel.

Parte II: EGB

Capítulo X: Niveles de Descripción y Sistemas de Computadoras. Se discuten varios niveles de cuadros visuales, tableros de ajedrez y

[20]Acertijo o anécdota paradójicas usadas en el Budismo Zen para probar la insuficiencia del razonamiento lógico y provocar ilustración.

sistemas de computadoras. El último de los cuales es examinado en detalle. Esto incluye describir lenguajes de máquinas, lenguajes ensambladores, lenguajes compiladores, sistemas operativos y otros tantos. Luego la discusión se torna hacia los sistemas compuestos de otros tipos, como equipos deportivos, núcleos, átomos, el clima y otros. Surge la pregunta de cómo existen niveles intermedios - o inclusive si ellos existen.

Capítulo XI: Cerebros y Pensamientos. "¿Cómo pueden los pensamientos ser soportados por el hardware del cerebro?"es el tema del Capítulo. Se den primero una vista general de las escalas macro y microscópicas del Cerebro. Luego se discute especulativamente sobre la relación entre conceptos y actividad neuronal, con cierto detalle.

Capítulo XII: Mentes y Pensamientos. Los poemas previos traen forzosamente la pregunta sobre si los lenguajes, o inclusive mentes, pueden ser "mapeadas"unas en otras. ¿Cómo es posible la comunicación entre dos cerebros físicamente separados? ¿Qué es lo que todos los cerebros humanos tienen en común? Se sugiere una respuesta con una analogía geográfica. Surge la pregunta, "¿Puede un cerebro ser comprendido, en algún sentido objetivo, por una persona independiente?".

Capítulo XIII: Bloop y FlooP y Gloop. Estos son los nombres de tres lenguajes de computación. Los programas Bloop solo pueden llevar a cabo búsquedas predecibles finitas, mientras los programas Floop pueden llevar a cabo búsquedas no predecibles o incluso infinitas. El propósito de este capítulo es brindar nociones intuitivas sobre recursividad primitiva y funciones recursivas generales en teoría de números, pues son esenciales en la prueba de Gödel.

Capítulo XIV: Sobre Proposiciones Indecidibles en TNT y Sistemas Relacionados. El título de este capítulo es una adaptación del título del artículo de Gödel de 1931, en el cual su Teorema de Incompletitud fue publicado por primera vez. Las dos grandes partes de la prueba de Gödel son cuidadosamente revisadas. Se muestra cómo la presuposición de consistencia de TNT fuerza a concluir que TNT (o cualquier sistema similar) es incompleto. Se discuten las relaciones con Geometría Euclidiana y No-Euclidiana. Se ingresan con cierto cuidado las implicaciones para la Filosofía de las Matemáticas.

Capítulo XV: Saltando fuera del sistema. Se muestra la repetibilidad del argumento de Gödel, con la implicación que TNT no es solo

incompleto, sino "esencialmente incompleto". Es analizado el ampliamente notorio argumento de J.R.Lucas que indica que el efecto del Teorema de Gödel demuestra que el pensamiento humano no puede en ningún sentido ser "mecanizado".

Capítulo XVI: Auto-Ref y Auto-Rep. Este capítulo trata de la conexión entre la auto-referencia es sus varios matices, y las entidades auto-reproducibles (por ejemplo: programas de computadora o moléculas de ADN). Se discuten las relaciones entre una entidad auto-reproducible y los mecanismos que le son externos y que le ayudan en reproducirse a si mismo (por ejemplo una computadora o proteínas) - particularmente la característica difusa de la distinción. El tópico central de este Capítulo es cómo viaja la información Entre varios niveles de tales sistemas.

Capítulo XVII: Church, Turing, Tarski y otros. El cangrejo de ficción de los diálogos pasados es reemplazado por varias personas reales, con sorprendentes habilidades matemáticas. Se presenta la Tesis de Church-Turing, que relaciona la actividad mental con la computación, en varias versiones con diferentes intensidades. Todas son analizadas, particularmente en términos de sus implicaciones para simular el pensamiento humano mecánicamente o programar en una máquina la habilidad de sentir, o crear belleza. La conexión entre la actividad mental y la computación genera otros tópicos: el Problema de Parada de Turing y el Teorema de la Verdad de Tarski.

Capítulo XVIII: Inteligencia Artificial: Retrospectivas. Este capítulo abre con la discusión de la famosa "Prueba de Turing"- una propuesta del pionero en computación Alan Turing sobre una manera de detectar la presencia o ausencia de "pensamiento"en una máquina. De allí se toma la reducida historia de la Inteligencia Artificial. Se cubren programas que - de cierta manera - juegan juegos, pruebas teoremas, resuelven problemas, componen música, hacen matemática y usan "lenguajes naturales"(Por ejemplo el Inglés).

Capítulo XIX: Inteligencia Artificial: Prospectos. Se dispara una discusión sobre cómo el conocimiento es representado en capas de contextos. Esto lleva a la idea moderna en Inteligencia Artificial de "marcos". Se presenta una forma de manejar un conjunto de acertijos visuales con esta idea de marcos, con el propósito de ser concretos. Luego se discute el profundo asunto de la interacción de conceptos en general, lo que lleva a ciertas especulaciones sobre la creatividad. El Capítulo concluye con un

conjunto de "Preguntas y Especulaciones"del autor sobre la Inteligencia Artificial y las mentes en general.

Capítulo XX: Bucles extraños, o jerarquías enredadas. Una gran conclusión de muchas de las ideas sobre sistemas jerárquicos y autoreferencia. Se refiere a las marañas que surgen cuando giramos hacia nosotros mismos - por ejemplo, cuando la ciencia prueba a la misma ciencia, el gobierno investigando sus propios malos manejos, el arte violando las reglas del arte, y finalmente, humanos pensando sobre sus propios cerebros y mentes. ¿Tiene el Teorema de Gödel algo que decir sobre esta última "maraña"? ¿Están conectados el libre albedrío y la sensación de conciencia con el Teorema de Gödel? El capítulo termina juntando nuevamente a Gödel, Escher y Bach.

9.4.5. Interpretando los resultados de Gödel

La transcendencia de los resultados de Gödel incluye relaciones con la física, la filosofía y la ciencia en general, en el libro "Imposibilidad, los límites de la ciencia y la ciencia de los límites"[21] de John Barrow, [Barrow, 1998], se presenta una interesante interpretación con un contexto físico, en una traducción libre:

El aspecto Kafkiano del trabajo de Gödel y su carácter se expresa en su famoso Teorema de Incompletitud... Los científicos quedamos en una posición similar a Kafka en "El Castillo". Sin fin, corriendo arriba y abajo a través de corredores, encontrando personas, tocando puertas, conduciendo nuestras investigaciones. Pero el logro final nunca será nuestro. En ningún lugar en el castillo de la ciencia existirá una salida final hacia la absoluta verdad. (Rudy Rucker)

La monumental demostración de Gödel sobre los límites de los sistemas matemáticos se infiltró gradualmente en la forma en que los filósofos y científicos ven el mundo y nuestra búsqueda por entenderlo. Superficialmente, parece que todas las investigaciones humanas sobre el Universo deben estar limitadas. La ciencia se basa en matemáticas; las matemáticas no pueden descubrir todas las verdades; entonces la ciencia no puede descubrir todas las verdades. Así es como iba el argumento. Comentadores con alguna apologética religiosa en mente aprovecharon los límites al poder del razonamiento humano que Gödel implicó. Uno de los contemporáneos de Gödel y estudiante de Hilbert, Hermann Weyl, describió el

[21] Traducción libre

descubrimiento de Gödel como ejercitar un 'drenar constante del entusiasmo'con el que él persiguió su investigación científica. Él creyó que su pesimismo subyacente, muy diferente al grito de guerra con el cual Hilbert se refirió a los matemáticos en 1900, era compartido 'por otros matemáticos que no eran indiferentes a lo que significaban sus esfuerzos científicos, en el contexto del completo cuidado y conocimiento, sufrimiento y existencia creativa en el mundo. 'En tiempos recientes, un escritor frecuente sobre teología y ciencia, Stanley Jaki, cree que Gödel nos impide ganar conocimiento del cosmos como una verdad necesaria,

Entonces claramente, ninguna cosmología científica, que necesariamente debe ser altamente matemática, puede tener su propia prueba dentro de sí misma, en lo que respecta a la matemática. En ausencia de esta consistencia, todos los modelos matemáticos, todas las teorías de partículas elementales, incluida la teoría de quarks y gluones... se quedan cortas en ser las teorías que muestren en virtud de sus verdades a priori que el mundo solo puede ser lo que es y nada más. Esto es verdad incluso si la teoría logra describir perfectamente todos los fenómenos del mundo físico que se conozcan en una época particular.

Jaki también ve el teorema de incompletitud de Gödel como una barrera fundamental para entender el Universo:

Considerando la fuerza del teorema de Gödel, parece ser que las fundaciones últimas de las enérgicas construcciones de la física matemática, permanecerán por siempre estocadas en este profundo nivel de pensamiento caracterizado por la sabiduría y la confusión de las analogías y las intuiciones. Para el físico especulativo, esto implica que existen límites en la precisión de la certeza, que incluso en el pensamiento puro de los físicos teóricos existe una frontera... Una parte integral de esa frontera es el científico mismo, como pensador...

Los teoremas de incompletitud Gödel han sido citados en tantos contexos, que el sueco Torkel Franzén ha publicado un libro [Franzén, 2005], titulado "Una guía incompleta del uso y abuso del Teorema de Gödel"[22] donde detalla centenas de interpretaciones que se han dado en varios ámbitos sobre los famosos teoremas previamente mencionados, inclusive varios de los autores que se mencionan en el presente trabajo están citados en su libro.

[22]Traducción libre.

A continuación citas del libro [Franzén, 2005], que permitirán aterrizar y contextualizar algunas de las interpretaciones que se dan de los famosos teoremas:

Escepticismo:

En ocasiones se considera que el Teorema de Incompletitud brinda alguna forma de soporte al escepticismo sobre las matemáticas. Se argumenta que , estrictamente hablando, o no podemos probar nada en matemáticas o que la consistencia de teorías como la Aritmética de Peano (AP) o Zermelo- Frankel (ZF) se muestran que están en duda por el teorema.

En muchos casos, no se brinda explicación sobre cómo la conclusión escéptica se supone que se deduce. Así, la Encyclopedia Britannica indica misteriosamente que la prueba de Gödel:
... establece que dentro de cualquier sistema rígido lógico-matemático existen proposiciones (o preguntas) que no pueden ser probadas o refutadas con base en los axiomas internos en ese sistema y que, por tanto, no está claro que los axiomas básicos de la aritmética no llevarán a contradicciones.

Un aspecto particular de este comentario lateral (que es actualmente prestado de la *Historia de las Matemáticas* de Carl Boyer y Uta Merzbach), es la abrupta conclusión desde la incompletitud a la posible inconsistencia, que no tiene aparentemente bases racionales y no es siquiera sugerido en el artículo. De manera similar, encontramos comentarios como:
Por el Teorema de Gödel, un sistema es o incompleto o inconsistente. Así, lógicamente hablando, es imposible para nosotros "probar "completamente ninguna proposición.

En estos extractos la ocurrencia de frases como "lógicamente hablando", es una notoria característica de muchas y alarmantes conclusiones inválidas[23], inspiradas en el teorema de incompletitud.

Las conclusiones escépticas basadas en el trabajo de Gödel, cuando se acompañan de un argumento inteligible, usualmente invocan específicamente el segundo teorema de incompletitud. Así, Nagel y Newmann indican que Gödel prueba:
... que es imposible establecer la consistencia lógica interna de una clase muy grande de sistemas deductivos - por ejemplo la aritmética elemental -

[23]Estas conclusiones inválidas, incurren en la falacia *Non sequitur* (no se sigue).

a menos que uno adopte principios de razonamiento tan complejos que su consistencia interna está abierta a dudas, tanto como los sistemas mismos.

Otros comentaristas van más lejos. Morris Kline en *Matemáticas: La pérdida de la certidumbre*, establece que "el resultado de Gödel en consistencia indica que no podemos probar la consistencia en ninguna aproximación a las matemáticas por principios lógicos seguros."

Existen dos ingredientes principales en esas reflexiones: la idea de que la consistencia de alguno o todos los sistemas formales que usamos en matemáticas es *dudosa*, y la idea de que la consistencia de esos sistemas no puede ser *probada* en el mismo sentido que otras sentencias matemáticas pueden ser probadas. Para tener una perspectiva de estas ideas, comenzaremos con el asunto de la duda.

La no relevancia del Teorema de Gödel frente a las dudas:

Nada en el Teorema de Gödel de ninguna manera contradice la visión de exista la duda sobre la consistencia de cualquiera de los sistemas formales que usamos en matemática. En efecto, nada en el Teorema de Gödel es de ninguna manera incompatible con la aseveración de que tenemos conocimiento certero de las verdades de los axiomas en esos sistemas, y por ende, de su consistencia.

Al considerar este punto, debemos distinguir entre dos cosas: el grado justificable o razonable de escepticismo o de confianza acerca de los axiomas matemáticos o métodos de razonamiento, y lo que tiene que ver el Teorema de Gödel en este asunto. Posiblemente tengamos una pobre visión sobre la afirmación de que sabemos con absoluta certeza la verdad de, digamos, los axiomas de ZFC[24], pero ¿cómo podemos usar el Teorema de Gödel para observar esta afirmación? ¿Podemos orientar el reclamo hacia una observación decisiva sobre si nosotros sabemos con absoluta certeza que los axiomas de ZFC son verdaderos, entonces la consistencia de ZFC debe ser demostrable en el mismo ZFC? No, porque esta no es para nada una observación decisiva. ¿Porqué debería existir una prueba de la consistencia de ZFC en ZFC solo porque sabemos con absoluta certeza que los axiomas de ZFC son verdaderos (y por tanto consistentes)? Obviamente, no podemos probar todo en matemáticas. No necesitamos del Teorema de

[24]La Teoría de Conjuntos de Zermelo Frankel con el Axioma de Elección (ZFC - Zermelo Frankel Choice)

> Gödel para saber que debemos adoptar ciertos principios sin prueba. Y dado que los axiomas de ZFC son absolutamente convincentes, tan obviamente ciertos en el mundo de los conjuntos, no podemos hacer algo mejor que adoptar estos axiomas como nuestro punto de partida. Puesto que los axiomas son verdaderos, también son consistentes.
>
> Nuevamente, el punto a tratar no es si está justificada esa visión de los axiomas de ZFC, sino si tiene sentido apelar al teorema de incompletitud para objetarlos. Si los axiomas de ZFC con manifiestamente verdaderos, ellos son obviamente consistentes, aunque no exista razones para esperar una prueba de consistencia de ZFC en el mismo ZFC.
>
> Desde el punto de vista del escéptico sobre la consistencia de ZFC, en una inspección más cercana, tampoco está claro cuál sería la relevancia del segundo teorema de incompletitud. ¿Cuál sería el interés de brindar una prueba de consistencia de ZFC en el mismo ZFC? Puesto que la consistencia de ZFC es precisamente lo que se está cuestionando, no hay motivo para esperar que esta prueba tenga algún peso.
>
> Así, si no tenemos dudas sobre la consistencia de ZFC, no hay nada en el segundo teorema de incompletitud para que surjan dichas dudas. Y, si tenemos dudas sobre la consistencia de ZFC, no tenemos motivos para creer que una prueba de consistencia de ZFC, formalizable en ZFC pueda hacer nada para disipar dichas dudas.

Como pudimos observar, es muy importante la precisión de los conceptos que se tratan en el trabajo de Gödel para que pueda ser adecuadamente interpretado y aplicado en cualquier disciplina del conocimiento.

Gödel mismo, comentó lo siguiente sobre las consecuencias del segundo teorema de incompletitud:

> Es *este* teorema (el segundo teorema de Incompletitud) el que hace particularmente evidente la no completabilidad de las matemáticas. Pues, *hace imposible que alguien pueda armar un sistema bien definido de axiomas y reglas, simultáneamente haciendo de forma consistente la siguiente aseveración sobre él: Yo percibo (con certidumbre matemática) que todos estos axiomas y reglas son correctas, y más aun creo que contienen a todas las matemáticas.* Si alguien realiza tal aseveración se contradice a sí mismo. Pues si percibe que los axiomas en consideración son correctos, también

percibe (con la misma certeza) que ellos son consistentes. Por lo tanto, tiene una percepción matemática que no deriva de sus axiomas.[25]

9.5. Conclusiones

Para finalizar el presente trabajo, como conclusiones y cierre me permito postular lo siguiente:

- Kurt Gödel será por siempre reconocido en la historia por cambiar los conceptos básicos de la lógica y remover los cimientos de la matemática, a tal punto que sus efectos se sienten hasta en la filosofía.
- El punto anterior devela claramente al autor del presente trabajo como "Gödeliano"(sea lo que sea que este término inventado pueda significar).
- Para el presente trabajo se tuvieron dos grandes objetivos: Exponer los Teoremas de Completitud e Incompletitud de Gödel e impulsar el desarrollo del área de Lógica Matemática.
- Sobre la prueba del primer objetivo, la lectura del presente trabajo por parte del amable lector es la muestra más fehaciente, sin embargo no deja de ser particular. La exposición tiene en términos generales los mismos tres componentes que una comunicación: Un emisor, un medio y un receptor. Considero que la autoreferencia del autor al momento de escribir estas líneas como primer componente , la autoreferencia de las líneas al momento de ser parte del presente documento como segundo componente y la autoreferencia del amable lector al momento de leerlas como tercer componente, completan la prueba buscada.
- Sobre el segundo objetivo, el presente trabajo solamente es un grano de arena en la búsqueda del desarrollo de la Lógica Matemática, si bien tiene una extensión suficiente como para lograr cierto avance y su desarrollo usando lógica (recursivamente) algebraica permite un interés puramente matemático, hay mucho camino que recorrer, con la participación activa del emisor y el receptor (ver el punto anterior).
- Los agradecimientos nunca son suficientes como se pudo apreciar en la correspondiente sección, aunque el esfuerzo de exhaustividad es notorio en esa sección, si bien (paradójicamente) insuficiente.
- La conclusión final necesaria, luego de las disgresiones anteriores, es sencilla: la profunda admiración al genio de KURT GÖDEL.

[25] Gödel, *Collected Works*, Vol III, p.309, así lo indica Barrow en [Barrow, 1998].

Bibliografía

[Ale, 1967] (1967). *Diccionario Práctico - Alemán Castellano y Castellano Alemán*. Brevis Duplex. Editorial Sopena Argentina.

[Arbib and trad Eva Sánchez, 1987] Arbib, M. A. and trad Eva Sánchez (1987). *Cerebros, Máquinas y Matemáticas*. Alianza Universidad, 2nd edition.

[Avigad, 2005] Avigad, J. (2005). Incompleteness via the halting problem.

[Barnes and trad. Xambó Descamps, 1978] Barnes, D. W. and trad. Xambó Descamps, J. M. M. (1978). *Una Introducción Algebraica a la Lógica Matemática*. EUNIBAR - Editorial Universitaria de Barcelona.

[Barrow,] Barrow, J. D. Gödel and physics.

[Barrow, 1998] Barrow, J. D. (1998). *Impossibility. The limits of Science and the Science of limits*. Oxford University Press.

[Birkhoff and trad Rafael Rodríguez, 1953] Birkhoff, G. and trad Rafael Rodríguez, A. M. (1953). *Álgebra Moderna*. Editorial Vicens-Vives, 2nd edition.

[Bocheński and trad. Rodolfo Fernández, 1976] Bocheński, J. and trad. Rodolfo Fernández (1976). *Compendio de Lógica Matemática*. Ed. Paraninfo.

[Boole and trad. Esteban Requena, 1979] Boole, G. and trad. Esteban Requena (1979). *El Análisis Matemático de la Lógica*. Colección Teorema. Cátedra.

[Bourbaki and trad. Jesús Hernández, 1976] Bourbaki, N. and trad. Jesús Hernández (1976). *Elementos de Historia de las Matemáticas*. Alianza Universidad, 2nd edition.

[Cattabriga, 2007] Cattabriga, P. (2007). Observations concerning gödelÅ> 1931.

[Chaitin, 1998] Chaitin, G. J. (1998). *The Limits of Mathematics*. Springer.

[Chaitin, 1999] Chaitin, G. J. (1999). *The Unknowable*. Springer.

[Chaitin, 2001] Chaitin, G. J. (2001). *Exploring Randomness*. Springer.

[Cohn, 1981] Cohn, P. M. (1981). *Universal Algebra*. D.Reidel Publishing Company.

[Cole, 1998] Cole, K. (1998). *The Universe and the Teacup*, volume The Mathematics of Truth and Beauty. Harcourt Brace Co.

[Davis, 1982] Davis, M. (1982). *Computability and unsolvability*. Dover Publications Inc.

[Davis, 2000] Davis, M. (2000). *The Universal Computer*. W.W.Norton Company.

[Dubreil and trad.R.Rodriguez, 1965] Dubreil, P. and trad.R.Rodriguez, M.-L. D.-J. (1965). *Lecciones de Álgebra Moderna*. Editorial Reverté S.A.

[Espanola, 2001] Espanola, R. A. (2001). *Diccionario de la Lengua Española*. Espasa, 22th edition.

[Feys and trad Guillermo Rosique, 1980] Feys, R. and trad Guillermo Rosique, F. B. F. (1980). *Los Símbolos de la Lógica Matemática*. Lógica y Teoría de la Ciencia. Paraninfo.

[Franzén, 2005] Franzén, T. (2005). *Gödel's Theorem. An Incomplete Guide to it's Use and Abuse*. A.K. Peters Ltd.

[Frege and trad. Luis Valdés, 1984] Frege, G. and trad. Luis Valdés (1984). *Investigaciones Lógicas*. Cuadernos de Filosofía y Ensayo. Editorial Tecnos S.A.

[Gödel and trad. B.Hirzel, 2000] Gödel, K. and trad. B.Hirzel (2000). On formally undecidable propositions of principia mathematica and related systems i.

[Gödel and trad. B.Meltzer, 1992] Gödel, K. and trad. B.Meltzer (1992). *On Formally Undecidable Propositions of Principia Mathematica and Related Systems*. Dover Books.

[Gödel and trad. Jesús Mosterín, 1989] Gödel, K. and trad. Jesús Mosterín (1989). *Obras Completas*. Alianza Universidad, 2nd edition.

[Goldstein, 2005] Goldstein, R. (2005). *Incompleteness. The Proof and Paradox of Kurt Gödel*. Atlas Books.

[Gómez, 2010] Gómez, J. (2010). *Matemáticos Espías y Piratas Informáticos*, volume Codificación y Criptografía of *National Geographic - El mundo es Matemático*. RBA Contenidos Editoriales y Audiovisuales,S.A.U.

[Haack and trad. Amador Antón, 1991] Haack, S. and trad. Amador Antón (1991). *Filosofía de las Lógicas*. Catedra, Teorema, 2nd edition.

[Halmos and trad. Antonio Martin-Lunas, 1966] Halmos, P. R. and trad. Antonio Martin-Lunas (1966). *Teoría Intuitiva de los Conjuntos*. Compañía Editorial Continental, México, 3rd edition.

[Hawking,] Hawking, S. Gödel and the end of physics.

[Hersh, 1997] Hersh, R. (1997). *What is Mathematics, Really?* Oxford University Press.

[Hilbert and trad.Víctor Sánchez, 1975] Hilbert, D. and trad.Víctor Sánchez, W. A. (1975). *Elementos de Lógica Teórica*. Editorial Tecnos, 2nd edition.

[Hillis, 1998] Hillis, W. D. (1998). *The Pattern in the Stone*. Science Masters. Basic Books.

[Hilton and trad. María Paz Bujanda, 1977] Hilton, P. and trad. María Paz Bujanda, Y.-C. W. (1977). *Curso de Álgebra Moderna*. Editorial Reverté S.A.

[Hintikka, 2000] Hintikka, J. (2000). *On Gödel*. Wadsworth Philosophers Series. Wadsworth Thompson Learning.

[Hofstadter, 1979] Hofstadter, D. R. (1979). *Gödel, Escher, Bach: an Eternal Golden Braid*. Basic Books, 20th anniversary edition.

[Holt, 1997] Holt, J. (1997). Hypotheses - the loophole.

[I.N.Herstein and trad. Federico Velasco, 1980] I.N.Herstein and trad. Federico Velasco (1980). *Álgebra Moderna*. Biblioteca de Matemática Superior. Editorial Trillas, 5th edition.

[Jack J. Bulloff and Hahn, 1969] Jack J. Bulloff, T. C. H. and Hahn, S., editors (1969). *Syposium Papers Commemorating the Sixtieth Birthday of Kurt Gödel*. Foundations of Mathematics. Springer-Verlag.

[Jansana, 1990] Jansana, R. (1990). *Una Introducción a la Lógica Modal*. Editorial Tecnos.

[J.N Crossley, 1988] J.N Crossley, C.J. Ash, C. B. J. S. N. W. t. J. A. (1988). *Qué es la Lógica Matemática?* Cuadernos de Filosofía y Ensayo. Editorial Tecnos S.A.

[Kleene, 2000] Kleene, S. C. (2000). *Introduction to Metamathematics*. Bibliotheca Mathematica. North-Holland, 13th edition.

[K.Podnieks, 1992] K.Podnieks (1992). Around the gödelÅ› theorem. Platonism, intuition and the nature of mathematics.

[Lahoz-Beltra, 2012] Lahoz-Beltra, R. (2012). *Turing - La Computación*, volume Pensando en Máquinas que Piensan of *Grandes Ideas de la Ciencia*. RBA Contenidos Editoriales y Audiovisuales,S.A.U.

[Lakatos and trad.Diego Ribes, 1987] Lakatos, I. and trad.Diego Ribes (1987). *Matemáticas, Ciencia y Epistemología*, volume 2 of *Philosophical Papers*. ALianza Universidad.

[Laki,] Laki, S. L. A late awakening to gödel in physics.

[Manaster, 1975] Manaster, A. B. (1975). *Completeness, Compactness ans Undecidability. An introduction to Mathematical Logic*. Prentice-Hall, Inc.

[Mendelson, 1964] Mendelson, E. (1964). *Introduction to Mathematical Logic*. The University Series in Undergraduate Mathematics. D. Van Nostrand Company, Inc., 2nd edition.

[Myers,] Myers, D. Godel's incompleteness theorem.

[Nagel and R.Newman, 1969] Nagel, E. and R.Newman, J. (1969). *La Demostración de Gödel*, volume Estructura Lógica, Arte, El Matemático of *SIGMA - El Mundo de las Matemáticas*. Ediciones Grijalbo S.A., 8th edition.

[Nagel and R.Newmann, 1960] Nagel, E. and R.Newmann, J. (1960). *GödelÅ› Proof*. New York University Press.

[neiro, 2012] neiro, G. D. P. (2012). *Gödel Los teoremas de incompletitud*, volume La intuición tiene su Lógica of *Grandes Ideas de la Ciencia*. RBA Contenidos Editoriales y Audiovisuales,S.A.U.

[Penrose, 1994] Penrose, R. (1994). *Shadows of the mind*. Oxford University Press. A search for the missing science of consciousness.

[Rylov, 2007] Rylov, Y. A. (2007). Gödel's theorem as a corollary of the impossibility of complete axiomatization of geometry.

[Shanker, 1988] Shanker, S. G., editor (1988). *Gödel's Theorem in Focus*. Croom Helm.

[Smith, 2005] Smith, P. (2005). *An introduction to Gödel's Theorems*. University of Cambdirge.

[Smullyan, 1987] Smullyan, R. (1987). *Forever Undecided. A puzzle guide to Gödel*. Oxford University Press.

[Smullyan and trad. Carmen García, 1978] Smullyan, R. and trad. Carmen García (1978). *Cómo se llama este libro?* Colección Teorema. Cátedra, 12th edition.

[Smullyan, 1992] Smullyan, R. M. (1992). *Gödel's Incompleteness Theorems*. Number 10 in Oxford Logic Guides. Oxford University Press.

[Stahl, 1973] Stahl, G. (1973). *Elementos de Metamatemática*. Ideas e indagaciones. Editorial Universitaria, Chile.

[Stewart and trad. José María Fraile, 1977] Stewart, I. and trad. José María Fraile (1977). *Conceptos de Matemática Moderna*. Alianza Universidad.

[Suppes, 1960] Suppes, P. (1960). *Axiomatic Set Theory*. Van Nostrand Company, Inc.

[Suppes and trad. Enrique Linés, 1978] Suppes, P. and trad. Enrique Linés, S. H. (1978). *Introducción a la Lógica Matemática*. Editorial Reverté S.A.

[Tarski, 1971] Tarski, A. (1971). *Undecidable Theories*. Studies in Logic and the foundations of Mathematics. North-Holland Publishing Company.

[Wang and trad. Pilar Castillo, 1987] Wang, H. and trad. Pilar Castillo (1987). *Reflexiones sobre Kurt Gödel*. Alianza Universidad.